DEFENDING WITH *CLAPPER*: APPLYING THE SUPREME COURT'S ARTICLE III STANDING INTERPRETATION TO DATA BREACH LAWSUITS

Conor L. McSweeney*

I. Introduction

Massive amounts of personal data are collected, analyzed, and stored in today's digital economy.[1] United States citizens are more susceptible to threats in the cyber-security landscape than ever before, and historical notions of personal privacy have significantly eroded.[2] By purchasing just one song on iTunes, creating a single so-

* J.D. Candidate, Suffolk University Law School, 2018.

[1] *See* Peter Segrist, *How the Rise of Big Data and Predictive Analytics Are Changing the Attorney's Duty of Competence*, 16 N.C. J. L. & TECH. 527, 530-31 (2015) (discussing the vast amount of personal data collected by corporations and the relative lack of regulation in the areas of data collection and its commoditization). Segrist further noted the reduction in privacy in modern times, stating: "…modern enterprise and invention have, through invasions upon his privacy, subjected [man] to mental pain and distress, far greater than could be inflicted by mere bodily injury." *Id.* at 530. The primary way corporations track users is through the recording of Internet Protocol ("IP") addresses and tying it to information from an Internet Service Provider ("ISP"), or through cookies that carry user information from a computer as it browses various web sites on the Internet. *Id.* at 537-40.

[2] *See Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), *archived at* https://perma.cc/6NUZ-ZJDD (noting the rapidly evolving threat landscape and advising best practices to businesses for guarding consumer's personal information); *see also* Sammi Caramela, *Cybersecurity: A Small Business Guide*,

 ISSN 1536-7983.

cial media account, or signing up for online banking, a consumer invariably increases the risk of their personal information being stolen and put up for sale on the Darknet.[3] While consumer participation in the digital economy evolved from convenient to mandatory, the chances of an unauthorized breach of personal data have increased from possible to likely.[4] Despite strict protections under federal law, the healthcare industry's adoption of modern digital practices have made our medical records vulnerable to fraud like all other content on the Internet.[5] Swiping your credit card at a brick and mortar retail store like Target, Inc. could result in the exploitation of cardholder data by identity thieves hacking through a backdoor to the computer network.[6]

BUSINESS NEWS DAILY (June 2, 2017), *archived at* https://perma.cc/T2ZP-S2X2 (listing the myriad of cybersecurity threats in today's landscape, such as malicious software ("malware") and Distributed Denial of Service ("DDoS") attacks).

[3] *See* Rick Delgado, *What the Rise of the Darknet Could Mean for You*, BETA NEWS (2016), *archived at* https://perma.cc/AJA8-NGF3 (explaining how customer data in possession of businesses ends up for sale on the Internet's black market); *see also* Donna Fuscaldo, *5 groups at greater risk of identity theft*, BANK RATE (Aug. 14, 2012), *archived at* https://perma.cc/AG7L-ZX7J (highlighting consumer vulnerability in the digital age when using social media, credit cards, smart phones, or public Wi-Fi); *see also* Andrew Delamarter, *The Darknet: A Quick Introduction for Business Leaders*, HARV. BUS. REV. (Dec. 9, 2016), *archived at* https://perma.cc/5WNW-LF2E (summarizing what the Darknet is and its origins for a business audience). The Darknet consists of a series of marketplaces and message boards that cannot be found through standard open Internet search engines and "can only be accessed through anonymizing software such as Tor, which obscures the user's IP address." *Id.* The cloak of anonymity and lack of traceability on the Darknet allows for the relatively easy transfer of illicit goods like drugs and weapons, but also vast caches of personal information from identity theft and corporate secrets obtained through hacking. *Id.*

[4] *See* Ivar A. Hartmann, *A Right To Free Internet? On Internet Access And Social Rights*, 13 J. HIGH TECH. L. 297, 303-04 (2013) (positing that access to the Internet has evolved to become an autonomous right crucial to expression in modern society); *see also* Michael L. Rustad, *Consumer Law Symposium: Punitive Damages In Cyberspace: Where In The World Is The Consumer?*, 7 CHAP. L. REV. 39, 39 (2004) (identifying the incredible number of Internet users today and the increasing risk of consumer identity theft to through "fraudulent internet scams" such as phishing and viruses).

[5] *See* Stanley C. Ball, *Ohio's Aggressive Attack On Medical Identity Theft*, 24 J. L. & HEALTH 111, 117-19 (2011) (explaining how data breaches exposing medical identity theft of one's medical information, stored online, can result in severe consequences for a victim's health insurance benefits).

[6] *See* Brian Krebs, *Sources: Target Investigating Data Breach*, KREBS ON SEC. (Dec. 13, 2013), *archived at* https://perma.cc/WXQ5-3PPL (acknowledging a 2013

There are countless examples just over the last few years where corporations proved to be incapable of protecting their client's personal information.[7] Sony Entertainment, Yahoo, Target, and EBay all have been subject to data breaches in recent years, and there does not appear to be any relief in sight.[8] In the aftermath of any data breach, a class-action lawsuit of affected persons typically follows in an attempt to hold the corporation accountable for violation of its duty to adequately protect its customers' personal information.[9] In order to overcome the initial hurdle necessary to sue the corporation,

data breach of Target, Inc. that affected 40 million credit and debit accounts due to the "theft of data stored on the magnetic stripe of cards used at the stores" rather than Target's online website).

[7] *See* Bartlomiej Hanus & Marian K. Riedy, *Yes, Your Personal Data Is at Risk: Get Over It!,* 19 SMU SCI. & TECH. L. REV. 3, 5-6 (2016) (pointing out that data breaches are a common occurrence when so many businesses are collecting the personal data of consumers online). "Data breaches regularly mak[ing] headline news stories . . . should come as no surprise. We live in the "big data" world of interconnected digital information . . . Any reasonable person should know this information is also subject to misuse." *Id.* The self-inflicted exposure brought on by citizens through pervasive use of the Internet has brought upon too heavy a burden for private industry and the government to effectively monitor. *Id.* at 7.

[8] *See Sony locks 93,000 online accounts after security breach,* BBC NEWS (Oct. 12, 2011), *archived at* https://perma.cc/UCS2-WT24 (highlighting a data breach on the Sony PlayStation network that resulted in hackers obtaining user name and password data of tens of thousands of customers); *see also Target Data Theft Affected 70 Million Customers*, BBC NEWS (Jan. 10, 2014), *archived at* https://perma.cc/BSY5-76M3 (describing how thieves stole the names and credit card information of 70 million Target customers); *see also* Jane Wakefield, *eBay faces investigations over massive data breach*, BBC NEWS (May 23, 2014), *archived at* https://perma.cc/W6LA-6ND5 (discussing the fall-out after eBay experienced a massive breach of personal data affecting approximately 145 million customers); *Yahoo 'state' hackers stole data from 500 million users*, BBC NEWS (Sept. 23, 2016), *archived at* https://perma.cc/4GTF-P2CK (disclosing Yahoo's acknowledgement that the names, email addresses and unencrypted security questions of 500 million users were exposed in a "state-sponsored" hack of Yahoo's IT systems).

[9] *See* J. Thomas Ritchie, *Data Breach Class Actions*, WESTLAW 44 BRIEF 12, 13-14 (2015) (noting the commonality of data breaches and the speed with which class action litigation has evolved in recent times). "In the most general terms, typical cases follow this pattern: a consumer, suing on behalf of a putative class, alleges that a company breached its duty to customers by allowing a data breach to occur and confidential information to fall into the hands of third parties." *Id.* at 14. Plaintiffs have so far been relatively unsuccessful pursuing these class action suits because of the issue presented by Article III standing. *Id.* at 15.

that is, to acquire Article III standing, a plaintiff must prove they experienced an injury-in-fact, such as identity theft or fraud.[10] While consumers do not always experience these harms immediately following a data breach, they are arguably at an increased risk of identity theft due to the public exposure of their sensitive personal information.[11] The Supreme Court most recently provided guidance on Article III standing analysis in *Clapper v. Amnesty International.*[12] While most circuits now refer to *Clapper* as the precedent for standing analysis in the corporate data breach context, some circuits disagree as to its applicability.[13]

Part II of this note traces the historical background of the Constitutional limitations on courts to hear cases and controversies when a plaintiff lacks standing.[14] Then, I will analyze standing in the

[10] *See id.* at 14 (explaining the first requirement in Article III standing analysis). "The first major fight in most data breach cases is whether the plaintiff has suffered an injury-in-fact sufficient to confer standing." *Id.*

[11] *See* Segrist, *supra* note 1, at 574 (concluding that the only way to mitigate potential harms of personal information being hacked and exposed is to limit your participation online and in the digital economy).

> In the current, largely unregulated, environment, where personal information is readily sold as a commodity, the risk that such personal information will someday be used against a person increases with each day that passes, each transfer of personal data between parties, and each click and keystroke. As such, the only true protection a person has is to limit the information that he or she volunteers to the world, to the best that they are able.

Id.

[12] *See* Clapper v. Amnesty Int'l USA, et al., 133 S. Ct. 1138, 1143 (2013) [hereinafter *Clapper II*] (summarizing the issue under review by the Supreme Court in the *Clapper* case as whether the plaintiffs have standing to bring suit against the United States government).

[13] *See* Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 856 (2015) (opining that *Clapper* changed the standing analysis to dismiss data breach cases alleging an increased risk of harm, but no actual harm). "Arguably, *Clapper* ... compels the conclusion that Peters lacks standing to bring her federal claims to the extent they are premised on the heightened risk of future identity theft/fraud." *Id. But see* In re Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1213-14 (2014) (ignoring *Clapper's* holding). "*Clapper* did not change the law governing Article III standing." *Id.* at 14. The Ninth Circuit distinguishes the subject matter of the *Clapper* case as being distinct from a corporate data breach and does not agree that it overrules existing case precedent within its jurisdiction. *Id.*

[14] *See infra* Part II.

data breach context, showing different examples of how the Seventh and Ninth circuits dealt with data breach class-actions in the pre-*Clapper* environment, along with a brief outline of the circumstances relevant to the *Clapper* decision. Part III will analyze the Supreme Court's decision in *Clapper* and its impact on the various circuit courts' standing analysis.[15] By highlighting the need for business certainty that *Clapper* brings to the issue of standing, Part IV of this note will defend *Clapper's* assertion of the firm injury-in-fact requirement.[16] Part IV will also assert that *Clapper* offers the most realistic guidance to the courts when participation in the digital economy backfires and a corporation experiences a data breach.[17] Part V will advocate that the Supreme Court hear a case regarding a data breach and hold the same result with respect to its earlier *Clapper* decision.[18] Businesses face unprecedented exposure to litigation in the digital economy and they simply cannot withstand the dangerous exposure to a lower standing threshold than was intended under the Constitution.[19]

I. History

A. Constitutional Basis for Standing

The framers of the Constitution granted federal courts limited jurisdiction to hear cases and controversies.[20] Standing law is associated with the Constitutional theory of separation of powers, and

[15] *See infra* Part III.
[16] *See infra* Part IV.
[17] *See infra* Part IV.
[18] *See infra* Part V.
[19] *See Clapper II*, 133 S. Ct. 1138, 1147 (2013) (quoting United States v. Richardson, 418 U.S. 166, 188 (1974)).
[20] *See* U.S. CONST. art. III, § 2, cl. 1 (referencing the constitutional basis for the standing requirement).

> 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 all Cases affecting Ambassadors, other public Ministers and Consuls;--to all Cases of admiralty and maritime Jurisdiction;--to Controversies to which the United States shall be a Party;--to Controversies between two or more States;--between a State and Citizens of another State;--between Citizens of different States,--between

is intended to prevent litigants from using the judicial process to usurp the powers of the legislative and executive branches.[21] American case law over time developed three essential elements to determine whether a plaintiff acquired standing, which is the minimum threshold that must be met by a plaintiff before for the merits of a case or controversy may be heard in a court of law.[22] First, the plaintiff must establish they suffered an "injury-in-fact," which means the plaintiff experienced "an invasion of a legally protected interest" that is (a) concrete and particularized, and (b) "actual or imminent, not conjectural or hypothetical."[23] Secondly, there must be a causal connection between the injury and the conduct complained of, such that it is reasonably traceable to the challenged action of the defendant.[24] Finally, it must be considered likely that the injury will be redressed favorably in court.[25] If a plaintiff does not have Article III standing

> 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.

Id.

[21] *See Clapper II*, 133 S. Ct. at 1147 (quoting United States v. Richardson, 418 U.S. 166, 188 (1974)) (discussing the constitutional background of modern standing law). "Relaxation of standing requirements is directly related to the expansion of judicial power." *Id.* The separation of powers at the core of the United States Constitution intended the legislative body to make the law while the courts should only interpret the law. *Id.* When the courts begin expanding the law beyond their constitutional authority, it affects the delicate balance of American democracy. *Id.*

[22] *See id.* (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)) (outlining the requirements for a plaintiff to be successful in their challenge against Article III standing). "Standing under Article III of the Constitution requires that an inquiry be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *See* Monsanto Co., 561 U.S. at 149.

[23] *See* Lujan v. Def. of Wildlife, 504 U.S. 555, 560 (1991) (setting forth the first element of the test for Article III standing that requires an injury-in-fact). The injury-in-fact requirement is the most heavily scrutinized in the Article III standing analysis for data breach cases. *Id.* at 564.

[24] *See id.* at 560 (explaining that the second element in the standing analysis requires there be a nexus between the harm and the alleged conduct). It is important to note the injury cannot be derived from the independent action of a third party who is not involved in the litigation. *Id.*

[25] *See* Raines v. Byrd, 521 U.S. 811, 818-20 (1997) (discussing third element of standing that requires there be a likelihood that the court will grant relief for the harm experienced by the plaintiff). The plaintiff cannot advance litigation based

in the eyes of the court, then there is no federal subject matter jurisdiction over the lawsuit and the case is dismissed.[26] The standing requirement is necessary to ensure the federal courts are not over-burdened by litigation that falls outside their constitutional authority.[27] While plaintiffs would undoubtedly prefer to jump straight to the litigation of a suit on its merits, the test for standing has endured to play its proper role in filtering out disputes.[28]

B. Applying Standing to the Data Breach Context

1. Focus on the First Element

The most important element of the Article III standing rule in the data breach context is the injury-in-fact requirement.[29] In order for a plaintiff to establish injury-in-fact, they must allege an injury has actually occurred, or is imminent, and such injury is "distinct and palpable as opposed to merely abstract."[30] Typically, this is met through actual direct injury following a data breach, like when a person experiences identity theft or the fraudulent misuse of their financial information after their personal information is exposed.[31] In one

upon a speculative claim, but those grounded in fact that show a likelihood of success on the merits. *Id.*

[26] *See* Cetacean Cmty. v. Bush, 386 F.3d 1169, 1174 (9th Cir. 2004) (highlighting the important role standing plays in allowing a plaintiff to be heard in federal court).

[27] *See Raines*, 521 U.S. at 820 (noting the separation of powers is necessary to maintain a balance emanating from the constitutional authority to hear cases and controversies in federal court).

[28] *See id.* (providing rationale for why the Article III standing test in federal courts withstood the test of time as a major part of the federal litigation process). "In the light of this overriding and time-honored concern about keeping the Judiciary's power within its proper constitutional sphere, we must put aside the natural urge to proceed directly to the merits of this important dispute and to settle it for the sake of convenience and efficiency." *Id.*

[29] *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (opining that many courts have held that plaintiffs whose data has "been compromised, but not yet misused" do not qualify for federal jurisdiction, for a lack of standing).

[30] *See* Whitmore v. Arkansas, 495 U.S. 149, 155 (1990) (highlighting the limitations upon which injury-in-fact can be asserted).

[31] *See* Ritchie, *supra* note 9, at 14 (discussing some of the most common injuries asserted by plaintiffs in data breach cases). The courts also consider costs associated with opening and closing accounts as well as credit monitoring services incurred to mitigate against the breach. *Id.*

rare data breach case, the court allowed a plaintiff's stress and anxiety associated with knowledge that their personal information was exposed to qualify as direct injury.[32] Inclusion of the concept of "imminence" leaves open a flexible interpretation by the courts that a plaintiff need not immediately experience the injury, as long as they are likely to be harmed in the near-future.[33] The Supreme Court held on numerous occasions that usage of the term "imminent" means the injury asserted must be "certainly impending."[34] Meanwhile, a new concept of "future injury" emerged in the Ninth Circuit where an individual acquired standing for direct injury due to the future expectation of a harmful conduct.[35] The courts have struggled for uniformity

[32] *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) (explaining the court's acceptance of the plaintiff's mental health and wellness argument as direct injury to satisfy the injury-in-fact requirement). This Ninth Circuit case is an isolated opinion on mental health injury but it radically stretched injury-in-fact possibilities. *Id.*

[33] *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 (1991) (concluding that the plaintiff's harm is not likely to occur within a reasonably ascertainable timeline, if ever). "Although 'imminence' is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes- that the injury is certainly impending." *Id.* Justice Scalia's decision slammed the brakes on the expansion of what constitutes "imminent" harm to align with the highly-developed law regarding the degree of certainty that a plaintiff will likely experience the alleged harm in order to acquire Article III standing. *Id.*

[34] *See Whitmore*, 495 U.S. at 158 (denying the opportunity to recover for future injuries). "A threatened injury must be 'certainly impending' to constitute injury in fact." *Id. See also* DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 345 (2006) (defining the elemental rule regarding "imminent" injury to mean the harm must be "certainly impending"); *see also* Pennsylvania v. West Virginia, 262 U.S. 553, 593 (analyzing whether the plaintiff's suit is premature because it has not yet experienced the alleged harm). "One does not have to await the consummation of threatened injury to obtain preventive relief. If the injury is certainly impending that is enough." *Id.*

[35] *See* Scott v. Pasadena Unified Sch. Dist., 306 F.3d 646, 656 (9th Cir. 2002) (outlining the requirements for a plaintiff to allege a future injury to satisfy the injury-in-fact requirement). "A plaintiff may allege a future injury in order to comply with this requirement, but only if he or she is immediately in danger of sustaining some direct injury as the result of the challenged official conduct…." *Id.* The concepts of future injury, and that a harm be certainly impending to qualify as imminent, are nearly one in the same. *Id.* However, the courts have developed the slightly different terminology and tests over time in different circuits to evaluate the injury-in-fact element of Article III standing. *Id.*

in addressing how far removed the threat of future harm may be from the conduct in order to satisfy the injury-in-fact element.[36]

2. Seventh and Ninth Circuit Pre-Clapper Determinations

The Seventh Circuit first implemented the looser injury-in-fact test for data breach cases in *Pisciotta v. Old Nat'l Bancorp*.[37] In *Pisciotta*, the court sustained the plaintiff's argument of heightened threat of future harm after thousands of bank customers had their personal data stolen by a computer hacker.[38] A class action lawsuit soon followed where plaintiffs sought to obtain economic and emotional damages for the compromise of their personal data entrusted to the bank.[39] The plaintiff's specifically sought the remedy of reimbursement costs for credit monitoring since they were more susceptible to future identity theft and fraud as a result of the hack.[40] In their complaint, the plaintiffs did not allege they experienced any direct financial harm as a result of the exposure of their personal information, only that they were at greater risk of future harm due to the breach.[41] The *Pisciotta* court elected to follow precedent from its sister circuits that allowed the injury-in-fact requirement to be satisfied because there was a threat of future harm, however the specific cases cited

---

[36] *See id.* (describing how a legal injury will be moot if there is no longer an injury-in-fact).

[37] *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631 (7th Cir. 2007) (introducing a seminal Seventh Circuit case on "future harm" analysis). However, it should be noted the court's opinion concurred with sister circuits rather than asserting the new interpretation of the law on its own. *Id.*

[38] *See id.* (noting the extent to which the breach exposed the bank customer's personal information). Some of the information exposed during this breach included the account holder's "name, address, social security number, driver's license number, date of birth, mother's maiden name, and credit card or other financial account numbers." *Id.*

[39] *See id.* (addressing the remedy plaintiffs were pursuing and the theory under which they were seeking a cause of action).

[40] *See id.* at 639 (ruling that a remedy for credit monitoring services does not exist under Indiana law).

[41] *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (distinguishing the facts of the case from a normal injury-in-fact analysis that relies upon a harm already being experienced by the plaintiff at the time of the suit). "[They did not] claim that they or any other member of the putative class already had been the victim of identity theft as a result of the breach." *Id.*

were for toxic torts and environmental damage claims.[42] Meanwhile, the *Pisciotta* Court disregarded cases from other jurisdictions where the injury-in-fact requirement was tested against similar cases of personal data exposure.[43]

The Ninth Circuit maintained a similar viewpoint with respect to the increased threat of future harm theory of standing in *Krottner v. Starbucks Corporation*.[44] The plaintiffs in *Krottner* did not allege a theft actually occurred, but similar to *Pisciotta*, they wanted the corporation to be responsible for guarding them against future identity theft.[45] In its decision, *Krottner* specifically referenced the *Pisciotta* holding as a prime example of other circuits sustaining the increased threat of future harm argument to satisfy the injury-in-fact element and confer Article III standing.[46] The *Krottner* court ultimately ruled that the injury-in-fact requirement necessary to confer

[42] *See id.* at 638-39 (citing rationale of other circuit courts that determined toxic tort suits could proceed under an increased risk of future harm or future injury argument). There are clear differences between the potential harm to one's financial status or personal information following a data breach, and the future harm to one's long-term health following negligent handling of toxic substances that the court may have over-looked. *Id.*

[43] *See id.* at 639-40 (disagreeing with the many district courts across the United States that found a lack of federal jurisdiction for standing when plaintiff's data was compromised but not misused). The *Pisciotta* court at least acknowledged that its holding veers from many other federal district courts in its analysis in setting a new path for litigants in the Seventh Circuit. *Id.*

[44] *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) (reasoning by the Ninth Circuit that its rationale for allowing future harm to meet injury-in-fact is supported by similar cases). "Although we have not previously determined whether an increased risk of identity theft constitutes an injury-in-fact, we have addressed future harm in other contexts." *Id.*

[45] *See id.* (reviewing the facts asserted in the plaintiff's complaint regarding the harm experienced and steps taken to mitigate future harm). Two of the plaintiffs argued that they expended considerable time and vigilance in guarding against potential misuse of their personal information, but at the time of the suit had not experienced any actual identity theft. *Id.*

[46] *See id.* (acknowledging its alignment with the Seventh Circuit case's rationale regarding the expansion of the injury-in-fact requirement for data breaches).

> In *Pisciotta*, the plaintiffs' only alleged injury was the increased risk that their personal data would be misused in the future; none alleged any completed financial or other loss . . . [and] [h]ere plaintiffs alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data.

standing in the data breach context could be met by establishing a "credible threat of real and immediate harm" in the future.[47]

3. A Primer on Clapper

After the decision in *Krottner*, there were two clear precedential decisions in two different circuits that advanced the theory that plaintiffs could acquire standing following a data breach if the court was satisfied that the plaintiff was credibly at an increased risk of future harm.[48] The Court in *Clapper*, however, did not set out to resolve the circuit-split that existed in the Seventh and Ninth circuits.[49] *Clapper* was brought to the attention of the Supreme Court following Congressional enactment of the Foreign Intelligsence Surveillance Act (FISA) Amendments Act of 2008 ("FISA Amendment") to allow foreign intelligence surveillance monitoring of communications of non-US citizens abroad as long as the government first established probable cause that the target's communications were of foreign origin.[50]

Id. at 1142-43.

[47] *See* Krottner v. Starbucks Corp., 628 F.3d 1139 at 1143 (holding that the plaintiffs "sufficiently alleged an injury-in-fact for purposes of Article III standing"). The court provided the example that if the allegations were of a more hypothetical nature, such as if the laptop had not been stolen, but could be stolen someday, then there would be a less credible threat of future harm. *Id.*

[48] *See* Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 856 (2015) (recognizing the existence of a circuit-split prior to *Clapper* where the Seventh and Ninth Circuits accepted the increased risk of harm argument as sufficient to satisfy imminent injury under the injury-in-fact requirement).

[49] *See id.* (interpreting *Clapper* to provide guidance to the circuit courts on injury-in-fact standing analysis).

[50] *See Clapper II*, 133 S. Ct. 1138, 1144 (2013) (outlining the events that led to Supreme Court's review of the case); *see FISA Amendments Act of 2008*, THE WALL STREET J. (June 19, 2008), *archived at* https://perma.cc/48ZK-Z4L2 (providing an overview on the FISA Amendment and its impact on United States Government protocol with respect to foreign intelligence gathering). The FISA Amendment established clear roles for the U.S. Attorney General and the Director of National Intelligence to establish procedures for targeting foreign individuals reasonably believed to be situated outside United States territory. *Id.* The FISA Amendment also clarified that if conversations of American citizens are picked up over the course of foreign surveillance, that such information can only be used "for proper intelligence or law enforcement purposes." *Id.* One of the biggest shifts in the foreign intelligence policy was the requirement to have probable cause to target an American citizen both within the United States, but also when they are believed to

The plaintiffs in *Clapper* were civil liberties attorneys, nongovernmental organization employees, and international journalists who believed they were at increased the risk of unwarranted surveillance as a result of their regular communications with foreigners.[51] Despite the very obvious differences between a corporate data breach and foreign surveillance by the United States government, *Clapper* presents a workable roadmap to reign in the expanded Article III injury-in-fact interpretation.[52]

III. Premise

Clapper originated in federal district court but was quickly thrown out when the court granted a motion for summary judgment in favor of the government for lack of Article III standing.[53] The Second Circuit reversed, disagreeing with the district court, because they believed the plaintiffs satisfied the certainly impending requirement for standing by establishing an objectively reasonable likelihood that their communications would be intercepted at some time in the future.[54] The Supreme Court subsequently granted certiorari and its

be overseas. *Id.* *See also* David Smith, *Trump's Evidence-free Wiretap Claim Follows Rightwing Obama 'Coup' Stories*, THE GUARDIAN (Mar. 4, 2017), *archived at* https://perma.cc/ECY7-482Y (discussing the potential existence of a FISA warrant to monitor then-candidate Donald Trump's phone calls). The FISA Amendment gained renewed relevance with the news media reporting on the possible use of the FISA Court to obtain a warrant to investigate President Donald Trump's conversations with Russian nationals during the 2016 United States Presidential Election. *Id.*

[51] *See Clapper II*, 133 S. Ct. at 1144-45 (identifying the plaintiffs' constitutional argument against enactment of the FISA Amendment). The plaintiffs were attorneys, international non-governmental organizations and media organizations who regularly communicated with colleagues and clients abroad who may be subject to surveillance under the FISA Amendment, thereby subjecting American citizens to unnecessary government monitoring. *Id.*

[52] *See id.*at 1151 (explaining why parties cannot manufacture their own hypothetical future harm to satisfy Article III standing).

[53] *See Clapper I*, 638 F.3d at 121 (observing that the district court judge agreed with the government that the plaintiffs lacked standing in granting the summary judgment).

[54] *See id.* (reversing the district court's grant of summary judgment after accepting the plaintiff's future injury argument). "Because standing may be based on a reasonable fear of future injury and costs incurred to avoid that injury, and the plaintiffs have established that they have a reasonable fear of injury and have incurred costs to avoid it, we agree that they have standing." *Id.* at 122.

ruling serves as an update to the United States federal court system on Article III standing analysis.[55]

A. Clapper Under the Microscope

The plaintiffs in *Clapper* attempted to acquire standing with two different theories.[56] First, the plaintiffs claimed there was an objectively reasonable likelihood their communications would be acquired under the FISA Amendment at some point in the future that would cause them injury, which they argued satisfied the certainly impending requirement under Article III standing law.[57] Second, the plaintiffs claimed their risk of surveillance under the FISA Amendment is so substantial that they were forced to undertake costly and burdensome measures to protect the confidentiality of their international communications.[58] In the plaintiffs' view, this second theory constituted a present injury fairly traceable to the enactment of the FISA Amendment.[59]

[55] *See Clapper II*, 133 S. Ct. at 1146 (acknowledging its decision to review the circuit court's decision because of the lower court's "novel view of standing"). Justice Alito delivered the 5-4 majority opinion for the court, while Justice Breyer was joined by Justice's Ginsberg, Sotomayor, and Kagan in dissent. *Id.* at 1142, 1155.
[56] *See id.* at 1146 (addressing each argument advanced by the plaintiffs in attempt to satisfy the standing requirement in their challenge against the FISA Amendment).
[57] *See id.* at 1147 (outlining the first position taken by the plaintiffs that they met the "objectively reasonable likelihood" standard to acquire standing). The plaintiffs believed this to be the stronger argument and relied upon the Second Circuit's novel interpretation. *Id.* However, Justice Alito dismissed this argument right away. *Id.* "This argument fails… [T]he Second Circuit's 'objectively reasonable likelihood' standard is inconsistent with our requirement that 'threatened injury must be certainly impending to constitute injury in fact.'" *Id.* (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).
[58] *See id.* at 1150-51 (describing the costs and burdens associated with carrying out their duties as professionals following enactment of the FISA Amendment).
[59] *See* Bradford C. Mank, *Clapper v. Amnesty International: Two or Three Competing Philosophies of Standing Law?*, 81 TENN. L. REV. 211, 214 (2014) (reviewing the Court's refusal to accept future surveillance as sufficient to meet the plaintiffs' fairly traceable argument).

1. Certainly Impending

The *Clapper* Court considered it highly speculative that the United States government would "imminently target" communications of the plaintiffs following enactment of the FISA Amendment.[60] Despite the nearly five years that elapsed between enactment of the law and proceedings before the Supreme Court, the plaintiffs did not offer any evidence that their communications actually were monitored after the FISA Amendment became law.[61] The plaintiffs' likelihood of surveillance argument was ultimately based on a series of assumptions, rather than grounded in fact.[62] There was no objective evidence presented to the Court that supported the assertion that the plaintiffs' personal communications were likely to be intercepted.[63]

The purpose of the certainly impending requirement under Article III standing law is to ensure the eventuality of the harm is not stretched beyond the original conduct for injuries not likely to occur.[64] The Court clarified that possible future injury predicated on a series of events speculative in nature would fail.[65] According to the Court, the plaintiffs in *Clapper* relied on a "highly attenuated chain of

[60] *See Clapper II*, 133 S. Ct. at 1143, 1148 (noting the subjectivity and conjecture involved in arguing that the plaintiffs would be targeted).
[61] *See* Kristen Choi, *Clapper v. Amnesty International USA: Balancing National Security and Individuals' Privacy*, 34 J. NAT'L ASS'N ADMIN. L. JUD. 444, 470-71 (2014) (discussing the missing links in the chain between enactment of the legislation and monitoring of the plaintiffs as argued). The plaintiffs lacked any factual evidence that they would be targeted by the government, which severely undermined their legal position. *Id.* at 470.
[62] *See Clapper II*, 133 S. Ct. at 1149 (analyzing the theory advocated by the plaintiffs that their communications would be intercepted).
[63] *See id.* (reviewing the lack of evidence supporting the plaintiffs' argument that the future harm would be carried out against them); *see also* Choi, *supra* note 61, at 473 (acknowledging the relative weakness of the plaintiffs' argument). "[I]t was mere speculation as to whether the government would subject Respondents' communications to electronic surveillance using the FISA Amendments Act." *Id.*
[64] *See Clapper II*, 133 S. Ct. at 1147 (highlighting the importance of the narrow "certainly impending" requirement in order to find standing for a plaintiff). The Court reiterated in *Clapper* the distinction between threatened injury and an allegation of possible future injury. *Id.*
[65] *See id.* at 1148 (dismissing the hypothetical nature of the possible future injury argument). "[R]espondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending." *Id.*

possibilities" to establish the threatened injury and deemed the circumstances insufficient to be considered certainly impending.[66]

2. Present Injury

The second argument advanced by the plaintiffs was that the threat of surveillance compelled them to avoid communication methods that increased the likelihood of interception by the government.[67] As a result of these precautionary measures, the plaintiffs spent more money on travel costs to communicate with their overseas clients and sources in-person.[68] The Second Circuit in its earlier reversal believed that these economic and professional harms resulted in present injury-in-fact, stemming from the plaintiffs' reasonable fear of harmful government conduct likely to occur in the future.[69] However, the

[66] *See id.* (observing the amount of assumptions required by plaintiff's future injury argument). Plaintiffs' argument presupposes the following:

> [The] respondents' 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.

Id.

[67] *See* Choi, *supra* note 61, at 471 (outlining the theory of present injury suffered by the plaintiffs and presented before the Court to acquire standing). Justice Alito feared the Court's acceptance of the argument on fairly traceable grounds advanced by the plaintiffs would have a dilutive impact on the Article III standing threshold. *Id.*

[68] *See* Choi, *supra* note 61, at 465-66 (discussing the difficulty of maintaining professional relationships with counterparts overseas that may be under FISA surveillance).

[69] *See Clapper II*, 133 S. Ct. at 1151 (2013) (criticizing the Second Circuit's improper analysis of present injury in their prior reversal). "The Second Circuit's analysis improperly allowed respondents to establish standing by asserting that they suffer present costs and burdens that are based on a fear of surveillance…" *Id.*

Supreme Court held this view severely watered-down the "fundamental requirements of Article III", because it allowed the plaintiffs to establish injury for suffering present costs as long as they were based upon non-paranoid fears.[70]

Since the future harm was hypothetical, and not certainly impending, the Court held the plaintiffs could not manufacture standing though their financial outlay on secure communication devices and travel expenses.[71] The chain of traceability was disrupted between the FISA Amendment and the self-inflicted injuries because the United States government did not actually conduct any surveillance upon the plaintiffs.[72] The Court posited that adhering to the Second Circuit's decision might open the door for plaintiffs to secure a lower threshold for Article III standing by making expenditures that are based on any reasonable, non-paranoid fear.[73] The Court also noted that prior to enactment of the FISA Amendment, the plaintiffs already had an incentive to take precautions in protecting sensitive overseas communications with foreign counterparts.[74] The Court ultimately ruled that although the self-inflicted injuries were incurred to avoid government surveillance, a subjective fear of surveillance is insufficient to give rise to Article III standing.[75]

---

[70] *See id.* (concluding that acceptance of the plaintiff's theory on present injury weakens the constitutional protections of Article III standing). The Court also noted the harm still was not certainly impending to justify a finding of present injury, even if the expenditures were reasonable under the circumstances. *Id.*

[71] *See Clapper II*, 133 S. Ct. at 1151 (2013) (articulating the fear that plaintiffs could self-injure to gain standing against a defendant where they otherwise would not have been harmed). Justice Alito further noted that the manufactured present injury argument amounted to a repackaged version of the "certainly impending" argument. *Id.* This is because the Court's determination of whether the plaintiffs' expenditure was based upon a non-paranoid fear would involve the same analysis of whether the injury was certainly impending. *Id.* at 1152-53.

[72] *See id.* at 1152 (demonstrating the lack of causal relationship between the FISA Amendment and the activities undertaken by the plaintiffs to avoid detection by the government).

[73] *See* Choi, *supra* note 61, at 471 (noting Alito's fear that accepting hypothetical arguments of future harm would lower the constitutional standard for Article III standing).

[74] *See Clapper II*, 133 S. Ct. at 1152 (opining that safety precautions to protect the confidentiality of overseas communications are good practice, however the pure fear of being surveyed does not result in automatic standing).

[75] *See id.* at 1151-53 (holding the inapplicability of the expenses incurred out of fear satisfying the strict requirements for standing). The Court provided significant clarity to the standing analysis that took into account technological advances in

B. Reaction to Clapper

1. Ninth Circuit Holding Steady

Despite the detailed analysis offered up by the Supreme Court in the *Clapper* decision regarding Article III standing, the Ninth Circuit continues to rely upon its precedent set in *Krottner* for data breach standing cases.[76] In one Ninth Circuit case, the defendant, Adobe Systems, advocated that *Clapper* served as authority to extinguish the Ninth Circuit's approach to standing in *Krottner*.[77] However, the Ninth Circuit declined to overrule *Krottner*, because the end-result would have been to eliminate its own increased threat of future harm standard.[78] The *Adobe* court disagreed that the Supreme Court intended the *Clapper* decision to have a far-reaching impact on existing standing law and insisted that *Clapper* should only considered within its specific context.[79] The *Adobe* court also distinguished the likelihood (or lack thereof) of harm occurring in *Clapper*, from the immediate risk of actual harm related to stolen personal information.[80]

---

communications, surveillance, and personal data that corresponded with the data breach context. *Id.*

[76] *See* In re Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (2014) (holding that *Clapper* does not overrule *Krottner*); *see also* In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 961 (2014) (rejecting the notion that *Clapper* sets forth a new Article III framework); In re Zappos.com, Inc., 108 F. Supp. 3d 949, 957 (2015) (agreeing that *Clapper* does not overrule *Krottner*).

[77] *See Adobe*, 66 F. Supp. 3d at 1212 (arguing that data breach cases regularly conclude that increased risk of future harm is insufficient to confer Article III standing under the "certainly impending" standard).

[78] *See id.* at 1214 (holding that both *Krottner* and *Clapper* may coexist together in the Ninth Circuit). "The Court does not find that *Krottner* and *Clapper* are clearly irreconcilable." *Id.*

[79] *See id.* (questioning Adobe's argument that *Clapper* intended to overrule *Krottner* and apply to data breach cases generally). "In the absence of any indication in *Clapper* that the Supreme Court intended a wide-reaching revision to existing standing doctrine, the Court is reluctant to conclude that *Clapper* represents the sea change that Adobe suggests." *Id.* The *Adobe* court also noted that since *Clapper* involved the review of a government body potentially violating the Constitution, it merited a more rigorous standing analysis than a data breach class-action. *Id.*

[80] *See Adobe*, 66 F. Supp. 3d at 1214-15 (identifying some of the information that was stolen from the plaintiffs). "Hackers deliberately targeted Adobe's servers and

The Ninth Circuit reinforced its position that *Clapper* does not overrule *Krottner* in another data breach case, *In re Zappos.com, Inc.*[81] However, the *Zappos* court achieved a different outcome than *Adobe* despite applying existing Ninth Circuit precedent.[82] The *Zappos* court interpreted the requirement in *Krottner* that the credible threat of harm be real and immediate, as equivalent to the firm certainly impending requirement under *Clapper*.[83] The *Zappos* court advanced a theory previously overlooked in Ninth Circuit cases where it evaluated the relationship between the plaintiff, the defendant, the anticipated harm, and the action necessary by independent third parties to bring about that harm.[84] In *Zappos*, hackers stole the personal information of 24 million people, yet only twelve individuals were part of the class-action against Zappos, and only three of the twelve were concerned enough about the increased threat of identity theft and fraud to self-fund credit monitoring services.[85] Two and a half years passed between the hack against Zappos and the Ninth Circuit decision, and the court considered the lack of any actual injury against the

spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses and credit card numbers and expiration dates." *Id.* at 1215.

[81] *See Zappos*, 108 F. Supp. 3d at 955-56 (introducing *Adobe,* another post-*Clapper* Ninth Circuit case and explaining its holding). This Court agrees that *Clapper* does not necessarily overrule *Krottner*. *Id.* at 957. However, the *Zappos* court specifically mentioned the Ninth Circuit's decisions in *Sony* and *Adobe* while diverging from their analysis. *Id.* at 955-56.

[82] *See id.* at 957 (distinguishing the result in *Adobe* versus *Zappos*). "However, just because *Krottner* is controlling does not consequently mean that its outcome dictates the Court's conclusion as to standing here…." *Id.*

[83] *See id.* (emphasizing that the same immediacy of harm requirement applies in both *Krottner* and *Clapper*).

[84] *See See Zappos*, 108 F. Supp. 3d at 957-58 (indicating a distinction applies when a third party needs to carry out some action to cause the harm). The Court argued that when an independent third party needs to take specific action that would culminate in harm to the plaintiff, the alleged injury is less likely to confer standing. *Id.*

[85] *See id.* at 958 (discussing the plaintiffs' lack of actual identity theft or fraud taking place over the period of time passed since the data breach). "Plaintiffs still claim that the threat they face is immediate, though there is no indication when or if that threat will materialize." *Id.* Without any actual injury experienced by the plaintiffs, the court can only speculate as to possible future injuries. *Id.*

plaintiffs during that time period to be persuasive.[86] The court reasoned there must be a point in time at which a future threat can no longer be considered certainly impending or immediate, despite the feasibility it may occur.[87] In the absence of an allegation of actual theft or fraud from any of the plaintiffs, the *Zappos* court ruled that the risk of harm was not immediate and therefore not certainly impending.[88]

2. Other Circuits Falling into Line

In *Peters v. St. Joseph Servs. Corp.*,[89] the Fifth Circuit thoroughly rejected pre-*Clapper* theories regarding the threat of future harm and used *Clapper* as the basis for standing analysis in the data breach context.[90] The *Peters* court believed the plaintiff's allegations of future injury to be conjectural, speculative and hypothetical.[91] Bringing *Clapper* into the analysis, the *Peters* court compared the plaintiff's theory of standing to that of *Clapper* in that both relied upon a "highly attenuated chain of possibilities" for the harm to occur.[92] Summarily, the court agreed that *Clapper* (arguably) resolved any existing circuit splits on the matter of standing for data breach class actions.[93]

---

[86] *See* Corey Varma, *The Presumption of Injury: Giving Data Breach Victims "A Leg To Stand On*", 32 J. MARSHALL J. INFO. TECH. & PRIV. L. 301, 305 (2016) (noting that not a single plaintiff experienced actual identity theft or fraud following the Zappos data breach).

[87] *See Zappos*, 108 F. Supp. 3d at 958 (contending that a line must be drawn where the threat is no longer immediate or certainly impending for standing litigation).

[88] *See id.* at 959 (reaffirming the Court's finding that the harm posed to the plaintiffs was not certainly impending under both *Krottner* and *Clapper* precedents).

[89] 74 F. Supp. 3d 847, 855 (2015) (explaining how the present case follows the precedent set by *Clapper* despite the circuit split).

[90] *See id.* at 853-54 (applying *Clapper's* legal rules and standing definitions to the case at hand).

[91] *See id.* at 854 (exposing the uncertainty regarding whether the harm was likely to occur, if ever). "The risk of future harm is, no doubt, indefinite. It may even be impossible to determine whether the misused information was obtained from exposure caused by the Data Breach or from some other source." *Id.*

[92] *See id.* (asserting that class-action cases analyzed for Article III standing require an actual or imminent injury). The court was mindful to prevent an indefinite risk of future harm interpretation from taking hold in the Fifth Circuit. *Id.*

[93] *See* Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d at 854 (holding that identity theft fraud is insufficient because it fails to satisfy the requirement of certainly impending to constitute and injury in fact, as outlined in *Clapper*). The federal claims

The Second and Third Circuits soon followed suit.[94] In a Second Circuit case, the plaintiff argued they were damaged monetarily with credit monitoring expenses and the loss of time spent mitigating the exposure of their personal information.[95] However, the Second Circuit applied the *Clapper* ruling to dismiss this argument, asserting that the plaintiffs cannot manufacture standing by proactively purchasing credit monitoring services, even if the expenditure is made based on a reasonable, non-paranoid fear.[96] The *Whalen* court held the plaintiff could not satisfy the certainly impending injury requirement without actual, direct injury, even though they faced an increased threat of identity theft and the prospect of future fraudulent charges incurred on their account.[97]

Meanwhile, in *In re Horizon Healthcare Servs. Data Breach Litig.*, the Third Circuit looked to *Clapper* as authority and held the plaintiffs' alleged injury too speculative for Article III purposes.[98] The *Horizon* court reiterated that threatened injury must be certainly impending to constitute injury-in-fact, and that allegations of possible future injury were insufficient to confer standing.[99] None of the plaintiffs suffered any monetary loss or any other injuries such as identity theft, identity fraud, medical fraud, or phishing following the

advanced by the plaintiffs were dismissed to the extent they were based on an assertion that they are subject to identity theft in the future. *Id.*

[94] *See* Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581 (2015) (rejecting one of the plaintiff's arguments due to its incompatibility with *Clapper's* precedent); *see also* In re Horizon Healthcare Servs. Data Breach Litig., No. 13-7418, 2015 U.S. Dist. LEXIS 41839, at *1, *7 (D.N.J. Mar. 31, 2015) (introducing *Clapper's* "certainly impending" analysis to the asserted injury).

[95] *See Whalen*, 153 F. Supp. 3d at 581 (highlighting the financial and other costs experienced by the plaintiff following the data breach).

[96] *See id.* at 582-83 (prohibiting a plaintiff from recovering when the damages are self-inflicted and their changed position is not justified by the evidence). The court particularly notes that the affected credit card was cancelled after the breach so there was no basis for actual injury unless manufactured by the plaintiff. *Id.*

[97] *See id.* at 583 (affirming *Clapper* analysis applies to Second Circuit data breach cases). "Simply put, Whalen has not asserted any injuries that are 'certainly impending' or based on a 'substantial risk that the harm will occur." *Id.* (quoting *Clapper II*, 133 S. Ct. 1138, 1147 (2013).

[98] *See Horizon*, 2015 U.S. Dist. LEXIS 41839, at *7 (invoking *Clapper* as the judicial authority for standing in the Third Circuit).

[99] *See id.* (reaffirming the notion that possible future injuries are not sufficient for standing purposes).

data breach.[100] Therefore, the plaintiffs could not distinguish their actual injuries from hypothetical injuries and the future injuries alleged could only stem from the hypothetical conduct of a third party.[101]

IV. Analysis

The instances of large-scale hacking of corporate enterprises by malicious actors are not going to miraculously decline as consumers continue to adopt Internet technologies that collect their personal information.[102] Accordingly, the courts will continue to play a vital role in mediating disputes between consumers and corporations to determine the appropriate threshold of injury where a consumer may constitutionally pursue a remedy in court.[103] The *Clapper* Court arguably provided the certainty that businesses and lower courts were looking-for when analyzing standing in the corporate data breach context.[104] The basic tenet of the *Clapper* decision is the rejection of suits that are based on speculative and hypothetical theories of harm because they are not certainly impending.[105] Moreover, *Clapper* clar-

[100] *See id.* at *12 (listing the possible harms that could convey standing upon the plaintiff). The plaintiff did not experience any of these specific harms as a result of the stolen laptops and therefore could not obtain standing. *Id.* at *13.

[101] *See id.* at *17 (holding that the theories advanced by the plaintiff are inadequate to acquire Article III standing). "Plaintiffs' future injuries stem from the conjectural conduct of a third party bandit and are therefore inadequate to confer standing." *Id.*

[102] *See* Segrist, *supra* note 1, at 530-31 (noting the massive amounts of personal data collected by corporations and prevalence of consumers to adopt potentially harmful new technologies); *see also* Rustad, *supra* note 4, at 39 (demonstrating growth of internet adoption and continued expected expansion of internet-connected devices); *see also* Fuscaldo, *supra* note 3 (highlighting the vulnerabilities of consumers on the Internet).

[103] *See* Raines v. Byrd, 521 U.S. 811, 820 (1997) (observing the important role courts play in determining constitutional threshold issues for Article III standing law).

[104] *See Clapper II*, 133 S. Ct. 1138, 1146 (2013) (discussing the Court's rationale for weighing-in on the standing interpretation for the plaintiffs protesting the FISA Amendment).

[105] *See id.* at 1143-46 (summarizing the important findings of *Clapper* as it relates Article III standing law); *see also* Mank, *supra* note 59, at 274 (analyzing the "*Clapper* decision's strict interpretation of the 'certainly impending' standing injury test"). Mank's conclusion is very interested in understanding whether the *Clapper*

ifies that consumers cannot manufacture the present injury requirement to acquire standing.[106] While all circuits except the Ninth Circuit agree that *Clapper* resolved the split for standing analysis in the data breach context, the *Zappos* decision opens the door for possible unification of the Ninth Circuit with the *Clapper* ruling.[107]

A. Class Action Lawsuits Based on Speculation and Conjecture

Much to the dismay of corporate defendants, consumers continue to bring lawsuits based on hypothetical and speculative future harm not yet realized.[108] The constitutional basis for standing is being stretched by consumers putting forth a sequence of improbable events to satisfy the certainly impending element.[109] In the specific data breach context, consumers are attempting to transform a corporation's compliance with public notification requirements into sufficient evidence that the corporation is at fault for breach of its duty to protect personal information.[110] But there is a significant gap between a corporation experiencing a data breach, and a consumer's

---

decision will have a far-reaching impact on standing law or if this strict interpretation would only be applied to a limited set of cases involving foreign intelligence collection. *Id.*

[106] *See Clapper II*, 133 S. Ct. at 1151 (2013) (criticizing plaintiff's argument that their expenditures could be justified to satisfy the present injury requirement).

[107] *See* Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 856 (2015) (rejecting the plaintiff's argument on the grounds of *Clapper*); *see also* Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581-82 (2015) (dismissing the plaintiff's complaint because it cannot survive *Clapper* analysis); In re Zappos.com, Inc., 108 F. Supp. 3d 949, 957 (2015) (equating the *Krottner* holding to the *Clapper* holding); *but see* In re Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (2014) (determining that *Clapper's* firm analysis on certainly impending and present injury do not apply in the Ninth Circuit's analysis of standing).

[108] *See Zappos*, 108 F. Supp. 3d at 958 (observing that after two and a half years since the data breach, not one plaintiff had actually experienced fraud or identity theft that resulted in financial harm).

[109] *See Peters*, 74 F. Supp. 3d at 857 (reviewing the loose chain of assumptions drawn by the plaintiffs to advance their argument that harm was certainly impending).

[110] *See Zappos*, 108 F. Supp. 3d at 958 (surmising that several consumers notified of the breach brought suit against the corporation following disclosure but did not experience any identity theft or fraud in over two years since the breach); *see also* In re Horizon Healthcare Servs. Data Breach Litig., No. 13-7418, 2015 U.S. Dist. LEXIS 41839, at *8-*9 (D.N.J. Mar. 31, 2015) (viewing that the plaintiffs did not

personal information ending up in the hands of a malicious actor who can actually use that information to steal their identity or commit fraud.

Meanwhile, corporations are otherwise forced to expend considerable resources defending these speculative suits unless they are successful in getting the case dismissed with a motion for summary judgment for lack of Article III standing.[111] There are already unprecedented costs corporations must contend with by insuring their operations in the event of a breach, securing their data to prevent a breach from ever occurring, and complying with extensive United States and international privacy regulations.[112] The *Clapper* decision serves to limit this corporate exposure by rejecting standing for plaintiffs who only advance an allegation of possible future injury.[113] Application of the *Clapper* decision to Article III standing in the data breach context in all federal circuits provides greater certainty to businesses participating in the digital economy and consumers who will know in advance the likelihood their case will proceed to trial.[114]

B. Unfair Manufacture of Injury

When consumers are unsuccessful in advocating the threat of future harm theory, there are instances where they attempt to manufacture present injury through purchasing credit monitoring services

---

experience any monetary loss as a result of the data breach but brought the class action suit against the corporation). Like in contract law where breach of a condition of the contract does not necessarily result in a cause of action that will result in damages for the non-breaching party, in the data breach context, consumers should have to prove their damages at the pleading stage for them to be able to move forward in litigation against the corporation. *Id.*

[111] *See* Ritchie, *supra* note 9, at 13-14 (analyzing the speed with which lawsuits are being brought by plaintiffs after a data breach is announced in the news). The data breaches are of such a grand scale affecting millions of people in one hack that class action suits will inevitably follow. *Id.*

[112] *See* Ritchie, *supra* note 9, at 13-14 (noting the immense litigation exposure corporations have when they experience a data breach and consumer information gets exposed); *see also* Segrist, *supra* note 1, at 530-31 (outlining some of the risks of conducting business online that corporations must be aware of). Consumer protections for personal information are lagging behind private industry and the government's massive data collection schemes. *Id*.

[113] *See Clapper II*, 133 S. Ct. 1138, 1151 (2013) (rejecting the credible threat of future harm argument put forward by the plaintiffs to defeat the FISA Amendment).

[114] *See id.* (settling certainly impending standing analysis from a constitutional perspective).

and other protective measures.[115] Consumers argue that this financial outlay should satisfy the standing requirement because the expenditure is aimed at preventing the exacerbation of a data breach.[116] Prior to *Clapper*, some circuit courts allowed consumers to acquire standing in such a fabricated manner, much to the dismay of private enterprise, as long as the purchase of credit monitoring was based on a "non-paranoid fear."[117] This method of acquiring standing essentially acts as a rubber-stamp for a plaintiff-led lawsuit following a data breach if there is some rational explanation for the expenditure.[118]

The ruling in *Clapper* should serve to reign-in the degradation of the constitutional threshold for standing, and prevent the courts from becoming overburdened by hearing cases and controversies without merit.[119] Article III standing acts as an early filter to prevent suits by consumers where they have not actually experienced any harm from the exposure of their personal information.[120] Consumer advocates may argue the threshold should be lower because of the perceived negligence and failure of the corporation to protect the consumer's personal information.[121] However, the framers of the United States Constitution never intended for plaintiffs to take advantage of

[115] *See* Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581 (2015) (highlighting that the plaintiff did not put forward any reasonable argument that they were at threat of harm that would justify expenditure on personal credit monitoring services). In addition, the *Whalen* court infers that the Supreme Court dismissed the costs for credit monitoring argument entirely when utilized to "manufacture standing." *Id.*

[116] *See Clapper II*, 133 S. Ct., at 1145-46 (providing examples of plaintiff's perceivably manufactured standing through purchasing expensive air travel and encrypted messaging to prevent eavesdropping under the FISA Amendment).

[117] *See id.* at 1151 (recognizing prior to *Clapper* that consumer expenditures based on non-paranoid fears could be deemed acceptable and sufficient to meet present injury).

[118] *See id.* at 1147 (determining that the threatened injury must be "certainly impending" to sufficiently create standing).

[119] *See id.* (contending that imminence, while elastic, "cannot be stretched beyond its purpose . . ." outlined by Article III).

[120] *See id.* (explaining the elements of standing which must be met under Article III).

[121] *See id.* at 1150 (recognizing the Court's reluctance to base standing on speculation, resulting in less consumer-friendly standing interpretations).

loopholes that would allow them to manufacture jurisdiction in federal courts.[122]

C. Resolution of the Circuit Split

One of the greatest powers the Supreme Court maintains is the power to override any splits among the circuit courts that develop in different federal jurisdictions.[123] Particularly in the technological revolution, the Court is in a position to rule on novel issues of law in dire need of uniformity.[124] The corporate data breach context is a particularly ripe cross-section of law and technology, making the case even stronger for the application of the *Clapper* in the Ninth Circuit.[125] However, the Ninth Circuit continues to allow plaintiffs the right to acquire standing based on credible threats of future harm that are loosely tied together.[126] There is an argument that these actions are indicative of the judicial system as it is supposed-to when the Supreme Court neglects to intervene.[127] Consumer advocates will certainly argue that the Supreme Court is too slow to react to technological advances and the circuit courts are best suited to rule on such emerging issues of law.[128]

Nonetheless, the Ninth Circuit indicated it might be willing to self-correct as more cases are heard in its jurisdiction following the

---

[122] *See Clapper II*, 133 S. Ct., at 1151 (explaining how jurisdiction could be manufactured in the federal court system).
[123] *See* Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 856 (2015) (reasoning that the Supreme Court asserted its authority to resolve the prior circuit split in *Clapper*).
[124] *See* Raines v. Byrd, 521 U.S. 811, 820 (1997) (highlighting the imminent importance of the Supreme Court in evaluating constitutionality of issues before them).
[125] *See* In re Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1213 (2014) (setting precedent for Ninth Circuit to reject *Clapper* and continue to hold *Krottner* as good law for data breach standing analysis).
[126] *See id.* at 1213-14 (contending that the Ninth Circuit does not need to follow *Clapper* as it relates to constitutional standing); *see also* In re Zappos.com, Inc., 108 F. Supp. 3d 949, 957 (2015) (denying the defendant's argument that the *Clapper* decision overrules *Krottner* in the Ninth Circuit).
[127] *See Adobe*, 66 F. Supp. 3d at 1214 (discrediting the Supreme Court's analysis in *Clapper* because it involved review of a government body as a defendant rather than a corporation).
[128] *See id.* (explaining how the circuit courts are quicker to adapt to technological advances than the Supreme Court).

Clapper decision.[129] The *Zappos* court's analysis of the amount of time elapsed between the data breach and the lawsuit, as well as the lack of harm experienced by the plaintiff, are ideologically synchronized with the *Clapper* doctrine.[130] As long as the Ninth Circuit cases achieve the same outcomes as the other circuits, it may not matter if they hold *Krottner* or *Clapper* as the defining precedent.[131]

D. Supreme Court Resolution (Again)

The Ninth Circuit's reluctance to fully adopt the *Clapper* decision like its sister circuits inevitably sets the stage for the Supreme Court to evaluate constitutional Article III standing once again.[132] To settle the split among the circuits and ensure data breach standing requirements are uniform across the federal courts of the United States, the Supreme Court should specifically interpret a standing case for a corporate data breach.[133] The technology industry is one of the greatest growth engines in the American economy and businesses deserve greater certainty regarding their liability in data breach cases.[134] Litigation planning is an important part of corporate risk management

[129] *See Zappos*, 108 F. Supp. 3d at 957 (2015) (holding that even though *Krottner* remains good law, it applies the same legal rules of analysis to constitutional standing as *Clapper*).
[130] *See id.* (noting that the certainly impending requirement is the same under both *Clapper* and *Krottner*).
[131] *See Adobe*, 66 F. Supp. 3d at 1214 (arguing that the *Krottner* and *Clapper* precedents may coexist in the Ninth Circuit as long as the correct outcome is achieved).
[132] *See Zappos*, 108 F. Supp. 3d at 956-57 (distinguishing the Ninth Circuit precedent applicable to standing cases from the recent *Clapper* decision).
[133] *See Adobe*, 66 F. Supp. 3d at 1214 (arguing that the Supreme Court did not explicitly intend to overrule *Krottner*); *contra* Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 856 (2015) (recognizing that *Clapper* resolved any split among the circuits on Article III standing); *see also* Mank, *supra* note 59, at 274 (surmising that the *Clapper* decision may increase uncertainty in the courts because of its narrow interpretation in the foreign surveillance context). Mank argued the lower courts may have trouble applying the *Clapper* ruling more broadly on 'certainly impending' standing injury because of its unique fact pattern, and questioned its potential influence on Article III standing precedent. *Id.* at 275. This potential confusion for lower courts, already experienced in several Ninth Circuit holdings, increases the necessity to revisit Article III standing at the Supreme Court. *Id.*
[134] *See* Riedy & Hanus, *supra* note 7, at 5-6 (advancing the position that the benefits of technology also bring harms that must be acknowledged by consumers when they allow their personal information to be harvested).

and the constitutional threshold for clients acquiring standing following a data breach should be clearly determined by the courts to only occur when the business is at fault for the direct injuries of identity theft or fraud.[135]

V. Conclusion

With consumers willing to run the risk of exposing their personal information on the Internet, where corporate actors provide convenience and entertainment in exchange for a loss of consumer privacy, a greater degree of guidance is needed from the Supreme Court. Like any legal rule established by the Supreme Court, there will be specific outcomes for plaintiffs that appear unjust, but *Clapper's* Article III standing interpretation strikes the necessary constitutional balance between consumer and corporate fairness. The costs of doing business and risk allocation must be predictable for private enterprise to be able to thrive in the Internet ecosystem and maintain a competitive edge for United States businesses. The Ninth Circuit ultimately needs to ditch its reputation as a rogue circuit in favor of a bright line rule established by the Supreme Court that is fair to businesses and consumers alike. The Supreme Court would be wise to hand down another Article III standing decision, this time in the data breach context, to specifically overrule the stubborn Ninth Circuit's refusal to accept *Clapper* and settle the injury-in-fact threshold for all future plaintiffs.

[135] *See* Ritchie, *supra* note 9, at 14-15 (commenting on the tremendous scale of consumer class actions on Article III standing and difficulty corporations have dealing with them).