UIC
REVIEW OF INTELLECTUAL PROPERTY LAW

MALICIOUS V. NEGLIGENT LOSS OF DATA: THE SECOND CIRCUIT'S QUESTIONABLE TEST TO DETERMINE DATA BREACH STANDING

LUKASZ KORNAS

ORCID: 0000-0003-4725-3841

ABSTRACT

Data breaches are a modern reality. Plaintiffs sue in the aftermath of a data breach to get compensation from the party that failed to secure their data. However, plaintiffs often have trouble satisfying the standing requirement because federal courts rigidly interpret Supreme Court standing precedent. The Second Circuit's decision in *McMorris v. Carlos Lopez & Associates, LLC* clarified the standing requirement in the data breach context. However, the test leaves many plaintiffs without legal recourse. It generally only permits plaintiffs to proceed past the pleading stage when the data was stolen as part of a malicious attack or misused prior to the suit. The issue is that most data breaches are the result of negligence. This note explores the limitations of the Second Circuit's test, and it proposes some modifications that better account for modern realities. It also analyzes developments in Supreme Court standing jurisprudence, and how those developments are a welcome sign for future plaintiffs in the data breach context.

Cite as Lukasz Kornas, *Malicious v. Negligent Loss of Data: The Second Circuit's Questionable Test to Determine Data Breach Standing*, 21 UIC REV. INTELL. PROP. L. 271 (2022).

MALICIOUS V. NEGLIGENT LOSS OF DATA: THE SECOND CIRCUIT'S QUESTIONABLE TEST TO DETERMINE DATA BREACH STANDING

LUKASZ KORNAS

MALICIOUS V. NEGLIGENT LOSS OF DATA: THE SECOND CIRCUIT'S QUESTIONABLE TEST TO DETERMINE DATA BREACH STANDING.

LUKASZ KORNAS*

I. INTRODUCTION

Data digitalization is a key priority of companies looking to stay competitive in a digital economy.[1] As a result, the digital economy continues to expand at record speeds as technology advances.[2] The digital economy can be defined as "economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes."[3] Digitalization does not only refer to e-commerce,[4] but also offers "diverse digital solutions available for nearly all business functions."[5] The COVID-19 pandemic served as a major catalyst for a "surge in the use of digital technologies due to the social distancing norms and nationwide lockdowns."[6] With the start of economic recovery in 2021, many companies continue to digitalize with hopes that digitalization will provide the best returns.[7] While there are advantages to digitalization, there are also risks; one of the greatest risks being a lack of data security.

Companies are increasingly using digital means to store confidential data, which exposes their data to a greater risk of being unintentionally circulated. The pandemic

---

* © 2022 Lukasz M. Kornas, Juris Doctor Candidate, May 2023, UIC School of Law School; B.A. in Psychology, University of Illinois Chicago (2019). I want to thank my family, my editor, Jennifer Armstrong, and the rest of the RIPL staff for their guidance and support. This achievement would not have been possible without them.

[1] Rex Ahlstrom, *The Role Of Data In The Age Of Digital Transformation*, FORBES (Jan. 17, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/01/17/the-role-of-data-in-the-age-of-digital-transformation/?sh=766259124509 (because of market trends regarding digitalization, "global spending on digital transformation technologies and services was expected to increase by nearly 20% in 2018 to more than $1.1 trillion").

[2] Kosha Gada, *The Digital Economy In 5 Minutes*, FORBES (June 16, 2016), https://www.forbes.com/sites/koshagada/2016/06/16/what-is-the-digital-economy/?sh=23a712197628. Half of the population is online because of rapid development of technology. *Id.* As a result, "[a] young, dynamic, $3 trillion ecosystem based on technological infrastructure, increasingly intuitive devices and interfaces, vast audience networks, a whole new medium for advertising and an unlimited supply of content" is available to users. *Id.*

[3] Heidi Booth, *What is the digital economy?*, DIGITAL PRESENCE (July 23, 2021), https://www.hubspace.ca/what-is-the-digital-economy. "UNCTAD found that companies, on average, reacted to a range of pandemic related factors 20 to 25 time faster than expected. When asked about their transition to working remotely, the response rate was 40 times faster than prior to the COVID19 crisis." *Id.*

[4] *Id.*

[5] *Id.*

[6] Rahul De, Neena Pandey, & Abhipsa Pal, *Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice*, 55 INT. J. INF. MANAGE. 1, 1-2 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7280123.

[7] Kumar Ritesh, *Digital Risks In 2021*, FORBES (Feb. 18, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/02/18/digital-risks-in-2021. Many employees have started to work remotely, and companies have begun to utilize "cloud services and communication tools hastily" to adopt to the pandemic. As a result, companies are at great risk of data breaches. Likewise, human errors and insider attacks are also expected to heighten." *Id.*

has taught employers that the biggest threat to ensuring data security is employee negligence.[8] Additionally, companies are not adequately prepared for the ongoing shift towards digitalization.[9] Companies have few security measures regarding access to their sensitive files.[10] Any employee who has access to data may inadvertently leak that data. Because data is a valuable asset, the consequences of its leak can be catastrophic.[11]

Data breaches occur "when information is accessed, taken, or used by a person without authorization."[12] Breaches occur for a variety of reasons, but the most common are criminal activity, employee accidents or negligence, computer failures, or system failures, and once the data is leaked, it is difficult to minimize the damage.[13] Data breach cases usually result in class action lawsuits in which the plaintiffs allege the defendants were negligent in developing and maintaining their security measures.[14] However, as it currently stands under Article III jurisprudence, many litigants will have trouble satisfying the injury-in-fact requirement unless they fall victim to identity theft or their data is otherwise misused.[15] The issue is that victims of a data breach will naturally seek to protect their information even if the breach was accidental because someone who received that information, either accidentally or intentionally, may still abuse it.[16]

---

[8] Carmen Reinicke, *The biggest cybersecurity risk to US businesses is employee negligence, study says*, CNBC (June 21, 2018), https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html:

> Cybersecurity practices have not yet caught up. A majority of executives agree that the risk of a data breach is higher when an employee works remotely, yet few businesses have comprehensive off-site policies in place for those workers. Over half of small business owners said they have no policy for remote workers.

[9] Varonis, *2019 VARONIS GLOBAL DATA RISK REPORT*, 12 (2019), https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf?_hstc=45788219.ea1c243f9c6ced0c6a2e66bee594c072.1632484843394.1632484843394.1632484843394.1&__hssc=45788219.1.1632484843395&__hsfp=1637000307&hsLang=en (analyzing 785 organizations, and finding "22% of all folders in a company were open to every employee . . . 53% of companies found over 1,000 sensitive files open to every employee . . . [and] 15% of companies found more than 1 million folders accessible to every employee").

[10] *Id.*

[11] *Data as an* asset, KPMG, 2 (2019), https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/10/data-as-an-asset.pdf (noting data storage costs are near zero which makes data refining paramount in the modern market).

[12] Ellen Chang, *What Is a Data Breach?*, EXPERIAN (Mar. 27, 2009), https://www.experian.com/blogs/ask-experian/what-is-a-data-breach (stating once data breaches occur because of employee negligence or accidents, companies and employees can be discouraged from "taking the proactive steps necessary to help prevent and plan for a data breach—a phenomenon known as 'breach fatigue'").

[13] *Id.*

[14] *Id.*

[15] Alexander (Sandy) R. Bilus & Erik J. VanderWeyden, *After TransUnion, Lower Courts Grapple with Article III Standing in Data Breach Lawsuits*, ABA (Apr. 27, 2022), https://www.americanbar.org/groups/litigation/committees/privacy-data-security/articles/2022/after-transunion-lower-courts-grapple-with-article-iii-standing-data-breach-lawsuits/.

[16] U.S. SOC. SEC. ADMIN., *Identity Theft and Your Social Security Number*, PUB. NO. 05-10064, 1-2 (2021) https://www.ssa.gov/pubs/EN-05-10064.pdf [hereinafter Identity Theft and Your SSN].

No circuit court has expressly "foreclosed plaintiffs from establishing standing based on a risk of future identity theft — even those courts that have declined to find standing on the facts of a particular case."[17] The Sixth, Seventh, Ninth, and D.C. Circuits have found standing at the pleading stage on a theory of increased risk of identity theft.[18] Conversely, the Third, Fourth, Eight, and Eleventh Circuits have refused to find standing on that same theory based on the facts presented before them.[19]

This note argues that the new standing test established by the Second Circuit in *McMorris v. Carlos Lopez Association, LLC* is flawed because it leaves a majority of plaintiffs without recourse after a data breach. Part II provides information about the standing requirement in general and as applied to data breach cases, including an overview of the differing approaches taken by circuit courts. Part III provides a detailed overview of the background and analysis employed by the Second Circuit in McMorris. Part IV outlines the flaws in the Second Circuit's data breach standing test and proposes modifications. Part V concludes that the Second Circuit's test is flawed because it fails to account for accidental and negligent data breaches.

"Buying personal information from 'inside' sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services, or credit." *Id.*

[17] McMorris v. Carlos Lopez & Ass'n., LLC, 995 F.3d 295, 300 (2d Cir. 2021).

[18] *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387-91 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 691-97 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141-43 (9th Cir. 2010); Ree v. Zappos.com, Inc. (*In re* Zappos.com, Inc.), 888 F.3d 1020, 1023-29 (9th Cir. 2018) (Court found standing where hackers "allegedly stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers," but not social security numbers, despite no evidence of misuse); AFGE v. OPM (*In re* OPM), 928 F.3d 42, 50-61 (2019) (Court found standing where hackers stole the Social Security numbers, fingerprint record, addresses, and other confidential information of former, present, and prospective government employees despite their being no evidence of misuse because the targeted attack was likely for the purpose of misusing the data); Attias v. Carefirst, Inc., 865 F.3d 620, 625-29 (D.C. Cir. 2017).

[19] *See* Reilly v. Ceridian Corp., 664 F.3d 38, 41-46 (3d Cir. 2011) (Court dismissed case when a hacker hacked defendant's payroll system and potentially gained access to, read, and copied personal employee information that consisted of first and last names, social security numbers, bank account information, and birth dates because allegations of increased risk of identity theft was hypothetical); Beck v. McDonald, 848 F.3d 262, 269-77 (4th Cir.), *cert. denied*, Beck v. Shulkin, 137 S.Ct. 2307, 2307 (2017) (Court dismissed case where hospital lost, likely through theft, a laptop with patient information that included birth dates, the last four digits of social security numbers, and physical descriptors because there was no impending threat of harm, no showing of misuse, and no showing of substantial risk of harm); Alleruzzo v. SuperValu, Inc. (*In re* SuperValu, Inc.), 870 F.3d 763, 767-74 (8th Cir. 2017) (Court dismissed the case where grocery store was hacked and lost credit and debit card information because the risk of future harm was too speculative; however, one litigant had standing because he suffered a fraudulent charge on his card); Tsao v. Captiva MVP Rest. Partners, Ltd. Liab. Co., 986 F.3d 1332, 1337-45 (11th Cir. 2021) (Court dismissed for lack of standing where the plaintiff alleged that a restaurant where he shopped at twice was the victim of a data breach which resulted in the loss of his credit card information because mitigation efforts were not sufficient to establish injury-in-fact).

II. BACKGROUND

Digitalization is transforming the way businesses operate, and for many, COVID-19 accelerated the process.[20] However, this progress is not without setbacks. With a greater percentage of the workforce working remotely, there is a greater risk of data breaches.[21] The threat, however, does not only come from hackers who steal data with the intent to sell it. Metadata from 2016 and 2017 shows that around 84% of data breaches were inadvertent.[22] The breaches were primarily the result of employee negligence.[23] Yet, as it currently stands, it is unlikely that companies will implement measures to better secure their data unless they are held liable for their employee's negligence.

A. Foundation for Article III Standing

Standing is a major hurdle plaintiffs must overcome in a data breach case.[24] To make the standing requirement even more difficult to satisfy, courts disagree on what the standing threshold is.[25] Although recently, more courts have followed the general trend towards finding standing at the pleading stage in data breach cases.[26] Article III, Section 2 of the Constitution identifies the standing requirement,[27] which has been

---

[20] Suphachai Chearavanont, *How digitization and innovation can make the post-COVID world a better place*, WORLD ECONOMIC FORUM (Aug. 11, 2020), https://www.weforum.org/agenda/2020/08/how-digitization-and-innovation-can-make-the-post-covid-world-a-better-place (stating the pandemic has presented potential for more digitalization of data, and "the shift to remote working and e-learning will likely extend beyond the COVID-19 pandemic").

[21] Mark Nevins, *New Dangers Of Working From Home: Cybersecurity Risks*, FORBES (May 19, 2021), https://www.forbes.com/sites/hillennevins/2021/05/19/new-dangers-of-working-from-home-cybersecurity-risks/?sh=5d3a4e5a22fb. "Companies have had to get better at cybersecurity in our digital age, but cybersecurity threats have grown significantly with distributed work. Work-from-home employees are at much greater risk than those in offices." *Id.*

[22] Mahmood Sher-Jan, *Data indicates human error prevailing cause of breaches, incidents*, THE PRIVACY ADVISOR (June 26, 2018), https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents. "Seasoned privacy professionals, however, know that in reality, the majority of incidents are inadvertent and unintentional, and can be classified as human error. And these incidents still trigger the same regulatory obligations as intentional and malicious incidents." *Id.*

[23] Matthew Stenberg, *Negligence Drives 90% of Data Breaches*, CYBELANGEL (Oct. 28, 2020), https://cybelangel.com/blog/negligent-data-breaches (stating common causes of such incidents include: "An overzealous or new employee foregoing security procedures for simplicity or time saving; an IT employee involved in shadow IT activities; or a third-party vendor leaving a server open with sensitive documents exposed").

[24] Gregory Szewczyk & Kelsey Fayer, *The Year 2021 in Review: Trends in Data Breach Litigation*, ABA (Feb. 11, 2022), https://www.americanbar.org/groups/litigation/committees/consumer/articles/2022/winter2022-year-2021-in-review-trends-in-data-breach-litigation/.

[25] *Id.* (stating "[c]ourts across jurisdictions have appeared to differ as to whether the risk of future harm constitutes an injury in fact sufficient for Article III standing, but the general trend in recent years has been a move toward finding standing").

[26] *Id.*

[27] U.S. CONST. art. III, § 2. The United States Constitution provides:

interpreted by the Supreme Court to limit "the jurisdiction of federal courts to 'Cases' and 'Controversies.'"[28] The Court established that a plaintiff must demonstrate the existence of three factors to have standing to sue.[29] First, the plaintiff must allege an injury in fact which is both "concrete and particularized", and it must also be "actual or imminent."[30] Second, the plaintiff must show that there is a connection between the injury and conduct complained of.[31] Finally, the plaintiff must demonstrate that a favorable court ruling is likely to redress the alleged injury.[32] Injury in fact is the most difficult factor to prove in a data breach case because plaintiffs regularly claim that the breach exposes them to the risk of future harm, which courts often find is too speculative.[33]

B. Supreme Court Standing Jurisprudence

Injury in fact requires that the plaintiff's allegations be "certainly impending" and not simply a potentiality.[34] In *Clapper v. Amnesty International USA*, the plaintiffs worked with individuals abroad who were likely to be subject to surveillance under the Foreign Intelligence Surveillance Act ("FISA").[35] Specifically, Amnesty International ("AI") alleged that its members communicated with foreign individuals who the United States Government suspected were associated with terrorist organizations or located in a geographical area that was the focus of the Government's intelligence efforts.[36] AI argued that they incurred costs and were forced to undertake burdensome measures

---

> 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 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.

[28] Lujan v. Defs. of Wildlife, 504 U.S. 555, 559 (1992). "While the Constitution of the United States divides all power conferred upon the Federal Government into 'legislative Powers,' Art. I, § 1, 'the executive Power,' Art. II, § 1, and 'the judicial Power,' Art. III, § 1, it does not attempt to define those terms." *Id.*

[29] *Id.* at 560.

[30] *Id.* (stating an "injury in fact" can be defined as "an invasion of a legally protected interest").

[31] *Id.* (holding "there must be a causal connection between the injury and the conduct complained of – the injury has to be 'fairly . . . trace[able] to the challenged action of the defendant, and not . . . the result [of] the independent action of some third party not before the court.").

[32] *Id.* at 561. Therefore, "it must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'" *Id.*

[33] *For Consumers, Injury Is Hard to Prove in Data-Breach Cases*, CIAB, https://www.ciab.com/resources/consumers-injury-hard-prove-data-breach-cases/.

[34] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (holding "[the United States Supreme Court has] repeatedly reiterated that 'threatened injury must be certainly impending to constitute injury in fact,' and that '[a]llegations of possible future injury' are not sufficient").

[35] *Id.* at 406.

[36] *Id.*

to protect the confidentiality of its contacts abroad.[37] AI alleged the costs sustained from protecting their clients' identities to be the injury that was directly traceable to the government's conduct.[38]

The Court noted that it is particularly hesitant to find standing in cases where the judiciary is asked to review the actions of the other political branches in fields such as foreign affairs and intelligence gathering. [39] The Court explained that the "'threatened injury must be certainly impending to constitute injury in fact,' and that '[a]llegations of possible future injury' are not sufficient."[40] In *Clapper*, the Court held AI's allegations of surveillance of their contacts to be speculative because no facts were offered to show that the foreign contacts' communications were targeted. [41] Alternatively, AI argued that they incurred costs in an effort to minimize the chances of surveillance.[42] However, this argument was dismissed by the Court because AI's self-inflicted costs were not the result of the government's activities, but the result of their fear of surveillance.[43]

No precise test exists to determine the boundaries of a case or controversy because it is a matter of degree.[44] The dissent in *Clapper* argued that the alleged harm was commonsense, and an understanding of human nature makes this injury sufficiently likely for Article III standing.[45] Specifically, the dissent first pointed to the fact that AI has, and continues to, engage in electronic communications that FISA permits the government to intercept.[46] Next, the plaintiffs will undoubtedly continue to engage in, and "the Government has strong *motive* to listen to," conversations of the sort at issue.[47] These conversations will include a lawyer's communications with his clients that involve confidential matters such as the potential terrorist activity the client is accused of engaging in.[48] Finally, the government has engaged in this sort of behavior

---

[37] *Id.* at 407.

[38] *Id.*

[39] *Clapper*, 568 U.S. at 409.

[40] *Id.* at 409 (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

[41] *Id.* at 411-12.

[42] *Id.* at 415.

[43] *Id.* at 418.

[44] *Clapper*, 568 U.S. at 423 (the dissent notes "[n]o one here denies that the Government's interception of a private telephone or e-mail conversation amounts to an injury that is 'concrete and particularized'").

[45] *Id.* at 422 (Breyer, J., dissenting) (stating "this harm is not 'speculative.' Indeed it is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen. This Court has often found the occurrence of similar future events sufficiently certain to support standing.").

[46] *Id.* at 427 (explaining "[t]hese communications include discussions with family members of those detained at Guantanamo, friends and acquaintances of those persons, and investigators, experts, and others with knowledge of circumstances related to terrorist activities").

[47] *Id.*

[48] *Id.* at 427-28. Specifically, the dissent expresses concern that:

> A fair reading of the affidavit of Scott McKay, for example, taken together with elementary considerations of a lawyer's obligation to his client, indicates that McKay will engage in conversations that concern what suspected foreign terrorists, such as his client, have done; in conversations that concern his clients' families, colleagues, and contacts; in conversations that concern what those persons (or those connected to them) have said and done, at least in relation to terrorist activities; in

in the past and has the capacity to conduct the sort of electronic surveillance at issue.[49] In other cases, the dissent noted that the Court found standing when the plaintiff took steps to mitigate the potential consequences of future injury.[50] Therefore, the word "certainly" does not require absolute certainty in the "certainly impending" standing requirement.[51] Instead, it requires "something more akin to 'reasonable probability' or 'high probability.'"[52]

The Supreme Court recently addressed the standing issue in *Spokeo, Inc. v. Robins*.[53] In *Spokeo*, Robins learned that Spokeo, a "people search engine," created a profile of Robins for an unknown person based on publicly available information, but it contained numerous inaccuracies.[54] The Court vacated and remanded the Ninth Circuit's determination of standing because the Ninth Circuit only considered whether the injury was particularized and did not consider whether it was concrete.[55] On remand, the Ninth Circuit was instructed to consider both factors of the injury-in-fact prong.[56] An injury is particularized when the plaintiff is affected in a personal or individual way, which means that the plaintiff actually suffered the harm themselves as a result of the alleged injury.[57] An injury is concrete when it is real instead of abstract; monetary loss or physical harm are examples of concrete injuries.[58] Concrete does not require the injury to be tangible; it can be intangible and still be concrete.[59] To determine if an injury is intangible, both history and congressional determination play an important role.[60] On remand, the Ninth Circuit found the alleged injury to be sufficiently concrete for Article III standing.[61]

> conversations that concern the political, social, and commercial environments in which the suspected terrorists have lived and worked; and so forth.

[49] *Clapper*, 568 U.S. at 429.

[50] *Id.* at 437. The dissent specifically pointed out that "the Court has found that a reasonable probability of future injury comes accompanied with present injury that takes the form of reasonable efforts to mitigate the threatened effects of the future injury or to prevent it from occurring." *Id.*

[51] *Id.* at 440-41. The dissent noted that it is only a matter of time before the injury occurs. Specifically, the dissent stated, "the ongoing threat of terrorism means that here the relevant interceptions will likely take place imminently, if not now." *Id.*

[52] *Clapper*, 568 U.S. at 441 (noting the government had motive and capacity to intercept communications, and no method to avoid interception of electronic communications that includes "a party who is an American lawyer, journalist, or human rights worker" has been developed).

[53] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544 (2016).

[54] *Id.* (stating the service requires that "an individual visits Spokeo's Web site and inputs a person's name, a phone number, or an e-mail address[.] Spokeo conducts a computerized search in a wide variety of databases and provides information about the subject of the search.").

[55] *Id.* at 1545.

[56] *Id.*

[57] *Id.* at 1548.

[58] *Spokeo, Inc.*, 136 S. Ct. at 1549. (holding "[a] 'concrete' injury must be 'de facto'; that is, it must actually exist." The standard dictionary definitions of real and abstract are applied to determine whether an injury is concrete.).

[59] *Id.*

[60] *Id.* (discussing "because that requirement in turn is grounded in historical practice, it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts").

[61] Robins v. Spokeo, Inc., 867 F.3d 1108, 1111-118 (9th Cir. 2017). "Spokeo published a report which falsely stated his age, marital status, wealth, education level, and profession, and which included a photo of a different person." *Id.* The Ninth Circuit agreed that Robins' employment prospects were potentially harmed.

After the *McMorris* opinion was issued, the Supreme Court decided *TransUnion LLC v. Ramirez*,[62] which presents the issue of whether a future risk of harm is sufficient for Article III standing.[63] *TransUnion* concerned a class action lawsuit where defendants claimed that TransUnion failed to take reasonable steps to ensure the accuracy of its credit reports in violation of the Fair Credit Reporting Act. [64] Specifically, the defendants alleged that TransUnion issued credit reports to third parties that erroneously flagged them as potential terrorists.[65] Of the 8,185 class members, only 1,853 suffered reputational harm, while the credit reports of the remaining 6,332 class members were not provided to third-parties.[66] The Supreme Court reasoned that the 1,853 class members who had their inaccurate credit reports disseminated suffered a concrete injury because the dissemination resulted in a harm to their reputation, which "bears a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts."[67] This harm has a "close relationship" to the tort of defamation.[68] The other 6,332 class members did not suffer a concrete harm because their credit reports were not disseminated, and "[p]ublication is 'essential to liability' in a suit for defamation."[69] The 6,332 class members further attempted to argue that they were at substantial risk of future harm; however, the Court concluded that the risk here was insufficient to give rise to Article III standing.[70]

---

[62] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

[63] *Id.*

[64] *Id.* The Fair Credit Reporting Act imposes the following three requirements that are relevant to this case:

> First, the Act requires consumer reporting agencies to "follow reasonable procedures to assure maximum possible accuracy" in consumer reports. §1681e(b). Second, the Act provides that consumer reporting agencies must, upon request, disclose to the consumer "[a]ll information in the consumer's file at the time of the request." §1681g(a)(1). Third, the Act compels consumer reporting agencies to "provide to a consumer, with each written disclosure by the agency to the consumer," a "summary of rights" prepared by the Consumer Financial Protection Bureau. §1681g(c)(2).

[65] *Id.* at 2200-02.

[66] *Id.* at 2200.

[67] *TransUnion LLC*, 141 S. Ct. at 2208-09. "Under longstanding American law, a person is injured when a defamatory statement 'that would subject him to hatred, contempt, or ridicule' is published to a third party." *Id.*

[68] *Id.* at 2209.

[69] *Id.*

[70] *Id.* at 2010-12 (stating "plaintiffs [did not] present evidence that the class members were independently harmed by their exposure to the risk itself—that is, that they suffered some other injury (such as an emotional injury) from the mere risk that their credit reports would be provided to third-party businesses").

C. Circuit Courts' Interpretation of Standing Requirements in Data Breach Cases

Several circuits have addressed the issue of data breaches, but reached differing conclusions based on the facts alleged.[71] The D.C. Circuit found standing where an unknown intruder hacked into twenty-two servers of CareFirst, a health insurance company, and obtained consumer's personal information, including social security numbers and email addresses.[72] The D.C. Circuit reversed the district court's dismissal of the case for a lack of standing because an unauthorized party gained access to CareFirst's servers and stole personal information.[73] It presumably did so for purposes of identity theft or credit theft.[74] The D.C. Circuit reasoned that, unlike in *Clapper*, a long sequence of uncertain events involving multiple parties does not have to occur for the plaintiff to suffer a harm like credit fraud or identity theft.[75] Since the data was stolen, it is plausible to infer that the hackers stole the data for malicious reasons.[76]

The Sixth Circuit addressed standing in the data breach context after Nationwide Mutual Insurance Company was hacked and lost the personal information, including social security numbers and birth dates, of approximately 1.1 million consumers.[77] Nationwide informed plaintiffs of the breach and offered one year of free credit monitoring and identity-fraud protection through a third-party vendor.[78] Plaintiffs alleged that they would continue to suffer financial harm resulting from the breach by maintaining continued credit and identity-fraud monitoring and paying for all associated expenses.[79] The Sixth Circuit concluded that the substantial risk of harm and the reasonable mitigation costs incurred are sufficient to establish Article III standing.[80] The key here is the fact that the data was stolen as part of a targeted attack, instead of an accidental breach, because hackers stole data to use it for fraudulent purposes.[81]

The Seventh Circuit addressed Article III standing in a data breach case after luxury department store Neiman Marcus was hacked in 2013.[82] It learned that fraudulent charges had been made on their client's debit and credit cards in December 2013.[83] On January 10, 2014, Neiman Marcus announced that it was the victim of a cyberattack that had occurred between July and October 2013 and around 350,000 cards have been exposed.[84] Some clients filed a class action, but their suit was

---

[71] *McMorris*, 995 F.3d at 300 (noting that "requiring plaintiffs to allege that they have already suffered identity theft or fraud as the result of a data breach would seem to run afoul of the Supreme Court's recognition that '[a]n allegation of future injury may suffice' to establish Article III standing").

[72] *Attias*, 865 F.3d at 623-24 (stating plaintiffs "raised eleven different state-law causes of action, including breach of contract, negligence, and violation of various state consumer-protection statutes").

[73] *Id.* at 628-29.

[74] *Id.*

[75] *Id.* at 629.

[76] *Id.* at 628.

[77] *Galaria*, 663 F. App'x at 386 (noting the plaintiffs alleged "invasion of privacy, negligence, bailment, and violations of the Fair Credit Reporting Act").

[78] *Id.*

[79] *Id.* 387-88.

[80] *Id.* at 388.

[81] *Id.*

[82] *Remijas*, 794 F.3d at 689-90.

[83] *Id.* at 690.

[84] *Id.*

dismissed because the district court found that they lacked standing.[85] 9,200 individuals suffered fraudulent charges as of the lawsuit, but all of them were reimbursed.[86] The Seventh Circuit recognized that a substantial risk of harm can suffice to establish Article III standing.[87] Article III standing was present because the plaintiffs must continue to take steps to protect their data, and it stands to reason that the hackers stole the information, "sooner or later, to make fraudulent charges or assume those consumers' identities."[88]

III. THE CASE

McMorris v. Carlos Lopez & Assocs., LLC concerns the appeal of Devonne McMorris who had her data breach claim dismissed because she and her co-plaintiffs failed to "allege an injury in fact sufficient to confer Article III standing."[89]

A. The Facts of the Case

In June 2018, Carlos Lopez & Associates, LLP ("CLA") experienced a data breach, when an employee accidentally emailed a spreadsheet containing sensitive employee information to the company's then-current employees.[90] The spreadsheet contained "Social Security numbers, home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire" of 130 then-current and past employees.[91] It took CLA two weeks to instruct its then-current employees to resolve the accidental data breach, but CLA did not contact any former employees regarding the breach nor take any other steps to mitigate the breach.[92]

B. Procedural History

The Plaintiffs, Robin Steven, Sean Mungin, and Devonne McMorris, filed a class-action lawsuit against CLA and Carlos Lopez, CLA's principal.[93] The chief allegation was that CLA breached its duty to protect confidential employee information.[94] The plaintiffs argued that, despite not yet being the victims of fraud or identity theft, they

---

[85] *Id.*

[86] *Id.* at 692.

[87] *Remijas*, *794 F.3d at* 693.

[88] *Id.* at 693.

[89] McMorris v. Carlos Lopez & Ass'n., LLC, 995 F.3d 295, 297 (2d Cir. 2021).

[90] *Id.* at 297-98.

[91] *Id.* at 298.

[92] *Id.*

[93] *Id.* (stating the complaint included counts for "state-law claims for negligence, negligence per se, and statutory consumer protection violations on behalf of classes in California, Florida, Texas, Maine, New Jersey, and New York").

[94] *McMorris*, 995 F.3d at 298 (stating that specifically, plaintiffs alleged CLA "'breached its duty to protect and safeguard [their] personal information and to take reasonable steps to contain the damage caused where such information was compromised'").

were "'at imminent risk of suffering identity theft' and becoming the victims of 'unknown but certainly impending future crimes.'"[95] Plaintiffs were also forced to take preventative measures such as purchasing identity theft protection services, credit monitoring services, and cancelling their credit cards.[96]

CLA filed a motion to dismiss with the district court, but before a ruling was issued, the parties reached a settlement and asked the district court to certify it.[97] Prior to the fairness hearing, the district court ordered, *sua sponte*, a briefing to determine whether plaintiffs had Article III standing.[98] During the fairness hearing, the district court informed the parties about its preliminary conclusion that plaintiffs lacked Article III standing because they failed to allege a concrete and particularized injury that was certainly impending.[99] The district court pointed to the fact that none of the class members alleged that their identity was actually stolen or misused.[100]

Furthermore, the district court noted the dissemination of plaintiffs' personal information was not the result of an intentional act, or a criminal attempt to hack CLA, which could lead to the inference that the hacker intended to retain and misuse the data.[101] The essence of the case was that defendants failed to exercise sufficient care to protect the confidential data from being disseminated among the company's employees.[102] On November 22, 2019, the district court issued its opinion, refusing to certify the settlement and dismissing the case.[103] McMorris appealed the district court's decision without the other plaintiffs in the class.[104]

C. The Second Circuit's Analysis

McMorris is the first case where the Second Circuit addressed whether a plaintiff has standing to sue based on a theory of future risk of identity theft or fraud resulting from the inadvertent disclosure of the plaintiff's personal data.[105] The Second Circuit identified a few factors to determine whether a plaintiff has Article III standing to sue after a data breach including:

> (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.[106]

---

[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *McMorris*, 995 F.3d at 298 (the district court holding it is hard to call this case a data breach case because the data was misplaced by a CLA employee instead of being acquired by a third-party).
[100] *Id.*
[101] *Id.* at 298-99.
[102] *Id.* at 299.
[103] *Id.*
[104] *McMorris*, 995 F.3d at 299.
[105] *Id.* at 300.
[106] *Id.* at 303.

These factors are highly relevant but non-exhaustive.[107] In applying the facts, the Second Circuit found that McMorris did not have Article III standing to sue.[108] Regarding the first factor, plaintiffs did not allege that their data was lost because of an intentional attack or obtained by a third party outside their workplace.[109] While the plaintiffs did allege that their personal information was disclosed without authorization to CLA employees, there was no allegation that anyone outside the company gained access to that information.[110] The Second Circuit also noted that the plaintiff's allegations were insufficient to establish a substantial risk of future identity theft because it would require the assumption that then-current CLA employees would either misuse the data themselves or provide it to a malicious third party.[111]

The plaintiffs also did not allege that their data was misused because of the accidental disclosure.[112] While plaintiffs do not need to show that they experienced actual identity theft or fraud, they must at least allege facts that suggest their personal information might be misused in some form.[113] The plaintiffs thus failed to satisfy the second prong of the test.[114] Regarding the third factor, the information stolen was substantial.[115] However, the Second Circuit reasoned that absent evidence of actual misuse, the disclosure of highly sensitive information is not sufficient.[116]

IV. ANALYSIS

A. The Limitations of the "Increased Risk of Identity Theft" Framework

Data breach cases are regularly brought under the theory that the plaintiff faces an increased risk of future identity theft.[117] Generally, the plaintiff will invest time and money to mitigate that risk, such as through purchasing identity theft services, and will request compensation for the time and money spent.[118] However, the Supreme Court warns that plaintiffs cannot manufacture standing by inflicting harm on themselves.[119] The question then becomes whether taking steps to mitigate the chances of personally identifiable information being misused constitutes manufacturing standing.

---

[107] *Id.*

[108] *Id.*

[109] *McMorris*, 995 F.3d at 303.

[110] *Id.*

[111] *Id.* at 304 (stating "we would have to assume that then-current employees of CLA . . . would either misuse the data themselves or leak or expose the spreadsheet containing Plaintiffs' PII to a malicious third party, and, if the latter, that such a third party would then misuse Plaintiffs' PII").

[112] *Id.*

[113] *Id.*

[114] *McMorris*, 995 F.3d at 304.

[115] *Id.*

[116] *Id.*

[117] *Id.* at 300.

[118] Bohnak v. Marsh & McLennan Cos., 2022 U.S. Dist. LEXIS 8256, at *8-9 (S.D.N.Y. Jan. 17, 2022).

[119] *Clapper*, 568 U.S. at 416.

In an effort to answer this question, various circuit courts have considered similar factors in the data breach context, and the Second Circuit composed its non-exhaustive, three-part test using the most common of these factors.[120] The problem with the "increased risk of identity theft" framework is that it limits plaintiffs' ability to litigate their case beyond the pleading stage in circumstances where sensitive data, like Social Security numbers, is negligently leaked. Absent a breach caused by a malicious third party or evidence of data misuse, the plaintiff has a slim chance, if any, chance of pursuing their case. This presents a series of problems because most data breaches are the result of negligence.[121] The Second Circuit is the first circuit to clearly crystalize the "increased risk of identity theft" framework,[122] but as the law develops, courts may shift away from such stringent application of that standard.

TransUnion LLC, decided after *McMorris*, offers some guidance in shifting away from the "increased risk of identity theft" framework. In that case, the Supreme Court held that "plaintiffs [whose inaccurate credit reports were not disseminated] did not demonstrate that the risk of future harm materialized."[123] However, the Court in *TransUnion LLC* did acknowledge that the dissemination of the inaccurate credit reports was a concrete harm because it bore resemblance to the tort of defamation.[124] Whereas, data breach cases typically begin when the personally identifiable information is disseminated. McMorris had her personally identifiable information disseminated to then-current employees of CLA.[125] While there was no evidence of harm, McMorris and the other victims of the data breach would have almost certainly preferred their personal information remain confidential. *TransUnion LLC* suggests that the dissemination of private information may be sufficient to confer standing where the "asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts."[126] In the future, litigants suing after a data breach may find some success by alleging that a data breach bears a "close relationship" to a harm recognized in American courts, such as, but not limited to, negligence, breach of an implied contract, or invasion of privacy. Such claims would likely bear close resemblance to the defamation argument in *TransUnion LLC*.

B. The Second Circuit's Data Breach Standing Test

1. The First Factor: How was the Data Exposed?

The first factor of the *McMorris* test asks "whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data[.]"[127] Courts that find

---

[120] *Id.* at 301-03.
[121] Reinicke, *supra* note 8.
[122] *McMorris*, 995 F.3d at 303-04.
[123] *TransUnion LLC*, 141 S. Ct. at 2211.
[124] *Id.* at 2208-09.
[125] *McMorris*, 995 F.3d at 298.
[126] *TransUnion LLC*, 141 S. Ct. at 2200.
[127] *McMorris*, 995 F.3d at 299. The Second Circuit noted that no one outside CLA is alleged to have acquired the information because the leak was accidental; thus, the breach is "[f]ar from being a

standing in a data breach case usually do so in part because the data was stolen as part of a malicious attack.[128] The Seventh Circuit noted in *Remijas* that hackers steal data to misuse it.[129] This first element of the test is often considered the most important.[130] It has the power to make or break a case.[131] However, it is important to consider whether the accidental dissemination of a person's personally identifiable information will prompt that person to take action to protect their data, and what the expenses associated with those steps are. According to most circuit courts, these questions are incompatible with the Supreme Court's prohibition against finding standing based on the possibility or reasonable likelihood of future injury.[132] Likewise, it clashes with the prohibition against plaintiffs inflicting harm on themselves to manufacture standing.[133] However, individuals who seek to protect their data are not doing so as a self-infliction of harm. Rather, it is a natural response to a data breach. Essentially, the harm is the need to protect the data that was leaked, and the effort to do so comes at a cost to the plaintiff.

The dissent in *Clapper* noted that the interception by the government of the plaintiffs' communications "is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen."[134] This standard makes more sense in the data breach context because the

---

'sophisticated' or 'malicious' cyberattack 'carried out to obtain sensitive information for improper use[.]'" *Id.*

[128] *See AFGE*, 928 F.3d at 56 (noting "hackers stole Social Security numbers, birth dates, fingerprints, and addresses, among other sensitive personal information. It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft"); *see also Alleruzzo*, 870 F.3d at 772 (stating the "[d]efendants failed to secure customer Card Information on their network; their network was subsequently hacked; customer Card Information was stolen by the hackers; and Holmes became the victim of identity theft after the data breaches"); *Attias*, 865 F.3d at 629 (where "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"); *Galaria*, 663 F. App'x at 390 (stating that but for Nationwide's allegedly lax security, the hackers would not have been able to steal Plaintiffs' data. These allegations meet the threshold for Article III traceability, which requires "more than speculative but less than but-for" causation"); *Ree*, 888 F.3d at 1027 (stating "[a]lthough there is no allegation in this case that the stolen information included social security numbers, as there was in *Krottner*, the information taken in the data breach still gave hackers the means to commit fraud or identity theft").

[129] *Remijas*, 794 F.3d at 693. "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.*

[130] *McMorris*, 995 F.3d at 301. "First, and most importantly, our sister circuits have consistently considered whether the data at issue has been compromised as the result of a targeted attack intended to obtain the plaintiffs' data." *Id.*

[131] *Id.* (holding "[w]here plaintiffs fail to present evidence or make any allegations that an unauthorized third party purposefully obtained the plaintiffs' data, courts have regularly held that the risk of future identity theft is too speculative to support Article III standing").

[132] *Clapper*, 568 U.S. at 409-10.

[133] *Id.* at 416.

[134] *Id.* at 422 (Breyer, J., dissenting). Justice Breyer discusses facts that, with commonsense inferences, demonstrate that the Government intercepted the plaintiff's communications:

> First, the plaintiffs have engaged, and continue to engage, in electronic communications of a kind that the 2008 amendment, but not the prior Act, authorizes the Government to intercept. . . . Second, the plaintiffs have a strong motive to engage in, and the Government has a strong motive to listen to,

stakes do not generally involve national security or the separation of powers.[135] The adverse impact of a data breach primarily affects the ordinary person whose data was exposed. Commonsense inference and ordinary human knowledge tell us that individuals who have their data exposed will seek to protect it. The extent of the harm depends on the type of data exposed, as the third factor of the *McMorris* test recognizes, because people will be more inclined to pay to protect sensitive data like Social Security numbers. Yet, despite progress in this field, negligent parties are yet to be held accountable.

Another issue with finding standing primarily when the breach is the result of a targeted attack is the fact that most breaches occur because of employee negligence.[136] According to the Second Circuit, most of the victims of such a breach have no chance at any sort of relief, like having the company pay for monitoring services, because their harm is too speculative.[137] *Clapper* also noted that parties cannot manufacture standing by inflicting harm on themselves.[138] In a data breach case, the dissemination of personal information is the injury, and it should be sufficient to confer standing. Due to the cost of litigation, most data breach cases are likely to get settled relatively quickly to avoid unnecessary expenses and costs.[139] In *McMorris*, the parties reached a settlement agreement and asked the district court to approve it, but the district court

---

> conversations of the kind described.... At the same time, the Government has a strong motive to conduct surveillance of conversations that contain material of this kind. . . . Third, the Government's past behavior shows that it has sought, and hence will in all likelihood continue to seek, information about alleged terrorists and detainees through means that include surveillance of electronic communications. . . . Fourth, the Government has the capacity to conduct electronic surveillance of the kind at issue. To some degree this capacity rests upon technology available to the Government.

[135] *Id.* at 402-06 (displaying the statute in question authorized the surveillance of individuals located outside the United States who were suspected of being threats to national security).

[136] Sher-Jan, *supra* note 22 (noting most data breaches are inadvertent but still should be followed by an investigation into the breach to prevent future incidents).

[137] *McMorris*, 995 F.3d at 301.

[138] *Clapper*, 568 U.S. at 416 (stating parties "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending").

[139] Kristen L. Burge, *Your Data Was Stolen, But Not Your Identity (Yet)*, ABA (Jan. 11, 2018), https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2018/your-data-was-stolen-not-your-identity-yet/. The author utilized the expertise of Tyler G. Newby, cochair of the ABA Section of Litigation's Privacy & Data Security Committee, and Fabrice N. Vincent, cochair of the Section's Class Actions & Derivative Suits Committee, and noted:

> But 'reality is that most, if not all, of these cases settle before trial . . . Newby concedes. Drawing on public policy, Vincent advocates the nature of the data breached should inform damages and the remedy, not dictate access to the courts. 'Only such a system will properly motivate the data holder to take the steps necessary to prevent data breaches as well as to offer real solutions to data breaches that have already occurred,' suggests Vincent. 'In a perfect world, all compromised persons would have standing to sue, and the severity of the breach, e.g., the importance of the compromised data and likelihood or actuality of ensuing further harm, would inform the magnitude of recoverable damages/remedy analysis (instead of a harsh standing rule that can unfairly bar claims in the first instance),' maintains Vincent.

refused sua sponte.[140] In other words, the district court proactively denied relief to the plaintiffs even though they managed to settle the case before any lengthy and expensive litigation.

2. The Second Factor: What was Done with the Data?

The second factor of the *McMorris* test asks "whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud[.]"[141] The Second Circuit reasoned that evidence of misuse is not a necessary component of standing in a data breach case.[142] However, the Second Circuit also recognized that the risk of identity theft is greater if at least one plaintiff had their compromised data misused.[143] Evidence of misuse is an important element in a data breach standing test because if one plaintiff's data was misused, another's data can be misused. The Seventh Circuit reasoned in *Remijas* that if hackers steal data, they plan to misuse it.[144] An offshoot to this argument is that if someone misuses another's accidentally leaked data, they will likely misuse the data of other's affected by the breach. Even if the data was not misused, that does not mean the plaintiff has not suffered a harm simply by having their data exposed because the plaintiff may reasonably seek to avoid misuse through monitoring services. This proposition is implicit in the Second Circuit's recognition that misuse is not required for standing.

3. The Third Factor: The Nature of the Data

The third factor of the *McMorris* test asks, "whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud."[145] If an individual's Social Security number is breached, the risk is much greater than when credit card information is leaked. Credit cards can easily be cancelled, but social security numbers cannot easily be replaced, and the Social Security Administration is slow to resolve the issue.[146] Hence, individuals cannot ignore or easily resolve the breach of their social security number and are often forced to purchase identity

---

[140] *Id.* at 298.

[141] *McMorris*, 995 F.3d at 303. Misuse, while not necessary to show standing in a data breach case, helps demonstrate that the plaintiff faces a greater risk of identity theft and/or fraud. Plaintiffs did not allege misuse in this case. *Id.*

[142] *Id.* at 301.

[143] *Id.* (holding "courts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused — even if plaintiffs' particular data subject to the same disclosure incident has not yet been affected").

[144] *Remijas*, 794 F.3d at 693.

[145] *McMorris*, 995 F.3d at 299. The Second Circuit noted that "the dissemination of high-risk information such as Social Security numbers and dates of birth — especially when accompanied by victims' names — makes it more likely that those victims will be subject to future identity theft or fraud." *Id.*

[146] Identity Theft and Your SSN, *supra* note 16, at 3. "If someone has misused your Social Security number or other personal information to create credit or other problems for you, Social Security can't resolve these problems. But there are several things you should do." *Id.*

protection. Naturally, plaintiffs' reactions to data breaches will vary based on the type of data exposed. The Second Circuit recognized in McMorris that the information that was leaked placed the plaintiffs at a significant risk of identity theft or fraud.[147] The leaked information, among other things, consisted of social security numbers. Despite this, the Second Circuit refused to acknowledge that plaintiffs will reasonably seek to protect the sensitive data that was disseminated, irrespective of the cause of the breach.[148]

The circulation of information that can easily and inexpensively be protected, such as credit card information,[149] should not give rise to standing, but the circulation of sensitive information should be sufficient to grant the plaintiff standing because of the devastating consequences.[150] Thus, the type of information stolen or circulated should be a key factor in determining whether to grant standing.

C. The Rise of Digitalization Will Result in More Data Breaches

The McMorris test fails to account for the fact that plaintiffs will be left without recourse as data becomes one of the most valuable commodities in a continually digitalized economy because companies are not adequately prepared to safeguard their

---

[147] *McMorris*, 995 F.3d at 305.

[148] *Id.* at 304.

[149] *Lost or Stolen Credit, ATM, and Debit Cards*, FED. TRADE COMM'N, https://consumer.ftc.gov/articles/lost-or-stolen-credit-atm-debit-cards#:~:text=Federal%20law%20already%20protects%20you,easy%20for%20you%20to%20report (last visited Dec. 10, 2021). People have a lot of protection when their debit or credit cards are lost or stolen, and the process to freeze a debit or credit account is very simple:

> If your credit, ATM, or debit card is lost or stolen, federal law limits your liability for charges made without your permission, but your protection depends on the type of card — and when you report the loss. It's important to act fast. If you wait until someone uses your card without permission, you may have to pay some or all of those charges. If someone uses your ATM or debit card before you report it lost or stolen, what you owe depends on how quickly you report it.

[150] Gayle Sato, *The Unexpected Costs of Identity Theft*, EXPERIAN (Sept. 30, 2020), https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft. The author discussed the various consequences that arise when a person's identity is stolen:

> Although debit and credit card issuers limit your liability for fraudulent charges, you could still be on the hook for the loss if you don't report phony charges in time. And since time is money, the hours you spend tracking, reporting and resolving the effects of identity theft are also a significant loss. According to a report from the SANS Institute, it takes an average of six months and roughly 200 hours of work to recover your identity after it's been compromised. It may even cause you to have to take time off from your job. . . . Having your identity stolen can be traumatic. In a survey of consumers who experienced identity crime, the Identity Theft Resource Center found that 77% reported increased stress levels and 55% experienced fatigue or decreased energy. Additionally, respondents said they had trust issues with friends and family, and problems with their employers or schools.

data. [151] Companies are incorporating electronic forms of data storage at an increasingly fast pace.[152] As a result, the use of data is leading to more data breaches, both malicious and unintentional.[153] With the loss of data, like social security numbers, employees and consumers will naturally seek to protect their exposed information even if it was not maliciously stolen or misused.[154] The courts' interpretation of standing jurisprudence does not account for the realities of the modern economy. Because, courts fail to recognize that a data breach caused by negligence is an injury in itself, once private data is disseminated, it cannot be undone.[155] Another major, related cause is the failure of companies to incorporate reasonable safeguards to protect their data and restrict access.[156] Considering the impact of COVID-19 on the economy, the threat of data breaches is greater, and the consequences to the victims more devastating.[157]

Since the COVID-19 pandemic, more companies have allowed their employees to work remotely which increases the risk of data breaches.[158] This trend will likely continue well into the future.[159] Companies are slow to implement cybersecurity measures.[160] Because employee negligence is already a key driver of data breaches,[161] the problem will only get worse as companies continue to promote remote work unless companies also invest in data protection.[162] The current standing jurisprudence for data breach cases offers little relief to many individuals who have had their data exposed due to negligence because courts are only willing to find standing under limited circumstances, such as the loss of data to hackers.[163] Therefore, companies have little incentive to protect their data with reasonable safeguards. Some states have addressed the problem of data breaches by passing statutes,[164] but generally, courts

---

[151] Data as an asset, *supra* note 11. "Only 18 percent of organizations feel they are very or extremely effective at maintaining an enterprisewide data management strategy." *Id.*

[152] Ahlstrom, *supra* note 1. "Data serves as the critical energy source of a business, so addressing data quality and governance offers a major opportunity for generating a competitive advantage. Organizations that capitalize on it early will differentiate themselves and pull out in front as market leaders." *Id.*

[153] Sher-Jan, *supra* note 22.

[154] Identity Theft and Your SSN, *supra* note 16, at 1-2.

[155] Stenberg, *supra* note 23 (noting breaches occur because employees either fail to take reasonable precautions to protect data or abuse poor company security measures to their advantage).

[156] *2019 VARONIS GLOBAL DATA RISK REPORT*, *supra* note 9.

[157] Booth, *supra* note 3.

[158] Chearavanont, *supra* note 20.

[159] *Id.*

[160] Stefan Leipold, *Cybersecurity Policies In The Age Of Remote Work*, FORBES (Mar. 15, 2021), https://www.forbes.com/sites/forbesbusinesscouncil/2021/03/15/cybersecurity-policies-in-the-age-of-remote-work/?sh=1b0533694442 (stating "organizations often remain unaware of the cybersecurity implications of the remote workforce. The new way of working expands the potential for cybersecurity threats with new vulnerabilities surrounding every employee working from home or a local cafe.").

[161] Reinicke, *supra* note 8. "Employee negligence is the main cause of data breaches . . . The report found that 47 percent of business leaders said human error such as accidental loss of a device or document by an employee had caused a data breach at their organization." *Id.*

[162] Ritesh, *supra* note 7 (noting that many companies are at a heightened risk of data breaches because they did not take cybersecurity considerations into account in the early stages of their software development).

[163] *AFGE*, 928 F.3d at 50-61; *Attias*, 865 F.3d at 625-29; *Galaria*, 663 F. App'x at 387-91; *Krottner*, 628 F.3d at 1141-43; *Ree*, 888 F.3d at 1023-29; *Remijas*, 794 F.3d at 691-97.

[164] Joseph J. Lazzarotti, et al., *California May Lower the Standing Threshold in Data Breach Litigation*, WORKPLACE PRIVACY, DATA MANAGEMENT & SECURITY REPORT (July 11, 2018),

are left to establish their own standards. However, courts have remained hesitant to find standing based solely on the fact that sensitive data was leaked.

A major issue is that courts have trouble applying standing principles to data breach cases.[165] The injury-in-fact prong is particularly difficult to meet and is often the main point of contention in a data breach case.[166] Therefore, the question often comes down to whether the plaintiff can establish that the injury is both particularized and concrete and either actual or imminent.[167] This is further complicated by courts' determination that plaintiffs cannot establish standing by inflicting harm on themselves by taking steps to avoid a potential injury in the future.[168] The Supreme Court has offered some guidance in this field[169] but has yet to grant certiorari to a case concerning data breach standing. This has proven to be problematic because courts' take a very conservative approach in granting standing, leaving many plaintiffs without recourse.

The particularized element requires that the injury affect the plaintiff in a personal and individualized way.[170] An injury is concrete when it actually exists; in other words, the injury must be real as opposed to abstract.[171] In the data breach context, courts agree that identity theft is a concrete and particularized injury.[172] However, oftentimes, plaintiffs sue before falling victim to identity theft. Courts are generally more willing to find a data breach to be both concrete and particularized when it results from a targeted attack, and when the data taken is sensitive, like a social security number.[173] However, digitalization is bound to result in more beaches. Based on current trends, more people will lose their data through the negligence of companies and their employees.[174] However, if the breach was not caused by a targeted attack, courts will likely deny relief. Such an approach is a major setback to the expectation that people's data will be protected when they share it with another organization as part of a contractual or transactional agreement.

---

https://www.workplaceprivacyreport.com/2018/07/articles/consumer-privacy/california-may-lower-the-standing-threshold-in-data-breach-litigation/ (discussing California passed a bill that permits consumers, defined as someone who provides personal information to purchase or lease a product or obtain a service, to sue for breach of personal information without showing actual injury. A breach is defined as "'unauthorized access, use, modification, or disclosure of personal information.'").

[165] *McMorris*, 995 F.3d at 300 (noting no court has explicitly foreclosed the possibility of finding standing on a theory of increased risk of future identity theft).

[166] *Id.*

[167] *Spokeo, Inc.*, 136 S. Ct. at 1545 (holding there is no standing unless the injury is both particularized and concrete).

[168] *Clapper*, 568 U.S. at 419.

[169] *Id.* at 409-14 (noting "speculative chain of possibilities does not establish that [an] injury based on [the] potential" of future injury will occur); *Spokeo*, *Inc.*, 136 S. Ct. at 1545 (defining what a particularized and concrete injury is).

[170] *Spokeo, Inc.*, 136 S. Ct. at 1548.

[171] *Id.*

[172] *AFGE*, 928 F.3d at 55 (stating "the loss of a constitutionally protected privacy interest itself would qualify as a concrete, particularized, and actual injury in fact. And the ongoing and substantial threat to that privacy interest would be a concrete, particularized, and imminent injury in fact.").

[173] *McMorris*, 995 F.3d at 301-04 (noting sister circuits have consistently considered whether the breach was caused by a targeted attack).

[174] Sher-Jan, *supra* note 22.

Courts also require that the injury be actual or imminent for the injury-in-fact prong to be met.[175] In the preeminent Supreme Court case on standing, *Clapper*, the analysis was particularly stringent because it concerned national security and the separation of powers.[176] The statute in *Clapper* permitted government surveillance when the target was either a foreign power or agent.[177] Therefore, the Court was more deferential to the government considering the interests at stake and concern for ensuring the separation of powers. Because data breach cases generally do not involve issues of national security, the analysis is not likely to be as stringent. Data breach cases will come down to how certain future identity theft is. However, given the modern importance of data, the cause of action should not be so limited. When data is impermissibly disseminated, the burden should shift to the negligent party to mitigate the damage.

V. CONCLUSION

Data breaches will continue to increase in frequency as businesses and the economy continue to digitalize.[178] The new non-exhaustive, 3-prong data breach standing test developed by the Second Circuit offers some guidance, but it still leaves many victims of data breaches without recourse.[179] The Second Circuit's test is the most comprehensive attempt at clarifying the standing requirement in a data breach case and will provide guidance for future litigants.[180] However, the test is not without its flaws, and courts should continue to refine it to eventually offer relief to victims of data breaches caused by negligence.

To create the test, the Second Circuit analyzed the rationales of other circuits and found that a plaintiff generally has no standing in a situation where the data breach

---

[175] *Clapper*, 568 U.S. at 409 (noting imminence is an elastic concept but requires the injury to be certainly impending).

[176] *Ree*, 888 F.3d at 1026.

[177] *Clapper*, 568 U.S. at 403.

[178] Ritesh, *supra* note 7.

[179] *McMorris*, 995 F.3d at 301 (noting courts routinely find the injury to be too speculative where the data breach was not the result of a targeted attack).

[180] Phillip N. Yannella, *Second Circuit ruling clarifies when data breach plaintiffs have adequately pleaded Article III standing*, CONSUMER FINANCE MONITOR (May 7, 2021), https://www.consumerfinancemonitor.com/2021/05/07/second-circuit-ruling-clarifies-when-data-breach-plaintiffs-have-adequately-pleaded-article-iii-standing. The author recognized the importance of the Second Circuit's data breach standing test:

> McMorris may prove to be a landmark opinion. The Second Circuit's opinion is the first to set forth a list of factors for courts to assess when determining whether there is a substantial risk of identity theft and it is likely that litigants, and potentially other courts, will cite the McMorris factors in future cases. Beyond the substantial risk test, plaintiffs and defendants will likely cite different aspects of the Second Circuit's opinion to advance their arguments. Data breach plaintiffs will cite McMorris for the proposition that fear of future identity theft can establish standing, and to argue that there is not a circuit court split on this issue. Defendants on the other hand will cite the Second Circuit's ruling that out of pocket expenses to guard against identify theft does not automatically create standing.

was accidental.[181] Courts justify this view by claiming that criminals steal data to misuse it.[182] Thus, accidental or negligent breaches are insufficient to show harm.[183] Denying standing to victims of accidental and negligent breaches only incentivizes companies to ignore cybersecurity in favor of cutting costs.[184] Fortunately, the Supreme Court has offered some guidance in *TransUnion LLC*.[185] Future litigants will want to attempt to argue that a data breach "bears a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts."[186] This argument can potentially take many forms, ultimately depending on the facts of each case, and how those facts relate to a harm traditionally recognized by American courts.

Furthermore, denying standing when the data breach was caused by an accident or negligence ignores how victims will react to a data breach. Victims of data breaches will be prompted to protect their data at significant expense to themselves, and victims will be unable to secure any sort of compensation for their loss. Going forward, courts will have to consider how to handle accidental and negligent breaches. While the Second Circuit's test offers a model for other courts to develop a more comprehensive test, it is not sufficient for modern realities.

---

[181] *McMorris*, 995 F.3d at 301-3.

[182] *Remijas*, 794 F.3d at 693.

[183] *McMorris*, 995 F.3d at 304 (holding "[a]ccordingly, we conclude that the sensitive nature of McMorris's internally disclosed PII, by itself, does not demonstrate that she is at a substantial risk of future identity theft or fraud").

[184] U.S. Dep't of Lab., *CYBERSECURITY PROGRAM BEST PRACTICES* 4, https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf. "Employees are often an organization's weakest link for cybersecurity. A comprehensive cybersecurity security awareness program sets clear cybersecurity expectations for all employees and educates everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat." *Id.*

[185] *TransUnion LLC*, 141 S. Ct. at 2209.

[186] *Id.*