Journal of Law and Policy

Volume 24 | Issue 1 Article 3

2016

Standing Up For Their Data: Recognizing the True Nature of Injuries in Data Breach Claims to Afford Plaintiffs Article III Standing

Andrew Braunstein

STANDING UP FOR THEIR DATA: RECOGNIZING THE TRUE NATURE OF INJURIES IN DATA BREACH CLAIMS TO AFFORD PLAINTIFFS ARTICLE III STANDING

Andrew Braunstein[*]

Over the last several years, data breaches have become increasingly more common, due in no small part to the failures of organizations charged with storing and protecting personal data. Consumers whose data has fallen victim to these breaches are more often turning to federal courts in attempts to be made whole from the loss of their information, whether simple credit card information or, as breaches become more sophisticated, social security information, medical and financial records, and more. These consumers are often being turned away from the courthouse, however, due to a failure of many federal courts to find that the plaintiffs have Article III standing to pursue claims.

Many of the district courts hearing data breach claims have refused to grant standing because of their interpretation of a recent case addressing constitutional standing, Clapper v. Amnesty International. *These courts have concluded that* Clapper *represents a "tightening" of the traditional standing test under which data breach plaintiffs' claims that they will suffer harm are too speculative. These courts are misguided in their analyses.*

First, the Supreme Court's decision in Clapper *was based on an especially rigorous application of the traditional standing test due to constitutional and national security concerns present in the case. Data breach claims should not be subject to this same level*

[*]J.D. Candidate, Brooklyn Law School, 2016; B.A. in Government & Politics, The University of Maryland, 2013. The author thanks the *Journal of Law and Policy* staff and editors for their insight and guidance throughout the note writing process. He thanks his family and friends for their continued support and encouragement during the note writing process and much more.

of rigor. Second, these district courts are misreading Clapper *to require a demonstration of an injury in data breach cases that is not necessary. These courts are looking for some type of quantifiable injury stemming from the data breach when all that* Clapper *requires is a demonstration that the plaintiffs' data was lost in the breach. Courts should subscribe to this more accurate application of the standing test and of* Clapper *to grant data breach plaintiffs the day in court to which they are entitled.*

INTRODUCTION

In late October of 2014, a group of hackers known as the "Guardians of Peace" breached Sony Pictures' computer network and stole thousands of confidential documents and emails.[1] The group was purportedly working with the North Korean government and breached Sony's network as retaliation for the planned release of *The Interview*, a satirical comedy imagining and depicting the assassination of North Korean leader Kim Jong-un.[2] The Guardians of Peace gradually released its trove of stolen documents to the media and threatened more serious action if the film was released as scheduled.[3] In response, Sony canceled the film's release.[4] This decision garnered widespread criticism from many in the entertainment industry, the news media, and even President Barack Obama who stated that Sony "made a mistake"

---

[1] Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST: THE SWITCH (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

[2] *Id.*; *see also* Peter Travers, *The Interview*, ROLLING STONE (Dec. 24, 2014), http://www.rollingstone.com/movies/reviews/the-interview-20141224.

[3] The hackers even went as far as to promise that theaters showing the film would "remember the 11th of September 2001." Kory Grow, *U.S. Says North Korea Was 'Centrally Involved' in Sony Hack*, ROLLING STONE (Dec. 17, 2014), http://www.rollingstone.com/movies/news/u-s-says-north-korea-was-centrally-involved-in-sony-hack-20141217; *see also* Peterson, *supra* note 1 ("[M]essages purported to be from the hackers alluded to 'The Interview' . . . explicitly mentioning the film while invoking the Sept. 11, 2011, terrorist attacks and threatening theaters that planned to show the film.").

[4] Grow, *supra* note 3.

by cancelling the film's release.[5] Sony ultimately decided to release *The Interview* in select theaters on Christmas Day[6] and also to distribute the film via streaming services such as iTunes, YouTube, and Google Play.[7] The threats of further action turned out to be unfounded and the consequences from the breach were mostly limited to the release of stolen information. The media focused its attention primarily on emails and other documents that offered a glimpse into the inner-workings of Hollywood.[8] However, the truly damaging information that was released was

---

[5] Daniel Kreps, *Barack Obama: Sony Made 'A Mistake' Canceling 'The Interview,'* ROLLING STONE (Dec. 19, 2014), http://www.rollingstone.com/movies/news/barack-obama-sony-mistake-canceling-the-interview-20141219; *see also* Travers, *supra* note 2 ("Prompted by free-speech advocates from George Clooney to President Obama, Sony has semi-reversed itself and set a limited U.S. theatrical release for *The Interview* in a few hundred independent cinemas.").

[6] Travers, *supra* note 2; Jordan Chariton, *'The Interview' to Stream on YouTube, Google Play, Xbox in Unique Sony Release*, WRAP (Dec. 24, 2014), http://www.thewrap.com/sony-youtube-interview-streaming-deal-in-the-works-report/.

[7] Chariton, *supra* note 6.

[8] Some of the most highly publicized documents were lists of executives' and celebrities' salaries and email exchanges disparaging celebrities and other public figures. For example, a spreadsheet was released listing the salaries of seventeen top executives at Sony Pictures Entertainment. Ted Johnson, *Sony Bosses' Alleged Salaries Leak Online Amid Hacking Fallout*, VARIETY (Dec. 1, 2014), http://variety.com/2014/biz/news/sony-bosses-alleged-salaries-leak-online-amid-hacking-fallout-1201368419/. Another document contained a twenty-five page list of executive complaints about the way Sony Pictures was managed, including complaints that "upper management allow[ed] certain talent and filmmakers to bleed [the company] dry with their outlandish requests for private jets, wardrobe and grooming stylists," and concessions that Sony has faltered because it keeps "making the same, safe, soul-less movies and TV shows." Sam Biddle, *Sony Hack Reveals 25-Page List of Reasons it Sucks to Work at Sony*, GAWKER (Dec. 3, 2014), http://gawker.com/sony-hack-reveals-25-page-list-of-reasons-it-sucks-to-w-1666264634. Arguably the most embarrassing (and widely circulated) emails were those between top Sony executives in which they insult various actors—for example, calling Kevin Hart a "whore" and Angelina Jolie a "minimally talented spoiled brat"—and even President Obama, making racially-based jokes about his taste in films. Katie Richards, *The 5 Most Embarrassing Revelations From Sony's Sprawling Hack*, ADWEEK (Dec. 14, 2014), http://www.adweek.com/news/advertising-branding/5-most-embarrassing-revelations-sonys-sprawling-hack-161937.

the "names, addresses, Social Security numbers, employment records, medical history, and financial information of more than 47,000 current and former Sony employees and associates."[9]

This dissemination was especially detrimental, not only because of its scale, but also because of the type of information involved. Though information such as names, addresses, and email addresses are typically already available to advertisers and other organizations, the combination of that information with employment records, medical records, financial records, and Social Security numbers can be especially harmful.[10] Almost immediately after the breach, the affected employees turned to the courts to remedy the damage caused by the loss of their information.[11] The plaintiffs' case seemed strong, not only because the type of data taken was especially valuable, but also because there were many indications that Sony was negligent, or at least careless, in properly safeguarding the information.[12]

Sony had suffered a similar data breach in 2011, during which hackers released the information of millions of subscribers to its PlayStation network.[13] The plaintiffs that lost their data in the 2014 breach claimed that Sony did not do enough to strengthen its networks after the earlier attack and, consequently, the risk of

---

[9] Anne Bucher, *Sony Pictures Hit With 2 More Data Hack Class Action Lawsuits*, TOP CLASS ACTIONS (Dec. 19, 2014), http://topclassactions.com/lawsuit-settlements/lawsuit-news/46162-sony-pictures-hit-2-data-hack-class-action-lawsuits/.

[10] *See* Jordan Robertson, *Here's Why Your Social Security Number Is Holy Grail for Hackers*, BLOOMBERG BUS. (Feb. 5, 2015), http://www.bloomberg.com/news/articles/2015-02-05/here-s-why-your-social-security-number-is-holy-grail-for-hackers.

[11] Seven different class action lawsuits have been filed against Sony. *7 Sony Data Breach Class Action Lawsuits May Be Merged*, TOP CLASS ACTIONS (Jan. 20, 2015), http://topclassactions.com/lawsuit-settlements/lawsuit-news/47912-7-sony-data-breach-class-action-lawsuits-may-merged/.

[12] Kashmir Hill, *Sony Pictures Hack Was a Long Time Coming, Say Former Employees*, FUSION (Dec. 4, 2014), http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/; *see also* Ralph Ellis, *Lawsuits Say Sony Pictures Should Have Expected Security Breach*, CNN (Dec. 24, 2014), http://www.cnn.com/2014/12/20/us/sony-pictures-lawsuits/ ("Sony was negligent because it didn't prepare for a massive cyberattack despite warnings and previous security breaches.").

[13] Ellis, *supra* note 12.

another breach had been foreseeable.[14] Moreover, the plaintiffs (and other reports) alleged that Sony did not act reasonably in securing the data on its networks.[15] For example, its information security team consisted of only eleven employees at the time of the breach, eight of whom were employed at the managerial or executive level.[16] Even more shockingly, the hackers gained significant access after finding an unprotected folder labeled "Passwords" that contained documents, spreadsheets, and PDF's containing thousands of passwords to computers on Sony's internal network.[17] The hackers also gained access to nearly one million customer records after exploiting a well-known and basic loophole that Sony had left open.[18] Despite the apparent strength of these claims on their merits, many of the plaintiffs have run up against the same obstacle that data breach plaintiffs have repeatedly faced: the burden of demonstrating that the harm they suffered is sufficient to maintain Article III standing.[19] This Note addresses how misapplication of the standing doctrine has become one of the most common barriers faced by those seeking a remedy for the loss of their personal information after a breach.

Part I of the Note examines the current landscape of the problem and how both the instances and scale of data breaches have increased dramatically over recent years. This part also examines some potential causes of this increase and explores several legal courses of action taken to remedy the problem and compensate victims. Part II discusses how the standing doctrine

---

[14] *See id.*

[15] *Id.*

[16] Hill, *supra* note 12.

[17] Adam Clark Estes, *The Sony Hack Gets Even Worse as Thousands of Passwords Leak*, GIZMODO (Dec. 4, 2014, 12:25 PM), http://gizmodo.com/sony-pictures-hack-keeps-getting-worse-thousands-of-pa-1666761704.

[18] *See* Herb Weisbaum, *What's With All These $#@& Data Breaches?*, NBC NEWS, http://www.nbcnews.com/id/43499438/ns/business-consumer_news/t/whats-all-these-data-breaches/#.VGIwzL6Qb0s (last visited Sept. 25, 2015).

[19] Paul A. Ferrillo, *Court: Neiman Marcus Customers Have Standing to Bring Putative Class Action Over Data Breach*, CYBER RISK NETWORK (July 28, 2015), http://www.cyberrisknetwork.com/2015/07/28/court-neiman-marcus-customers-have-standing-to-bring-putative-class-action-over-data-breach/ ("To date, standing has been a significant hurdle facing consumers trying to bring massive putative class action lawsuits after data breaches . . . .").

was applied in data breach claims by courts prior to *Clapper* with varying results. Part III addresses a recent seminal case in standing law, *Clapper v. Amnesty International USA*,[20] and examines how that case has resulted in an often stricter application of the standing test which has made it more difficult for data breach plaintiffs to obtain standing.[21] Finally, Part IV argues that courts have widely misapplied *Clapper* to data breach claims. Many district courts that have heard recent data breach claims have relied heavily on *Clapper* and have held that that data breach plaintiffs lacked standing, citing a stricter standing test derived from the Supreme Court's decision in that case.[22] These courts have concluded that the injuries alleged by data breach plaintiffs are too speculative to justify standing under *Clapper*.[23] However, as this Note argues, these courts have misinterpreted the Supreme Court's holding in *Clapper* and have overlooked crucial distinctions between that case and data breach claims.

This Note argues that *Clapper* did not impose a stricter standing test, but instead merely presented a stricter application of the traditional test due to the unique circumstances surrounding the case. Furthermore, this Note contends that district courts that have relied on *Clapper* to deny data breach plaintiffs standing have based their decisions on a misguided analysis of that case. The Court in *Clapper* denied standing based on a plaintiff's failure to show that it would be subjected to government surveillance.[24] Subsequent courts have used this reasoning to deny standing to data breach plaintiffs who fail to show some financial or

---

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

[21] *See* Ferrillo, *supra* note 19; *Does Clapper Silence Data Breach Litigation? A Two-Year Retrospective*, INFO. L. GROUP (Feb. 25, 2015), http://www.infolawgroup.com/2015/02/articles/breach-notice/does-clapper-silence-data-breach-litigation-a-two-year-retrospective/.

[22] S*ee, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 660 (S.D. Ohio 2014); *In re* Sci. Applications Int'l Corp., 45 F. Supp. 3d 14, 31 (D.D.C. 2014); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 879, 882 (N.D. Ill. 2014); *In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013).

[23] S*ee, e.g.*, *Galaria*, 998 F. Supp. 2d at 651–53; *In re Sci. Applications Int'l Corp.,* 45 F. Supp. 3d at 28; *Strautins*, 27 F. Supp. 3d at 876*; In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588, at *2.

[24] *Clapper*, 133 S. Ct. at 1152.

quantifiable harm resulting from a data breach.[25] These courts have used *Clapper* to hold that injury resulting from a data breach is likewise too speculative to support standing.[26]

These decisions have overlooked an important distinction, however. The *Clapper* Court denied standing because the plaintiffs could not prove that they were subjected to surveillance in the first place; not because they could not show that they suffered or were likely to suffer some adverse effect from the surveillance.[27] In most data breach cases, however, it is uncontested that the plaintiffs' data was wrongfully accessed in a breach.[28] Any further inquiry into whether that loss led to any additional damage is irrelevant under *Clapper*. This Note argues that courts deciding data breach cases should limit their standing inquiry to whether or not information was lost in the data breach. This Note concludes that data breach victims can demonstrate injury sufficient enough to maintain standing by simply proving the loss of their data.

I. THE INCREASING PROBLEM OF DATA BREACHES

A. The Recent Rise of Data Breaches[29]

While the publicity surrounding Sony's data breach captured the public's attention, similar types of breaches have been

---

[25] *See, e.g.*, *Galaria*, 998 F. Supp. 2d at 657.

[26] *E.g.*, *id.* at 655.

[27] *See Clapper*, 133 S. Ct. at 1152 ("[R]espondents do not face a threat of certainly impending *interception* . . . .") (emphasis added).

[28] S*ee, e.g.*, Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015) ("*Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place.").

[29] There are differing opinions on what constitutes a "data breach." Byron Acohido, *What Is a 'Data Breach' Really?* CREDIT.COM (Nov. 6, 2014), http://blog.credit.com/2014/11/what-is-a-data-breach-really-100639/. For the purpose of consistency throughout this Note, the term "data breach(es)" refers to, "generally, an impermissible use or disclosure [of electronically stored Personal Identification Information (PII)] that compromises the security or privacy of the protected . . . information." *Breach Notification Rule*, U.S. DEP'T OF HEALTH AND HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/breach-notification /index.html (last visited Sept. 25, 2015).

commonplace for years and unfortunately are becoming even more prevalent. Since 2005, more than 534 million personal records have been lost as a result of data breaches.[30] In 2014 alone there were 579 separate data breaches and experts predict this number will only rise "as consumers become more dependent on Internet-connected devices."[31] The actual number of breaches is likely even higher because security experts generally agree that most breaches are never reported to the public.[32]

Although many of these breaches have involved the dissemination of credit card numbers or basic personal identifiable information ("PII") like names, addresses, email addresses, and phone numbers, the more serious breaches are those in which information such as Social Security numbers, bank account numbers, or medical records, is involved.[33] When a credit card number is stolen, the affected consumers simply need to report the incident and order a new card from their bank.[34] The banks and credit card companies reimburse customers for any fraudulent charges.[35] Also, in most cases advertisers, data brokers, and other parties already have access to many consumers' basic PII.[36] On the other hand, when more sophisticated PII is accessed and wrongfully disseminated, the effects can be incredibly damaging.

---

[30] Weisbaum, *supra* note 18.

[31] Sarah Halzack, *Home Depot and JP Morgan Are Doing Fine. Is it a Sign We're Numb to Data Breaches?*, WASH. POST (Oct. 6, 2014), http://www.washingtonpost.com/news/get-there/wp/2014/10/06/home-depot-and-jpmorgan-are-doing-fine-is-it-a-sign-were-numb-to-data-breaches/.

[32] Weisbaum, *supra* note 18.

[33] *See* Robertson, *supra* note 10.

[34] *Dealing with Credit Card Fraud or Identity Theft*, BANK AM., https://www.bankofamerica.com/credit-cards/education/dealing-with-credit-card-fraud.go (last visited Sept. 25, 2015).

[35] The Fair Credit Billing Act (15 U.S.C. § 1601 *et seq.* (1974)) caps liability for unauthorized credit card charges at $50. *Disputing Credit Card Charges*, FED. TRADE COMMISSION (Aug. 2012), http://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges.

[36] For example, data brokers sell to advertisers information as broad as "marital status, income, job, shopping habits, travel plans and a host of other factors." *Getting to Know You*, ECONOMIST (Sept. 23, 2014), http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party.

For example, the theft of one woman's Social Security number allowed the thief to obtain a driver's license, passport, and bank account in the victim's name.[37] The thief also committed several felonies in the woman's name, impacting her ability to find employment.[38]

Though these types of sophisticated breaches that involve more than simple credit card information are less often publicized than large-scale retail breaches, they occur more frequently and often involve more valuable information.[39] For example, in one of the largest recorded breaches, Chinese hackers attacked the servers of Community Health Systems, one of the nation's largest hospital chains, and stole 4.5 million patients' "names, addresses, birth dates, telephone numbers and Social Security numbers."[40] This is only one example in an alarming string of recent data breaches affecting the healthcare industry.[41] Since the Department of Health and Human Services enacted reporting requirements in 2009 as part of a health record digitization effort, there have been 944 recorded incidents of data breaches involving the records of more than 30 million people.[42]

Other organizations outside the healthcare industry have also become targets for their valuable data over recent years. In fact, in a 2014 study of American companies, forty-three percent of

---

[37] Weisbaum, *supra* note 18.

[38] *Id.*

[39] Between 2005 and September 2015, there were 4,533 breaches involving information other than payment cards and only 65 breaches where credit or debit card information was disseminated. *Chronology of Data Breaches: Custom Sort*, PRIVACY RTS. CLEARINGHOUSE, http://www.privacyrights.org/data-breach/ (last visited Sept. 25, 2015) [hereinafter *Chronology of Data Breaches*].

[40] Jim Finkle & Caroline Humer, *Community Health Says Data Stolen in Cyber Attack from China*, REUTERS (Aug. 18, 2014), http://www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818.

[41] Jason Millman, *Health Care Data Breaches Have Hit 30M Patients and Counting*, WASH. POST: WONKBLOG (Aug. 19, 2014), http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/.

[42] *Id.*

respondents reported that they had fallen victim to a data breach.[43] While retailers seem to have gained the most publicity from these breaches, companies from JP Morgan to Apple have suffered breaches in which massive amounts of customer data was lost.[44] Colleges and universities have fallen victim to an equally concerning raft of data breaches in recent years.[45] In 2014 alone, twenty-eight separate breaches occurred in the education sector, resulting in the dissemination of more than one million records.[46] Breaches into educational institutions are often particularly

---

[43] PONEMON INST., IS YOUR COMPANY READY FOR A BIG DATA BREACH?: THE SECOND ANNUAL STUDY ON DATA BREACH PREPAREDNESS 1 (Sept. 2014), http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

[44] "Verizon's annual Data Breach Investigations Report (DBIR) from May of 2013 found that 24 percent of the confirmed data breaches in 2012 affected the retail and restaurant sector." Tony Bradley, *Retailer Data Breach Trend Not Likely to End Soon*, PC WORLD: NET WORK (Jan. 27, 2014), http://www.pcworld.com/article/2090839/retailer-data-breach-trend-not-likely-to-end-soon.html. In October 2014, the accounts of 76 million individual customers and 8 million small businesses at JP Morgan were hacked. Jake Swearingen, *Why the JP Morgan Data Breach Is Like No Other*, ATLANTIC (Oct. 3, 2014), http://www.theatlantic.com/business/archive/2014/10/why-the-jp-morgan-data-breach-is-like-no-other/381098/. In September 2014, Apple suffered a very well publicized data breach in which more than 100 users' iCloud accounts were hacked, leading to the release of nude photographs, including those of actress Jennifer Lawrence. James Cook, *Inside the iCloud Hacking Ring That Leaked Those Naked Celebrity Photos*, FIN. POST: BUS. INSIDER (Sept. 2, 2014), http://business.financialpost.com/business-insider/inside-the-icloud-hacking-ring-that-leaked-those-naked-celebrity-photos?__lsa=d3b4-b120. Only weeks after the incident, hackers infiltrated 350,000 Chinese iCloud accounts and accessed sensitive data such as account IDs and address book data. Robert Mann, *Just Weeks After Apple's Celebrity Photo Scandal, the Company Has to Deal With a Whole New Security Issue: This Time, It's in China*, ADWEEK (Nov. 6, 2014), http://www.adweek.com/news/advertising-branding/just-weeks-after-apples-celebrity-photo-scandal-company-has-deal-whole-new-security-issue-161261.

[45] In fact, the author of this Note was a victim of a 2014 data breach at the University of Maryland in which the "name[s], Social Security number[s], date[s] of birth, and University identification number[s]" of 287,580 . . . faculty, staff, students and affiliated personnel" were released. *UMD Data Breach*, U. MD., http://www.umd.edu/datasecurity/ (last visited Sept. 25, 2015).

[46] *Chronology of Data Breaches*, *supra* note 39.

harmful because of the nature of the information that these institutions maintain.[47] Colleges and universities often collect and store especially valuable information such as financial records, bank information, and even students' and faculty's Social Security numbers.[48]

B. The Causes of the Rise

One reason for the precipitous increase in the number and severity of data breaches is the continuous migration of information to electronic format. Consumers now overwhelmingly rely on credit cards to purchase goods, both in stores and online.[49] Additionally, businesses are increasingly replacing their file cabinets with electronic cloud based storage from services like Microsoft, Google, and newer companies like Box.[50] Universities have been making a similar transition to electronic storage for years and now store almost all student records in electronic databases accessible to administrators (and hackers) via the Internet.[51]

Consumers are also moving their personal data into an electronic format where it is vulnerable to unauthorized access. A

---

[47] *See* Kyle McCarthy, *5 Colleges with Data Breaches Larger Than Sony's in 2014*, HUFF POST COLLEGE (Jan. 15, 2015), http://www.huffington post.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html.

[48] In all five of the largest college or university breaches in 2014, partial or whole social security numbers, and in some cases corresponding names and bank information, were disseminated. *Id.*

[49] A report issued by Javelin Strategy and Research determined that in 2012, credit or debit cards purchases comprised 66% of all "in person" payments. Catherine New, *Cash Dying as Credit Card Payments Predicted to Grow in Volume: Report*, HUFF POST MONEY (June 7, 2012), http://www. huffingtonpost.com/2012/06/07/credit-card-payments-growth_n_1575417.html. Moreover, in 2012, nearly 6% of all commercial transactions were conducted online. *Id.*

[50] Quentin Hardy, *Google, Microsoft and Others Delve Deeper into Cloud Storage for Businesses*, N.Y. TIMES (June 25, 2014), http://www.nytimes.com /2014/06/26/technology/google-microsoft-and-others-delve-deeper-into-cloud-st orage-for-businesses.html.

[51] Jason Koebler, *Who Should Have Access to Student Records?*, U.S. NEWS (Jan. 19, 2012, 12:20 PM), http://www.usnews.com/news/articles/2012 /01/19/who-should-have-access-to-student-records.

2013 study by the Pew Research Center found that 51% of all adults in the United States now use online banking services that allow access to, and often storage of, important bank account information on home computers.[52] Thirty-two percent of U.S. bank account holders also use mobile banking services,[53] which makes information potentially even more vulnerable as it could be accessed on mobile phones. The migration to electronic storage has increased the quantity of information open to a breach and has left more consumers reliant on organizations to adequately protect their data.

Unfortunately, as discovered in the aftermath of Sony's 2014 breach, many organizations entrusted with storing consumer data are failing. Several companies that have suffered data breaches have been accused of failing to take adequate steps to protect the data they are charged with keeping safe.[54] A recent report found that of the 254 breaches in the first quarter of 2014 that resulted in the loss of more than 200 million records, "only 1% were 'secure breaches' or breaches where strong encryption, key management and/or authentication solutions" and other best practices were employed.[55] For example, in the Sony breach, hackers exploited a well-known and "basic" loophole to gain access to 101 million customer and employee records.[56]

Many organizations also fail when responding to a breach once it does happen. During a 2013 breach at Target, employees failed to react to alerts from a cyber-security team and "stood by as 40 million credit card numbers—and 70 million addresses, phone numbers, and other pieces of personal information—gushed out of its mainframes."[57] Neiman Marcus similarly failed to act when it

---

[52] Susannah Fox, *51% of U.S. Adults Bank Online*, PEW RES. CTR. (Aug. 7, 2013), http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/.

[53] *Id.*

[54] For example, one expert at a corporate security company stated that in several recent breaches, the hackers "were using basic techniques that have been understood for some [fifteen] years." Weisbaum, *supra* note 18.

[55] SAFENET, BREACH LEVEL INDEX: FIRST QUARTER RECAP 2014 (2014), http://breachlevelindex.com/pdf/Breach-Level-Index-Report-Q12014.pdf.

[56] *See* Weisbaum, *supra* note 18.

[57] Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. (Mar. 13, 2014),

ignored 59,746 warnings of "suspicious behavior" on its network.[58] The company had also disabled its security system's ability to automatically block suspicious flagged activity in order to make maintenance easier.[59] These oversights led to the loss of 350,000 customers' credit and debit card information.[60] Ultimately, consumers bear the brunt of the harm caused by this failure of organizations to store their users' information securely.

C. Legal Remedies for Data Breaches

Various legal strategies have been used in attempts to take action against companies that fail to protect consumers' data. The Federal Trade Commission ("FTC") has taken action against, and reached fifty civil settlements with, breached companies for unreasonable data security practices, "principally through enforcement of Section 5 of the FTC Act."[61] While these settlements may have in some instances "halted harmful data security practices [and] required companies to accord stronger protections for consumer data,"[62] they often serve a symbolic function rather than a practical one. The FTC has reached settlements with only a small fraction of the thousands of companies that have been breached.[63] The settlements also rarely

---

http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

[58] Ben Elgin et al., *Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data*, BLOOMBERG BUS. (Feb. 21, 2014), http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data.

[59] *Id.*

[60] Venkat Balasubramani, *Seventh Circuit: Data Breach Victims Have Standing Based on Future Harm*, TECH. & MKTG. L. BLOG (July 24, 2015), http://blog.ericgoldman.org/archives/2015/07/seventh-circuit-data-breach-victims-have-standing-based-on-future-harm.htm.

[61] FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT (2014) [hereinafter FTC Settlements], https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[62] *Id.*

[63] Since 2005 there have been nearly 5,000 data breaches. *Chronology of Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, http://www.privacyrights.org/data-breach/new (last visited Sept. 25, 2015).

impose any fines or damages and instead center on enforcing more effective data security practices.[64] In one such settlement, clothing retailer TJ Maxx agreed to "implement a comprehensive security program[,] . . . be audited by security professionals every other year for 20 years[,] . . . [and] identify internal and external security risks and assess the sufficiency of any safeguards in place to control these risks."[65] In a similar settlement, the FTC required health care billing company Accretive Health to implement a comprehensive information security program and submit the program for evaluation "every two years by a certified third party."[66] Often, these settlements merely require companies to take actions they should have already been taking; TJ Maxx, Accretive Health, and other breached companies should have had the agreed-to security protocols in place *before* their respective breaches. Perhaps the biggest flaw in the FTC settlements, however, is that consumers, the parties actually harmed by these data breaches, may not receive any type of compensation for their lost information.[67]

Because of this, many victims of data breaches have pursued claims in federal court against the organizations that were supposed to be securely storing their data.[68] These victims have

---

[64] *See, e.g.*, Shannon Henson, *FTC, TJX Settle Retail Data Breach Cases*, LAW360 (Mar. 28, 2008), http://www.law360.com/articles/51413/ftc-tjx-settle-retail-data-breach-cases.

[65] *Id.*

[66] *Accretive Health Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information,* FED. TRADE COMMISSION (Dec. 31, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/accretive-health-settles-ftc-charges-it-failed-adequately-protect.

[67] For example, the Accretive Health settlement agreement did not "include a monetary penalty." Marianne Kolbasuk McGee, *Accretive Health Breach: FTC Settlement*, DATA BREACH TODAY (Jan. 2, 2014), http://www.databreachtoday.com/accretive-health-breach-ftc-settlement-a-6332#.

[68] S*ee, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 69–70 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 650 (S.D. Ohio 2014); *In re* Sci. Applications Int'l Corp., 45 F. Supp. 3d 14, 19 (D.D.C. 2014); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 873 (N.D. Ill. 2014); *In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *1–2 (N.D. Ill. Sept. 3, 2013). Often, these cases are brought as a single class action in one jurisdiction. D. Christopher Robinson & Casey Wood Hensley, *Cyber Security*

alleged a variety of different claims. Plaintiffs have alleged that the information was a bailment and the "bailee"—the organization charged with keeping it safe—was negligent in doing so under property law concepts.[69] Others have claimed that the companies violated some state or federal regulation.[70] The most common claims, however, have been tort claims for failing to adequately store personal information.[71] Despite the apparent viability of these claims, many federal courts have dismissed them, finding that the plaintiffs did not have sufficient standing to bring a claim in

---

Breach Triggers Class Action Lawsuit Against eBay, FROST, BROWN, TODD LLC: CLASS COUNSEL BLOG (Aug. 15, 2014), http://www.classcounselblog.com/cyber-security-eBay-class-action-identity-theft. Other times, suits are brought as separate class actions in different jurisdictions that are subsequently "centralized" by the Panel on Multi-District Litigation into a single claim heard by a single district court. *Overview of Panel*, U.S. JUDICIAL PANEL ON MULTIDISTRICT LITIG., http://www.jpml.uscourts.gov/panel-info/overview-panel (last visited Sept. 25, 2015). The Panel "determine[s] whether civil actions pending in different federal districts involve one or more common questions of fact such that the actions should be transferred to one federal district for coordinated or consolidated pretrial proceedings; and . . . select[s] the judge or judges and court assigned to conduct such proceedings." *Id.* The actions are consolidated to "avoid duplication of discovery, to prevent inconsistent pretrial rulings, and to conserve the resources of the parties, their counsel and the judiciary." *Id.* Counsel for the original classes usually act together as co-counsel and if the claim proceeds to a final judgment or settlement, any damages awarded are distributed amongst the class often from a central fund overseen by the court. *See Multi-District Litigation FAQ's*, CLASS ACTION LITIG. INFO., http://www.classactionlitigation.com/mdl/faq.html (last visited Sept. 25, 2015).

[69] *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 651 (S.D. Ohio 2014); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 955 (S.D. Cal. 2012).

[70] Such plaintiffs often base their claims in legislation like the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*) which regulates the collection, dissemination, and use of consumer information. *See, e.g.*, *Galaria*, 998 F. Supp. 2d at 652. Plaintiffs can also pursue similar claims based on similar state statutes. *See, e.g.*, *In re Sony Gaming Networks*, 903 F. Supp. 2d at 965–66 (noting that plaintiffs pursued claims based on California's consumer protection statutes wherein companies were supposed to take reasonable measures to protect consumer information).

[71] *See, e.g.*, *Reilly*, 664 F.3d at 40; Krottner v. Starbucks Corp., 628 F.3d 1139, 1140–41 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 635 (7th Cir. 2007); *Galaria*, 998 F. Supp. 2d at 653; *In re Sony Gaming Networks*, 903 F. Supp. 2d at 959–60.

federal court under Article III of the Constitution.[72] These courts have found that the plaintiffs have not suffered a cognizable Article III injury unless or until their stolen information is used in a way that causes quantifiable financial harm.[73] Although some courts have been willing to find a sufficient injury even without some quantifiable, demonstrable harm,[74] the Supreme Court's decision in *Clapper v. Amnesty International USA*[75] largely changed the prevailing understanding of the injury requirement and led to dismissal of many more data-breach claims.[76]

However, *Clapper* should not be read to require the dismissal of these data breach claims. First, the Court in *Clapper* applied a stricter standing test because of the national security and separation of powers concerns present in the case.[77] Second, and more importantly, the injuries alleged in *Clapper* are distinguishable from those that data breach plaintiffs allege. In *Clapper*, the Court found that there was no injury because the plaintiffs could not show that they were subject to surveillance.[78] In all meritorious data breach claims, however, the plaintiffs can all show that they were subject to lost data. In *Clapper*, the Court did not require a showing of harm *resulting from* any surveillance; it simply found that the plaintiffs could not prove there was surveillance in the first place.[79] Data breach plaintiffs, by contrast, can all show that their data was lost and should not be forced by a misapplication of *Clapper* to demonstrate some type of harm beyond that initial loss.

---

[72] *See, e.g.*, *Katz*, 672 F.3d at 80–81; *Reilly*, 664 F3d at 46.

[73] *See, e.g.*, *Katz*, 672 F.3d at 79–80; *Reilly*, 664 F.3d at 42 ("We conclude that Appellants' allegations of hypothetical, future injury are insufficient to establish standing."); *Galaria*, 998 F. Supp. 2d at 656–57.

[74] *See, e.g.*, Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693–94 (7th Cir. 2015).

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

[76] *See* Heidi J. Milicic, *Standing to Bring Data Breach Class Actions Post-*Clapper, AM. BAR ASS'N: COM. & BUS. LITIG. (Aug. 7, 2014), http://apps.americanbar.org/litigation/committees/commercial/articles/summer2014-0814-data-breach-class-actions-post-clapper.html.

[77] *See Clapper*, 133 S. Ct. at 1147.

[78] *Id*. at 1152.

[79] *See id*.

Courts should recognize the true injuries of data breach claims and the sufficiency of those injuries for standing.

II. STANDING AND DATA BREACH CLAIMS

The doctrine of standing is derived from Article III of the Constitution.[80] The relevant clause states:

> The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their authority . . . to Controversies between two or more States;--between a State and Citizens of another State;--between Citizens of different States;--between Citizens of the same State claiming Lands under Grants of different states, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.[81]

Article III extends to federal courts the authority to hear a case or controversy between two adversarial parties.[82] Notably, the clause does not explicitly mention standing or any requirement of injury.[83] Since 1944, however, the Supreme Court has interpreted Article III's confinement of federal jurisdiction to "cases" or "controversies" as a requirement that a party have "standing to sue" in order to bring a claim in federal court.[84] To satisfy the modern standing test, a party must be able to prove a sufficient injury.[85]

---

[80] U.S. CONST. art. III, § 2, cl. 1.

[81] *Id*.

[82] *See id*.

[83] *Id.*

[84] Stark v. Wickard, 321 U.S. 288, 303–04 (1944) (holding that a plaintiff may only "secure judicial intervention" if he "possesses something more than a general interest in the proper execution of the laws . . . "); Bradford C. Mank, *Judge Posner's "Practical" Theory of Standing: Closer to Justice Breyer's Approach to Standing than to Justice Scalia's*, 50 HOUS. L. REV. 71, 77–78 (2012) [hereinafter Mank, *Judge Posner's Practical Theory*].

[85] *Wickard*, 321 U.S. at 305 (finding that the Plaintiff had "such a personal claim as justifies judicial consideration").

Until the late twentieth century, standing simply meant that a party bringing a federal claim needed to have a legitimate "genuine interest and stake" in the claim.[86] The standing requirement mainly served to ensure that a plaintiff had a true cause of action in each claim she brought.[87] Modern standing doctrine also reflects other constitutional ideals that the Supreme Court has sought to uphold by narrowing the circumstances under which parties may bring a claim.[88] One underlying concern of the standing doctrine is the issuance of advisory opinions.[89] By limiting standing to parties that have actually suffered a real injury, courts may only hear claims resulting from true "cases" or "controversies" rather than issuing decisions about speculative "what-ifs."[90] Standing doctrine also preserves separation of powers.[91] Many scholars and jurists believe that limiting standing is essential to ensure that federal courts only hear matters prescribed to them by the Constitution and Congress.[92] The Supreme Court has consistently enforced the standing requirement as a way to "prevent the judicial process from being used to usurp the powers of the political branches."[93]

Currently, the Supreme Court employs a three-part test to determine whether a party has sufficient standing to bring a claim

---

[86] Mank, *Judge Posner's Practical Theory*, *supra* note 84, at 77–78.

[87] *See* Cass Sunstein, *What's Standing After* Lujan*? Of Citizen Suits, "Injuries," and Article III*, 91 MICH. L. REV. 163, 168–171 (1992).

[88] Mank, *Judge Posner's Practical Theory*, *supra* note 84, at 78 ("Standing requirements are related to broader constitutional principles.").

[89] *Id.* ("Standing doctrine prohibits unconstitutional advisory opinions."). Some scholars argue that the standing doctrine does not actually assist in prohibiting advisory opinions, yet the Court and other scholars still often cite this as a major rationale for the development of the standing doctrine. *See, e.g.*, William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 247 (1988).

[90] Fletcher, *supra* note 89, at 222.

[91] *See* Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 881 (1983) (arguing that the standing doctrine is an essential element of separation of powers). For a further discussion of Scalia's argument see Mank, *Judge Posner's Practical Theory*, *supra* note 84, at 104–05.

[92] Scalia, *supra* note 91, at 881 ("[J]udicial doctrine of standing is a crucial and inseparable element [of separation of powers].").

[93] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013).

under Article III.[94] The plaintiff must first demonstrate that she has "suffered an 'injury in fact' . . . which is (a) concrete and particularized and (b) 'actual or imminent, not conjectural or hypothetical.'"[95] The plaintiff must then show that "there [is] a causal connection between the injury and the conduct complained of."[96] To satisfy this requirement "the injury has to be 'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.'"[97] Finally, the plaintiff must establish that "it [is] 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'"[98] The plaintiff carries the burden of satisfying all three prongs of this test.[99]

This test, and the Court in interpreting it, stresses that an injury must be imminent, and that merely speculative or hypothetical injuries will not suffice for purposes of standing.[100] In *Lujan v. Defenders of Wildlife*, a case in which the Court clarified the modern, pre-*Clapper* standing requirement, the Supreme Court held that the plaintiffs lacked standing to bring a claim challenging U.S. government agencies' failure to consult with the Secretary of the Interior before defunding projects that could harm endangered species in Egypt and Sri Lanka.[101] The plaintiffs claimed that they were injured because they intended on going back abroad to observe the endangered animals.[102] The Court dismissed this claim finding that the plaintiffs failed to demonstrate any required

---

[94] For further explanation of the three-part test see Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

[95] *Id.* (citations omitted) (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

[96] *Id.* at 560.

[97] *Id.* (alterations in original) (quoting Simon v. E. Ky. Welfare Rights Org., 42 U.S. 26, 41–42 (1976)).

[98] *Id.* at 561 (quoting *Simon*, 42 U.S. at 38, 43).

[99] *See id.*

[100] *See id.*; *see also* Bradford C. Mank, Clapper v. Amnesty Int'l*: Two or Three Competing Philosophies of Standing Law?*, 81 TENN. L. REV. 211, 220 (2014) [hereinafter Mank, Clapper v. Amnesty Int'l].

[101] *Lujan*, 504 U.S. at 558–59, 563, 578.

[102] *Id.* at 563.

"actual or imminent" injury.[103] The majority opinion cited one plaintiff's admission that she had "no current plans" to return and concluded that mere "'some day' intentions—without any description of concrete plans, or indeed even any specification of *when* the some day will be—[can]not support a finding of the 'actual or imminent injury' that our cases require."[104]

Prior to *Clapper,* federal district and circuit courts applied the standing test derived from *Lujan* to data breach claims with conflicting results. Some courts held that data breach plaintiffs could not claim sufficient injuries to maintain standing unless they could demonstrate that they were actually harmed by the data breach (for example, subjected to identity theft or other fraud).[105] These courts concluded that harms such as the increased risk of identity theft or the increased risk of data misuse did not meet *Lujan*'s "actual or imminent" injury requirement.[106] For instance, in *Reilly v. Ceridian Corp.*, the plaintiff, whose data was accessed in the breach of a payroll services company, pursued a claim against the company alleging injury in the form of an increased risk of identity theft and costs of monitoring credit activity.[107] The Third Circuit held that the plaintiffs' "allegations of hypothetical, future injury [were] insufficient to establish standing," mainly because the allegations of harm were "dependent on entirely speculative, future actions of an unknown third-party."[108] The court reasoned that the plaintiff could not demonstrate sufficient injury to maintain standing unless or until his information was

---

[103] *Id.* at 564 ("[The Plaintiffs' affidavits] plainly contain no facts, however, showing how damage to the species will produce 'imminent' injury . . . .").

[104] *Id.*

[105] *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 79–80 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011).

[106] *See, e.g.*, *Katz*, 672 F.3d at 79–81 (rejecting several claims because Plaintiff failed to meet "irreducible minimum requirements of pleading and Article III" in light of the fact that plaintiff did not allege any actual exposure or misuse of her personal information); *Reilly*, 664 F.3d at 46 ("[Plaintiffs'] allegations of an increased risk of identity theft as a result of the security breach are hypothetical, future injuries, and are therefore insufficient to establish standing.").

[107] *Reilly*, 664 F.3d at 40.

[108] *Id.* at 42.

misused in a way that actually caused some sort of cognizable injury.[109]

Other courts in pre-*Clapper* data breach cases reached the opposite conclusion and held that the plaintiff could demonstrate a sufficiently imminent injury to maintain standing.[110] These courts recognized that the increased risk of future harm that could occur as a result of the breach was a sufficiently imminent injury.[111] In *Krottner v. Starbucks Corp.*, for example, the Ninth Circuit concluded that the plaintiffs "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."[112] While the conflict over what burden data breach plaintiffs must meet to establish standing still exists, the Supreme Court's decision in *Clapper v. Amnesty International*, issued shortly after the decisions like those in *Reilly* and *Krottner*, has seemed to change the common understanding of standing in data breach cases and has been particularly persuasive to courts hearing such cases.

---

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

[110] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632–34 (7th Cir. 2007) (finding sufficient standing for plaintiffs bringing a data breach claim against a bank even though the plaintiffs did not incur any financial loss or suffer identity theft); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140–43 (9th Cir. 2010) (finding standing when Starbucks employees' PII was accessed from a stolen employee laptop).

[111] *See, e.g.*, *Krottner*, 628 F.3d at 1143 (holding that "Plaintiffs–Appellants have alleged a credible threat of real and immediate harm"); *Pisciotta*, 499 F.3d at 634 (holding that the "injury-in-fact requirement can be satisfied by a threat of future harm or by an act . . . increasing the risk of future harm that the plaintiff would have otherwise faced . . . ").

[112] *Krottner*, 628 F.3d at 1143. The court ultimately dismissed the claims, concluding that while the increased risk of identity theft was enough to maintain Article III standing, it was not enough to sufficiently plead the claims of negligence and breach of implied contract under Washington state law. *See id.* at 1140.

III. *CLAPPER V. AMNESTY INT'L USA*: AN APPARENT "TIGHTENING" OF THE STANDING TEST

While the Supreme Court has not definitively stated whether and under what circumstances data breach plaintiffs can meet their standing burden, in *Clapper v. Amnesty International* the Court seemed to offer some guidance.[113] In that case, Amnesty International's U.S. branch ("Amnesty") brought a claim against the federal government challenging the constitutionality of a National Security Agency ("NSA") surveillance program.[114] The Supreme Court did not reach the merits of the claims, but instead solely addressed whether Amnesty had Article III standing to bring its claims.[115]

Amnesty claimed that it frequently communicated with foreign organizations and individuals in other countries whom it believed were targets of NSA surveillance.[116] It asserted it had sufficient Article III standing because of the "objectively reasonable likelihood" that these communications with foreign entities would be acquired by the NSA.[117] Amnesty argued that this compromised its ability to "locate witnesses, cultivate sources, obtain information, and communicate confidential information to [its] clients."[118] Alternatively, Amnesty alleged that even if this potentially threatened injury was not sufficiently imminent for standing purposes, it also suffered the present injury of being

---

[113] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013) (ruling that that the Second Circuit's "objectively reasonable likelihood" standard does not satisfy the requirement that a "threatened injury must be certainly impending to constitute injury in fact").

[114] *Id.* at 1142. The plaintiff-respondents sought declaratory and injunctive relief, claiming that Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which permitted government surveillance of individuals who were reasonably believed to be outside of the United States and who were not "United States persons" was unconstitutional. *Id.* The term "United States person" denotes a U.S. citizen, a permanent resident alien, or a U.S. corporation. 50 U.S.C. § 1801(i) (2015).

[115] *Clapper*, 133 S. Ct. at 1155.

[116] *Id.* at 1142.

[117] *Id.* at 1143.

[118] *Id.* at 1145.

forced to "take costly and burdensome measures to protect the confidentiality of [its] international communications."[119]

The Court held that Amnesty did not have standing under either theory.[120] The majority opinion, written by Justice Alito, concluded that Amnesty's "theory of *future* injury [was] too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'"[121] The majority explained that the threatened injury rested on Amnesty's "highly speculative fear" of a "highly attenuated chain of possibilities."[122] The Court viewed this fear as even more speculative because several of the links in the chain relied on the decisions of independent actors including the NSA, the Foreign Intelligence Surveillance Court, and Amnesty's foreign contacts.[123] Ultimately, Amnesty could only speculate that the government would use surveillance in a way that would affect it, and this speculation was not enough to maintain standing.[124]

The Court found Amnesty's alternative theory of present injury similarly insufficient.[125] Amnesty claimed that it suffered ongoing injuries due to precautions it took to avoid having its communications intercepted, such as communicating "in generalities rather than specifics" and traveling to have in-person conversations rather than speaking over phone or email.[126] The

---

[119] *Id.* at 1143.

[120] *Id.* at 1155.

[121] *Id.* at 1143.

[122] *Id.* at 1148 ("[R]espondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under §1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.").

[123] *Id.* at 1148–50.

[124] *Id.* ("[R]espondents' speculative chain of possibilities does not establish that injury based on potential future surveillance is certainly impending . . . .").

[125] *Id.* at 1150.

[126] *Id.* at 1150–51 (internal quotation marks omitted).

Court rejected this claim as nothing more than a "repackaged version" of Amnesty's first attempt to gain standing.[127] It viewed the costs that Amnesty "incurred to avoid surveillance [as] simply the product of their fear of surveillance."[128] The majority was skeptical of Amnesty "manufactur[ing] standing merely by inflicting harm on [itself] based on [its] fears of hypothetical future harm that is not certainly impending." The Court further stated that granting standing for this injury would allow the plaintiffs, "for the price of a plane ticket [to] transform their standing burden from one requiring a showing of actual or imminent . . . interception to one requiring a showing that their subjective fear of such interception is not fanciful, irrational, or clearly unreasonable."[129] Ultimately, the Court found all the injuries Amnesty claimed too speculative to meet its standing burden.[130]

Many scholars and lower courts have viewed the Court's decision in *Clapper* as a "tightening" of the imminence test required to demonstrate Article III standing.[131] For many, the decision requires that a plaintiff now demonstrate not only that it would be objectively reasonable for an injury to occur, but also that the injury be *certainly* impending.[132] The decision was seen as an especially "pivotal point in the evolving law of data breach" standing.[133] Many observers viewed *Clapper* as making it nearly impossible for data breach plaintiffs to maintain standing if the only injury they can point to is the mere loss of their data.[134]

---

[127] *Id.* at 1151.

[128] *Id.*

[129] *Id.*

[130] *Id.* at 1155.

[131] *See, e.g.*, Mank, Clapper v. Amnesty Int'l, *supra* note 100, at 222.

[132] *Id.*

[133] Judy Selby & Corey Dennis, *No Data Misuse? No Standing for Data Breach Plaintiffs*, LAW360 (Apr. 24, 2014), http://www.law360.com/articles/529877/no-data-misuse-no-standing-for-data-breach-plaintiffs.

[134] *See, e.g.*, Mank, Clapper v. Amnesty Int'l, *supra* note 100, at 221–22; Milicic, *supra* note 76; David R. Singh et al., *Data Breach Class Action Defendants Look to NSA Case*, LAW360 (July 15, 2014), http://www.law360.com/articles/556770/data-breach-class-action-defendants-look-to-nsa-case; Selby & Dennis, *supra* note 133. Admittedly, some of this post-*Clapper* assessment may be attributable to the Defense bar eager for a new tool to protect data breach clients from costly class action litigation.

Academics and practitioners experienced in data breach cases argued that *Clapper* bars data breach plaintiffs unless they can demonstrate a concrete and cognizable harm that has occurred from the loss of data, such as identity theft or financial loss.[135]A number of courts have subscribed to this thinking and have dismissed data breach claims for lack of standing under *Clapper*.[136] The plaintiffs could not show any presently occurring harm and the courts dismissed the claims because the injuries the plaintiffs asserted were too speculative to satisfy *Clapper's* "certainly impending"[137] test for future injuries.[138]

In one of the first cases to apply the supposedly stricter *Clapper* test to a data breach plaintiff, *In re Barnes & Noble Pin Pad Litigation*, the District Court for the Northern District of Illinois dismissed the plaintiffs' claims for lack of standing.[139] The plaintiffs alleged various types of harms resulting from Barnes & Noble's alleged failure to safeguard customers' personal information and the resulting breach including:

> untimely and inadequate notification of the security breach, improper disclosure of their personal identifying information or 'PII', loss of privacy, expenses incurred in efforts to mitigate the increased risk of identity theft or fraud, time lost mitigating the increased risk of identity theft or

---

[135] *See, e.g.*, Mank, Clapper v. Amnesty Int'l, *supra* note 100, at 221–22; Milicic, *supra* note 76; Singh, *supra* note 134; Selby & Dennis, *supra* note 133.

[136] *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 650 (S.D. Ohio 2014); *In re* Sci. Applications Int'l Corp., 45 F. Supp. 3d 14, 31 (D.D.C. 2014); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 879, 882 (N.D. Ill. 2014); *In re* Barnes & Noble Pin Pad Litig., 12-CV-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013).

[137] Clapper v. Amnesty Int'l USA, 133 S. Ct 1138, 1143 (2013).

[138] *Galaria*, 998 F. Supp. 2d at 655; *In re Sci. Applications Int'l Corp.,* 45 F. Supp. 3d at 25; *Strautins*, 27 F. Supp. 3d at 875, 882*; In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588, at *5.

[139] *In re Barnes & Noble*, 2013 WL 4759588, at *5. The class action plaintiffs were customers of Barnes & Noble during the time when the company lost customers' credit card information to "skimming"; software was installed on the company's computers that automatically downloaded the number and cardholder information of credit cards swiped at Barnes & Noble registers. *Id.* at *1.

> fraud, an increased risk of identity theft, deprivation of the value of Plaintiffs' PII, and anxiety and emotional distress.[140]

The court found none of these injuries sufficient to meet the standing burden.[141] Applying *Clapper*, the court held that the plaintiffs failed to demonstrate that any of the injuries were certainly impending.[142] The court concluded that the plaintiffs, like those in *Clapper*, incurred expenses to mitigate the alleged increased risk of identity theft out of unfounded fear.[143] Thus, the court considered all of the plaintiffs' claimed injuries too speculative to meet its interpretation of the *Clapper* standard.[144] Several other courts have used the same test and analysis to produce similar holdings in the wake of the *Clapper* decision.[145] Contrary to the conclusions in these cases, the injuries alleged in data breach cases should be sufficient to maintain standing, even when analyzed using *Clapper*.

IV. DISTINGUISHING *CLAPPER*'S INJURIES

For several reasons, *Clapper* actually does support standing for data breach plaintiffs when the alleged injury is loss of their data. First, *Clapper* is, by the Court's own admission, an "especially rigorous" application of the Court's standing test due to the Court's concerns about the case's implications on separation of powers, foreign affairs, and national security.[146] Data breach claims, by

---

[140] *Id.* at *2.

[141] *Id.* at *3–6.

[142] *Id.*

[143] *Id.* at *4.

[144] *Id.* at *5.

[145] *See* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 655 (S.D. Ohio 2014) ("Plaintiffs failed to allege facts demonstrating the increased risk makes any future injury 'certainly impending' as opposed to speculative."); *In re* Sci. Applications Int'l Corp., 45 F. Supp. 3d 14, 28 (D.D.C. 2014) ("In sum, increased risk of harm alone does not constitute an injury in fact. Nor do measures taken to prevent a future, speculative harm."); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) ("*Clapper* compels rejection of [the] claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing.").

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

contrast, generally involve two civilian parties and the claims do not focus on issues of national security or foreign policy.[147] Instead, plaintiffs almost always bring fairly straightforward civil claims.[148] Second, the Court in *Clapper* did not employ a stricter or even different standard than that used in previous standing jurisprudence. The Supreme Court used the same standing test and found that the plaintiffs in *Clapper*, and the injuries they claimed, could not pass that test.[149] In the data breach context, however, plaintiffs suffer sufficient injuries to afford them standing under the traditional standing test.

Many courts relying on *Clapper* to deny data breach plaintiffs' standing analogize the alleged injuries in *Clapper* to data breach harms[150] and determine that data breach injuries are likewise too speculative.[151] This interpretation of *Clapper* overlooks an important distinction. The *Clapper* Court did not conclude that being subjected to government surveillance was too speculative a *type* of injury to maintain standing; instead, the Court held that the plaintiffs' claim that the injury had actually or would actually happen—that they were subjected or were likely to be subjected to that surveillance—was too speculative.[152] In the data breach context, however, the plaintiffs can easily prove that they have been subjected to a data breach and the loss of personal information.[153] This reading and application of *Clapper*, coupled

---

[147] *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 69–70 (1st Cir. 2012) (involving a dispute between an accountholder and broker); Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011) (involving a dispute between law firm employees and payroll processing firm); *Galaria*, 998 F. Supp. 2d at 650 (involving a dispute between consumers and insurer); *Strautins*, 27 F. Supp. 3d at 873 (involving a dispute between consumers and data security company).

[148] *See, e.g.*, *Katz*, 672 F.3d at 70; *Reilly*, 664 F.3d at 40; *Galaria*, 998 F. Supp. 2d at 649; *Strautins*, 27 F. Supp. 3d at 873 (all involving claims of negligence).

[149] *Clapper*, 133 S. Ct. at 1153.

[150] *See, e.g.*, *Galaria*, 998 F. Supp. 2d at 654 ("Plaintiffs' contention that an increased risk of harm constitutes injury-in fact is similar to the respondent's position in [*Clapper*].").

[151] *Id.* at 654–55.

[152] *Clapper*, 133 S. Ct. at 1150.

[153] *See, e.g.*, Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015) ("[I]t is important not to overread *Clapper. Clapper* was addressing

with the recognition that the *Clapper* Court was applying the traditional standing test in a uniquely rigorous way, makes it clear that data breach plaintiffs should have standing under *Clapper*.

A. The "Especially Rigorous" Application in Clapper

The majority opinion in *Clapper* indicates that the holding may not be applicable to other contexts like data breaches and instead might be limited to the facts and circumstances of that case.[154] The Court stated that its "standing inquiry ha[d] been especially rigorous when reaching the merits of the dispute would force [it] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."[155] The majority recited previous decisions where the court refrained from finding standing when it might expand judicial power at the cost of legislative or executive power, or otherwise intrude on a policy decision made by Congress or the Executive.[156] The Court further stated that this is especially true in the context of foreign relations and national security.[157] The majority pointed out that the Court

---

speculative harm based on something that may not even have happened to some or all of the plaintiffs. In our case, Neiman Marcus does not contest the fact that the initial breach took place.").

[154] *Clapper*, 133 S. Ct. at 1147. *See also* Mank, Clapper v. Amnesty Int'l, *supra* note 100, at 225–26 ("The Clapper decision sent mixed signals about whether its approach to standing was generally applicable to all cases or whether it was more limited to standing in intelligence-gathering and foreign affairs cases.").

[155] *Clapper*, 133 S. Ct. at 1147 (quoting Raines v. Byrd, 521 U.S. 811, 819–20 (1997)).

[156] *Id.* (first citing Raines v. Byrd, 521 U.S. 811, 819–20 (1997); then citing Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, 454 U.S. 464, 473–74 (1982) (finding that standing would violate Constitutional constraints on the power of the judiciary); and then citing Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 222 (1974) ("[H]ere the relief sought would, in practical effect, bring about conflict with two coordinate branches.")).

[157] *Id.* (first citing United States v. Richardson, 418 U.S. 166, 170 (1974) (denying standing to a plaintiff challenging the constitutionality of a statute allowing the director of the CIA to be the sole certifying auditor of agency expenditures); then citing Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 222 (1974) (ruling that plaintiffs lacked standing to challenge

had "often found a lack of standing [when] the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs."[158] The opinion then listed extensive precedent in which the Court had refused to grant standing to parties seeking to challenge the constitutionality of policies and programs created by the military or the intelligence community, such as the Central Intelligence Agency or NSA.[159]

Data breach claims should not be subject to this level of rigor. The vast majority of data breaches affect business and commercial entities like retail stores, banks, and other financial service providers, or institutions such as hospitals and universities.[160] Government entities, especially those involved in national security or foreign affairs, are rarely involved in breaches that expose consumer data.[161] Moreover, claims against data breach defendants typically sound in tort, contract, or property and do not contain the constitutional separation of powers implications that motivated the stricter standing inquiry in *Clapper*.[162] Therefore, data breach

---

Congress member's enlistment in Armed Forces Reserve); and then citing Laird v. Tatum, 408 U.S. 1, 11–16 (1972) (finding no standing for plaintiffs challenging Army intelligence program)).

[158] *Id.*

[159] *Id.* at 1148.

[160] In 2013, breaches of "Business," "Educational," "Financial/Credit," and the "Health/Medical" Industries composed approximately 90.9% of all data breaches. *ITRC 2013 Breach List Tops 600 in 2013,* IDENTITY THEFT RESOURCE CTR., http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html (last updated Feb. 5, 2015).

[161] Some institutions commonly affected by breaches, such as hospitals and universities, are considered government entities for some purposes. However, they are rarely involved in matters of intelligence or national security and there is no reason to think that a plaintiff pursuing an action for data breach against this type of entity would be denied standing because of separation of powers concerns. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 649 (S.D. Ohio 2014) (plaintiffs pursued claims under tort and property theories against a private entity); *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1211 (N.D. Cal. 2014) (plaintiffs pursued claim for declaratory relief against a private company).

[162] *See, e.g.*, *Galaria*, 998 F. Supp. 2d at 649 (plaintiffs alleged tort claims of increased risk of identity theft, loss of privacy, deprivation of value of PII, and a negligent bailment property claim.); *In re Adobe*, 66 F. Supp. 3d at 1211

claims do not deserve the "especially rigorous" application of the standing test found in *Clapper*.[163]

B. The Injuries Sustained by Data Breach Plaintiffs are Different Than Those in Clapper *and Are Sufficiently "Imminent"*

Data breach plaintiffs most commonly attempt to demonstrate standing by showing an increased risk of future harm due to the loss of data and the cost to monitor and/or mitigate this risk.[164] For example, the plaintiffs in *Galaria v. Nationwide Mutual Insurance Company* claimed that they:

> incurred . . . damages in the form of . . . the imminent, immediate, and continuing increased risk of identity theft, identity fraud . . . out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other data breach risk mitigation products . . . expenses incurred to mitigate the increased risk of identity theft, identify fraud and/or medical fraud . . . [and] the value of the time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud.[165]

The District Court in *Galaria* relied on *Clapper*'s analysis and "certainly impending" standard to deny standing to the plaintiffs for both the increased harm injuries and the mitigation injuries.[166] The court analogized these injuries to the injuries in *Clapper* and

---

(plaintiffs alleged *inter alia* that Adobe breached its contract by providing inadequate security measures).

[163] *Clapper*, 133 S. Ct. at 1147.

[164] *See, e.g.*, *Galaria*, 998 F. Supp. 2d at 651 (noting that the plaintiffs alleged harm from "increased risk of harm/cost to mitigate increased risk."); *In re Adobe*, 66 F. Supp. 3d at 1211 ("Plaintiffs allege that they have all suffered at least one of three types of cognizable injuries-in-fact: (1) increased risk of future harm; (2) cost to mitigate the risk of future harm; and/or (3) loss of the value of their Adobe products.").

[165] *Galaria*, 998 F. Supp. 2d at 651. The Plaintiffs also alleged harm in the form of "loss of privacy and . . . deprivation of the value of [their] PII." *Id.*

[166] *Id.* at 657–58.

held that "neither the increased risk nor the expenses to mitigate that risk constitute an injury-in-fact sufficient to confer standing."[167] Citing *Clapper* throughout its opinion, the *Galaria* court concluded that "the increased risk that Plaintiffs will be victims of identity theft, identity fraud, medical fraud, or phishing at some indeterminate point in the future" was too speculative to support standing.[168] The majority concluded that just as in *Clapper*, the plaintiffs could not "manufacture standing"[169] simply "by choosing to make expenditures in order to mitigate a purely speculative harm."[170] The court found that the plaintiffs' claims of increased risk of identity theft were comparably speculative to Amnesty International's claims that it had an increased risk of its communications being intercepted by the government.[171]

Other courts followed the same reasoning as the *Galaria* court, applying *Clapper's* "certainly impending" requirement and finding that the data breach plaintiffs' "theor[ies] of future injury" were too speculative to maintain standing.[172] In *Strautins v. Trustwave Holdings*, the District Court for the Northern District of Illinois compared the alleged injury—increased risk of future identity theft—to the injuries in *Clapper* and concluded that the injuries were based on a "chain of attenuated hypothetical events and actions by third parties independent of the defendant."[173] However, the courts deciding *Galaria* and *Strautins*, and others that reach the same conclusions, mistakenly conflate two very distinguishable sets of injuries.

An overly strict reliance on *Clapper* has caused these courts to overlook that the injury in data breach cases is the loss of the data itself. Although concrete financial or other injury may not immediately follow a data breach, courts need not look for this type of harm when applying the standing test, even as articulated in

---

[167] *Id.* at 658.

[168] *Id.* at 657.

[169] *Id.* (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143, 1151 (2013)).

[170] *Id.* at 658.

[171] *Id.* at 654–55.

[172] *Id.*

[173] Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014).

Clapper. The true injury the Court looked for in *Clapper* was the "interception" of the plaintiffs' communications. The Court did not search for any harm resulting from the interception; the interception itself would have been enough if the plaintiffs had been able to demonstrate it had actually occurred.[174] In the data breach context, the "interception" of the plaintiffs' data is the similarly sufficient injury. Because this type of loss necessarily occurs for plaintiffs who can show they are victims of a data breach, courts should recognize standing for data breach plaintiffs even if applying *Clapper*.

A later case addressing Article III standing, *Susan B. Anthony List v. Dreihaus* supports this proposition.[175] In *Dreihaus*, the Supreme Court considered the standing of plaintiffs pursuing a pre-enforcement challenge to an Ohio statute prohibiting the use of certain statements during political campaigns.[176] The Court held that the plaintiffs did have standing to challenge the statute even before it was enforced in a way that caused any harm or injury to the plaintiff.[177] The majority reasoned that the plaintiffs should not need to subject themselves to "an actual arrest, prosecution, or other enforcement" as "a prerequisite to challenge the law."[178] Part of the analysis hinged on the fact that the plaintiffs provided evidence to demonstrate that they would be subjected to the law.[179]

The Court used *Clapper*'s "certainly impending" imminence test and also took guidance from extensive precedent affording parties standing to challenge allegedly unconstitutional statutes *before* their enforcement.[180] These "pre-enforcement"[181] cases

---

[174] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151–52 (2013). The Court noted that the Second Circuit held that Amnesty had standing "due to the objectively reasonable likelihood that their communications will be intercepted at some time in the future." *Id.* at 1146.

[175] Susan B. Anthony List v. Dreihaus, 134 S. Ct. 2334 (2014).

[176] *Id.* at 2338.

[177] *Id.* at 2347.

[178] *Id.* at 2342.

[179] *Id.* at 2343. The Plaintiff alleged in its complaint an "inten[t] to engage in substantially similar activity in the future," contending that these future actions "will remain arguably proscribed by Ohio's false statement statute," and therefore the "threat of future enforcement of the false statement statute is substantial." *Id.* at 2343–45 (alteration in original).

[180] *Id.* at 2341–42.

instruct that "a plaintiff satisfies the injury-in-fact requirement where he alleges 'an intention to engage in a course of conduct . . . and there exists a credible threat of prosecution thereunder.'"[182] The Court recognized that the true injury in pre-enforcement cases was the mere passing and existence of a potentially unconstitutional law and not the resulting punishment.[183]

The Supreme Court has long recognized "pre-enforcement" standing, like that in *Dreihaus*, and has allowed plaintiffs to challenge potentially unconstitutional statutes before the statutes are actually enforced.[184] Such plaintiffs may suffer distress from the fear of eventually being arrested, prosecuted, fined, or otherwise punished while simply waiting for a statute to be enforced.[185] The Court has acknowledged that unconstitutional statutes might also have a "chilling effect" that has the same ultimate effect as the statute being enforced; people refrain from the prohibited behavior out of fear of eventual enforcement.[186] The Court has also recognized that it should not force individuals to subject themselves to punishment in order to challenge a potentially unconstitutional statute.[187]

---

[181] Steffel v. Thompson, 415 U.S. 452, 459 (1974) ("[I]t is not necessary that petitioner first expose himself to actual arrest or prosecution to be entitled to challenge a statute that he claims deters the exercise of his constitutional rights."); MedImmune, Inc. v. Genetech, Inc., 549 U.S. 118, 128–29 (2007) ("[W]e do not require a plaintiff to expose himself to liability before bringing suit to challenge the basis for the threat."); Virginia v. Am. Booksellers Assn., 484 U.S. 383 (1988); Holder v. Humanitarian Law Project, 561 U.S. 1 (2010).

[182] *Dreihaus*, 134 S.Ct. at 2342 (quoting Babbit v. Farm Workers, 442 U.S. 289, 298 (1979)).

[183] *See id.* at 2347.

[184] *See id.* at 2342 ("When an individual is subject to such a threat, an actual arrest, prosecution, or other enforcement action is not a prerequisite to challenging the law."); *see also Steffel*, 415 U.S. at 459; *MedImmune Inc.*, 549 U.S. at 128–29; Babbit v. Farm Workers, 442 U.S. 289 (1979); *Am. Booksellers Assn.*, 484 U.S. at 383; *Holder,* 561 U.S. at 1.

[185] *See Dreihaus*, 134 S. Ct. at 2342.

[186] *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 11 (1972) (citing to several cases where the Supreme Court has found that government action has a "chilling effect" on behaviors and speech even though it does not directly prohibit that behavior or speech).

[187] *See Dreihaus*, 134 S. Ct. at 2342.

This same reasoning applies in data breach cases and should allow data breach plaintiffs standing at the moment their data is lost in a breach. The fear of identity theft and the distress caused by anticipating the unauthorized use of one's PII are cognizable injuries, especially because plaintiffs cannot retrieve the exposed information which can now be used by any person anywhere in the world.[188] Furthermore, in the data breach context, victims have no control over how a third party will use their data. Courts should not force these victims to wait until their data is misused to permit them to seek to remedy their injuries in court.

Some lower courts hearing recent data breach claims have begun to recognize this and have applied *Clapper* to data breach cases to find sufficient basis for standing. [189] In a less publicized 2011 breach of Sony, the company's PlayStation network suffered a "massive breach . . . that led to the theft of names, addresses, and possibly credit card data belonging to 77 million user accounts."[190] The District Court for the Southern District of California concluded that the plaintiffs did have standing even under *Clapper*.[191] The court rejected Sony's argument that *Clapper* "tightened the 'injury-in-fact' analysis . . . previously relied upon by" courts addressing Article III standing.[192] The court recognized that, although *Clapper* used different language than earlier

---

[188] *See* Bob Unruh, *U.S. 'Forever Threatened by OPM Data Breach,'* WND (June 29, 2015), http://www.wnd.com/2015/06/u-s-forever-threatened-by-opm-data-breach/.

[189] *See, e.g.*, Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693–94 (7th Cir. 2015); *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 961–62 (S.D. Cal. 2014).

[190] Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

[191] *In re Sony Gaming Networks*, 996 F. Supp. 2d at 960. The court had already denied Sony's motion to dismiss for lack of standing but agreed to reconsider the motion after the *Clapper* opinion was issued, recognizing that "Article III standing is an 'indispensable part of a plaintiff's case.'" *Id.* at 960 (quoting Lujan v. Defenders of Wildfire, 504 U.S. 555, 561 (1992)). Notably, the court upheld its ruling that the Plaintiff's had sufficient standing, even when applying *Clapper* to the claim. *Id.* at 962–63.

[192] *Id.* at 961.

cases,[193] it "did not set forth a new Article III framework . . . [or] overrule previous precedent."[194] Instead, the court noted, "the Supreme Court's decision in *Clapper* simply reiterated an already well-established framework for assessing whether a plaintiff had sufficiently alleged an 'injury-in-fact' for purposes of establishing Article III standing."[195] The court rejected the stricter application of *Clapper* and recognized that *Clapper* merely restated the traditional standing test, which affords data breach plaintiffs standing.[196]

The *In re Sony* court also disagreed with Sony's second argument that the plaintiffs did not have sufficient standing because "their Personal Information was [never] actually accessed by a third party."[197] The court acknowledged that neither *Clapper*, nor any earlier standing cases, required these types of allegations.[198] The plaintiffs only needed to allege a "'credible threat' of impending harm based on the disclosure of their personal information following the intrusion."[199] In other words, data breach plaintiffs do not need to demonstrate that their information was actually used in a way that caused some sort of quantifiable monetary harm. Instead, the loss of the information itself is enough to warrant standing.

A similar 2014 decision lends additional support. In *In re Adobe Systems Inc. Privacy Litigation*, the District Court for the Northern District of California denied Adobe Systems' motion to dismiss a class action data breach claim for lack of Article III standing.[200] Adobe argued, like Sony, that *Clapper* established a stricter standing test that the plaintiffs in this case could not

---

[193] For example, in *Krottner,* a pre-*Clapper* data breach standing case, the court required a showing of a "credible threat of harm" that is "real and immediate." Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

[194] *In re Sony Gaming Networks*, 996 F. Supp. 2d at 961.

[195] *Id.*

[196] *Id.*

[197] *Id.* at 962.

[198] *Id.*

[199] *Id.*

[200] *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d. 1197, 1232 (N.D. Cal. 2014).

pass.[201] The court disagreed, however, noting that "*Clapper* did not change the law governing Article III standing," and "did not overrule any precedent [or] reformulate the familiar standing requirements of injury-in-fact, causation, and redressability."[202] Further, the court recognized that "*Clapper*'s discussion of standing arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result."[203]

The *In re Adobe* court held that the injuries the plaintiffs were claiming were "sufficiently concrete and imminent to satisfy *Clapper*."[204] The court based this conclusion primarily on the understanding that the true damage that should be analyzed in data breach claims is the loss of the information itself.[205] The court recognized that "in contrast to *Clapper*, where there was no evidence that any of respondents' communications either had been or would be monitored . . ., here there [was] no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken."[206] The *In re Adobe* court properly recognized that the injuries alleged in *Clapper* were too speculative only because there was no evidence that the plaintiffs' communications actually were or would be intercepted.[207] In data breach cases, however, the plaintiffs are in court only because their information has already been intercepted.[208]

---

[201] *Id.* at 1212.

[202] *Id.* at 1213.

[203] *Id.* at 1214 (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)).

[204] *Id.*

[205] *Id.* at 1214–15. ("[T]he threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*." There is no "need to speculate as to whether the hackers intend to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so.").

[206] *Id.*

[207] *Id.*

[208] *See id.* at 1215–16.

The In re Sony Networks and *In re Adobe* decisions[209] represent an important shift in data breach litigation. Not only did the courts recognize that the plaintiffs met their standing burden but they also explicitly stated that *Clapper* does not bar data breach claims and instead permits them even when the only harm a plaintiff can show is that their information was wrongfully accessed in a breach.[210] Courts should stop interpreting *Clapper* as a requirement that the plaintiffs demonstrate injury resulting from some *use* of lost information and instead should read *Clapper* to recognize that the true injury in a data breach claim is the loss of the information alone.

CONCLUSION

As data breaches become more common and more severe, more consumers are turning to the courts to remedy their injuries and are often being denied standing because of many courts' misapplication of *Clapper*.[211] These courts are mistakenly comparing the claimed injury in *Clapper*—government surveillance—to what they view as the injury in data breach cases—some harm stemming from the data breach.[212] The true injury in data breach cases, however, is the loss of the claimant's

---

[209] It should be noted that both of these cases were decided in the Ninth Circuit (in the Southern and Northern Districts of California, respectively) and the courts deciding these cases relied heavily on the Ninth Circuit decision in Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010), which granted standing for data breach plaintiffs. *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d. at 1211–12; *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 958 (S.D. Cal. 2012). It is currently unclear how much influence this circuit's precedent had on these decisions and how a district court in another circuit without this type of precedent would decide a similar set of facts.

[210] *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d. at 1214; *In re Sony Gaming Networks*, 903 F. Supp. 2d at 958.

[211] *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64, 80–81 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 663 (D. Oh. 2014).

[212] *See, e.g.*, *Galaria*, 998 F. Supp. 2d at 654 ("Plaintiffs' contention that an increased risk of harm constitutes injury-in-fact is similar to the respondent's position in *Clapper* . . . ").

information during the breach. This more truly comports with the Supreme Court's recognition in *Clapper* that the plaintiffs in that case did not have to demonstrate some negative effect stemming from surveillance, but had to show only the occurrence or imminent risk of "interception" itself.[213] Courts hearing data breach cases in the future should be careful to recognize that the real injury to data breach plaintiffs is not some type of expense or hardship following a data breach but is instead the interception of information itself. By recognizing this true nature of the injury in data breach claims, courts can grant data breach plaintiffs the standing, and the access to the judicial system, to which they are entitled.

[213] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1152 (2013).