American University National Security Law Brief

Volume 7 | Issue 1 Article 3

2017

Cybersecurity, Identity Theft, and Standing Law: A Framework for Data Breaches Using Substantial Risk in a Post-Clapper World

James C. Chou

CYBERSECURITY, IDENTITY THEFT, AND STANDING LAW: A FRAMEWORK FOR DATA BREACHES USING SUBSTANTIAL RISK IN A POST-*CLAPPER* WORLD

A man who is used to acting in one way never changes; he must come to ruin when the times, in changing, no longer are in harmony with his ways.

~Niccolò Machiavelli, THE PRINCE

JAMES C. CHOU*

INTRODUCTION

Large-scale cyberattacks[1] involving the theft of personal and confidential records continue to make headlines as cybersecurity evolves into a national issue.[2] In 2015 alone, there were over 2,000 cases of data breaches with known data loss across a range of institutions.[3] Many data breaches, such as

* Articles Editor, American University Law Review, Volume 66. J.D. Candidate, 2018 American University Washington College of Law; M.S., George Mason University, 2008; B.A., University of Virginia, 2005. Articles Editor, American University Law Review, Volume 66. My sincere thanks to Professor Jennifer Daskal for her wisdom and guidance, and the National Security Law Brief staff for their meticulous efforts and assistance in refining this Article. Above all, a sincere thanks to my parents, Jaw and My Duc, and to Carrie Zheng for their unwavering support

[1] "A [cybersecurity] incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." PAUL CICHONSKI ET AL., NAT'L INST. OF STANDARDS & TECH., U.S. DEPT. OF COMMERCE, SPECIAL PUB. 800-61, REVISION 2, (DRAFT), COMPUTER SECURITY INCIDENT HANDLING GUIDE 6 (2012). An incident can lead to web-service disruption, malware infection, and sensitive-data exposure.

[2] *See* President Barack Obama, Statement on Cybersecurity Framework (Feb. 12, 2014), https://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework ("America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace"); *see generally* EXEC. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE (2011).

[3] VERIZON, 2015 DATA BREACH INVESTIGATIONS REPORT 3 (2015) [hereinafter DBIR 2015]. For a list of major breaches involving national security or sensitive information, *see* David

those involving the Office of Personnel Management (OPM) and Ashley Madison, have implicated more than just financial or identify-theft concerns, they have also raised national security issues and exposed victims to potential blackmail.[4]

As the cyber threat evolves, there is more data suggesting that data-breach victims are at a heightened risk of becoming subsequent victims for identity theft and other related crimes.[5] In 2012, the Bureau of Justice Statistics estimated that identity theft affected 16.6 million people and inflicted financial losses totaling $24.7 billion, which is $10 billion more than burglary, vehicle theft, and general theft combined.[6] Furthermore, estimates for 2014 increased, with an estimated 17.6 million victims totaling near $15.4 billion.[7] More importantly, while forensic analysis of some data breaches suggest a zero-day or complex attack that is hard to prevent, many high-profile breaches could have been prevented through simple controls and safeguards.[8]

Inserra and Paul Rosenzweig, *Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation*, HERITAGE FOUNDATION (Oct. 27, 2014), www.heritage.org/research/reports/2014/10/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation.

[4] *See infra* notes 18-29 and accompanying text.

[5] *See* Susan Ladika, *Study: Data Breaches Pose a Greater Risk*, CREDITCARDS.COM (Jul. 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (noting that the chances of being victimized after data loss have increased from one-in-nine in 2010 to one-in-three in 2014); *see also* Eva Velasquez, *Study Shows Link Between Breaches and Fraud*, IDT911 (Jun. 10, 2010), http://idt911.com/education/blog/study-shows-link-between-breaches-and-fraud (noting the Identity Theft Resource Center's findings that data breach victims experience an eightfold increase of "existing [credit] card fraud" risk).

[6] ERIKA HARRELL & LYNN LANGTON, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012 6 (2013), http://www.bjs.gov/content/pub/pdf/vit12.pdf.

[7] ERIKA HARRELL, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2014 6-7 (2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[8] *See infra* notes 39-45 and accompanying text. A zero-day attack generally involves exploiting a vulnerability that a software developer (and the broader community) is not yet aware of. Kim Zetter, Hacker Lexicon: What Is A Zero-Day? WIRED (Nov. 11, 2014, 6:30 AM), http://www.wired.com/2014/11/what-is-a-zero-day/. Zero-day attacks are harder to defend against because there is no known patch or fix for the vulnerability. However, most data breaches involving consumer data are not in this category. *See* DBIR 2015, *supra* note 3, at 15 (finding that most vulnerabilities were known at the time a breach occurred). Plus, there are also established methods that corporations can use to "harden" their systems against zero-day attacks. *See generally* LINGYU WANG ET AL., K-ZERO DAY SAFETY: A NETWORK SECURITY

Since *Clapper v. Amnesty International USA*,[9] many courts have shut the door on victims alleging a heightened risk of injury, particularly when the injury is identity theft, because *Clapper* does not permit standing based on a heightened risk of injury alone.[10] But recently, the Seventh Circuit disagreed with that view when deciding *Remijas v. Neiman Marcus Group*,[11] a case involving a breach of Neiman Marcus' systems, holding that *Clapper* neither altered standing law nor did it foreclose all heightened risk injuries.[12] This Article agrees and argues that *Clapper* did not alter the Article III standing requirements; it merely reemphasized the Court's demand for a heightened scrutiny for constitutional challenges to government activity. Consequently, the Seventh Circuit correctly applied standing law in *Remijas* under a "substantial" risk theory.

Part I will discuss large-scale data breaches and its relationship with identity theft, *Clapper*, and Article III standing on imminent injuries. Part II argues that the minimum constitutional threshold should allow standing under a heightened-risk-of-identity-theft (HRIT) using a "substantial" or "reasonable" risk threshold. Part III applies Part II to data-breach cases, specifically, and suggests several factors the courts could consider when determining whether a victim faces a sufficiently imminent injury for Article III standing. Part III also demonstrates that the Seventh Circuit used similar factors in *Remijas*. I then conclude.

METRIC FOR MEASURING THE SECURITY RISK OF NETWORKS AGAINST UNKNOWN ATTACKS 10-13 (2013), http://csrc.nist.gov/staff/Singhal/ieee_tdsc_2013_final_version.pdf.

[9] Clapper v. Amnesty Int'l U.S.A., 133 S. Ct. 1134 (2013).

[10] *See* Peters v. St. Joseph Servs.' Corp., 74 F. Supp. 3d 847, 856 (S.D. Tex. 2015) ("*Clapper* has resolved the circuit split."); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 365 (M.D. Pa. 2015) ("Allegations of increased risk of identity theft are insufficient to allege a harm.").

[11] 794 F.3d 688 (7th Cir. 2015).

[12] *Id.* at 693-94.

I. BACKGROUND

A. Data Breaches and Lawsuits

The struggle for adequate cybersecurity continues as society further incorporates Internet and digital technology in all aspects of life.[13] A critical cybersecurity tenant is protecting sensitive personally identifiable information (PII) and online accounts, which includes names, addresses, social-security numbers (SSNs), financial data, consumer habits, passwords, medical records, and other information that can be used to further fraud and identity theft.[14] PII is becoming an extremely valuable commodity for criminals, foreign intelligence operatives, and independent actors within the digital age, who often utilize PII to commit fraud or espionage.[15] Massive black-markets have been established within the deep web to sell and purchase PII.[16] More

---

[13] *See* KASEY LOGAUGH, DELOITTE, THE NEW DIGITAL DIVIDE 5 (2014), http://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-rd-thenewdigitaldivide-041814.pdf (noting that digital sales were estimated at $1.1 trillion in 2013 and "projected to grow to $1.5 trillion by the end of 2014").

[14] *See* GARY STONEBURNER, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800-33, UNDERLYING TECHNICAL MODELS FOR INFORMATION TECHNOLOGY SECURITY, 2-5 (2001) (noting that "confidentiality," "availability," and "integrity" are the three main objectives for information security). "Confidentiality" is about securing "private" information from unauthorized access. Confidentiality is often prioritized "behind availability and integrity." *See also* 44 U.S.C. § 3542(B)(1)(B) (2015) (defining confidentiality); *see also* ERICA in Federal information policy); ERIKA MCCALLISTER ET AL., NAT'L INST. OF SCISTANDARDS & TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII), ES-1-2 (2010) (discussing various forms of PII).

[15] *See* Graham Messick and Maria Gavrilovic, The Data Brokers: Selling Your Personal Information (60 Minutes Mar. 9,2014) (transcript available at http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/) (noting that a complete set of identity information for health-insurance fraud could fetch hundreds of dollars on the black market); *see also* Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10X Price of Stolen Credit Card Numbers,* NETWORK WORLD (Feb 6. 2015, 5:49 AM), http://www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (noting that social security numbers, birth dates, and other personal information are more valuable than credit card accounts because they are reusable).

[16] *See* Namaan Huq, *Follow the Data: Dissecting Data Breaches and Debunking Myths*, TREND MICRO 22-35 (2015), https://www.trendmicro.com/cloud-content/us/pdfs/security-

interestingly, some organizations have even legally monetized PII by developing digital platforms enabling consumers to, effectively, sell their personal information (in the form of habits, preferences, and interests) for compensation.[17]

There were many interesting data-breach incidents in 2014-2015, particularly Ashley Madison, Office of Personnel Management (OPM), the healthcare sector, and retailers. These cases represent the expanding creativity and motivational spectrum that cyber-criminals have, who are expanding the range of financial and nonfinancial damages victims sustained.

In late 2015, a hacking group stole PII and user accounts from AshleyMadison.com[18] with the intention of forcing the site to shut down.[19] After "completely compromising the company's user databases," the attackers released an ultimatum:

> We have taken over all systems in your entire office and production domains, all customer information databases, source code repositories, financial records, emails. Shutting down [Ashley Madison] and EM will cost you, but non-compliance will cost you more: [w]e will release all customer records, profiles with all the customer's secret sexual fantasies, nude pictures, and

intelligence/white-papers/wp-follow-the-data.pdf (showing screenshots of various prices for different types of PII, financial records, and online accounts).

[17] *See* Ben Woods, *What's the True Value of Your Personal Data? Meet the People Who Want to Help You Sell it*, INSIDER (Sep. 17, 2013), http://thenextweb.com/insider/2013/09/17/whats-the-true-value-of-your-personal-data-meet-the-people-who-want-to-help-you-sell-it/ (discussing Handshake as a new platform where users can volunteer identifiable or anonymous personal information to businesses, earning $1,600 to $8,000).

[18] Brian Krebs, *Online Cheating Site Ashley Madison Hacked*, KREBSON SECURITY (Jul. 19, 2015, 11:40 PM), http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/.

[19] *The Ashley Madison Hack . . . in 2 Minutes*, CNN (Sep. 11, 2015, 11:34 AM), http://money.cnn.com/2015/08/24/technology/ashley-madison-hack-in-2-minutes/index.html.

> conversations and matching credit card transactions, real names and addresses, and employee documents and emails.[20]

When Avid Life Media, Ashley Madison's owner, failed to comply, the hackers released PII records of more than thirty-seven million members.[21] After the release, there were numerous repercussions, including the resignation of Avid Life Media's CEO, increased opportunities for extortion, and widespread public humiliation.[22] John Gibson, an Ashley Madison user and a pastor, committed suicide after the records release and left his wife and kids behind.[23]

A few months prior, OPM reported a massive breach of its personnel systems, including 19.7 million personnel records through its clearance-adjudication system, e-QIP.[24] The breach occurred sometime around March 2014 and OPM discovered the breach four months later.[25] The e-QIP system contained a "treasure trove" of information related to previous crimes, psychological problems, and sexual history.[26] It also included approximately 5.6 million fingerprint records.[27] Many cybersecurity and intelligence analysts

---

[20] Krebs, *supra* note 18.
[21] Alyssa Newcomb, *Ashley Madison Hack: What's Included in the Data Dump*, ABC NEWS (Aug. 19, 2015, 12:27 PM), http://abcnews.go.com/Technology/ashley-madison-hack-included-data-dump/story?id=33176238.
[22] David Bisson, *The Ashley Madison Hack – A Timeline*, TRIPWIRE, http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline/ (last updated Sep. 10, 2015); *see* Kristen V. Brown, *We Talked to 24 Victims of the Ashley Madison Hack About Their Exposed Secrets*, FUSION (Aug. 19, 2015, 7:06 PM), http://fusion.net/story/185647/ashley-madison-hack-victims/ ("The thing about this leak is that it's a public shaming.").
[23] *See* Laurie Segall, *Pastor Outed on Ashley Madison Commits Suicide*, CNN (Sep. 8, 2015, 7:10 PM), http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/index.html.
[24] *See* Brian Krebs, *Catching Up on the OPM Breach*, KREBS ON SECURITY (Jun. 15, 2015, 11:25 AM). https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/.
[25] *See id.*
[26] *Id.* (quoting Ellen Nakashima & Lisa Rein, *Chinese Hackers Go After U.S. Workers' Personal Data*, WASH. POST (Jul. 10, 2014) (characterizing the amount of information stolen as a "treasure trove"); Kim Zetter & Andy Greenburg, *Why the OPM Breach is Such a Security and Privacy Debacle*, WIRED (Jun. 11 2015, 10:40 PM), http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.
[27] *See* Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sep. 23, 2015),

have emphasized national-security implications with current and formal federal employees being potentially exposed to blackmail, identity theft, and counter-intelligence and collection activities.[28] Furthermore, many federal employees have expanded their frustration and anger about the government's failure to protect their PII.[29]

In another turn of events, the healthcare and health insurance sectors faced a record number of successful attacks with millions of medical records stolen over the past several years, imposing over six billion in costs.[30] Interestingly, healthcare records are becoming increasingly valuable to cybercriminals because, unlike credit-card numbers, "medical and prescription records are permanent."[31] Healthcare records also provide a complete profile,[32] which allows a greater range of exploitation options, such as

---

https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.

[28] *See* Zetter & Greenburg, *supra* note 26 (discussing how foreign intelligence agents could use the information obtained from background checks to blackmail current intelligence employees who have access to highly classified information). What makes the OPM breach worse is that security clearance applicants must often disclose sensitive PII of relatives, family members, and friends. *See* Josephine Wolff, *The OPM Breach Is Putting A Damper on My Thanksgiving*, SLATE (Nov. 24, 2015, 12:52 PM), http://www.slate.com/articles/technology/future_tense/2015/11/the_opm_data_breach_is_putting_a_damper_on_my_thanksgiving.html ("I'll . . . tell my family members that they may be at risk and there's nothing I can do about it.").

[29] *See* Wolff, *supra* note 28; *see also* John Schindler, *Ex-NSA Officer: OPM Hack is Serious Breach of Trust*, NPR (Jun. 13, 2015, :50 8:00 AM), http://www.npr.org/2015/06/13/414149626/ex-nsa-officer-opm-hack-is-serious-breach-of-worker-trust (discussing how the leak will create more vulnerable government employees, and the feeling of "betrayal" with the government's failure to protect information).

[30] *See* Dan Munro, *Data Breaches In Healthcare Totaled Over 112 Million Records In 2015*, FORBES (Dec. 15 2015, 9:11 PM), http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/ (noting there were more than 253 healthcare breaches in 2015 with a combined total of over 112 million medical records stolen, approximately one-in-three Americans); *see also* Shannon Pettypiece, *Rising Cyber Attacks Costing Health System $6 Billion Annually*, BLOOMBERG (May 7, 2015, 6:00 AM) https://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually (noting that hospitals are losing $2.1 million, on average, from insurance fraud).

[31] Fahmida Y. Rashid, *Why Hackers Want Your Health Care Data Most of All*, INFOWORLD (Sep. 14, 2015), http://www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html.

[32] *See* INST. FOR CRITICAL INFRASTRUCTURE TECH., HACKING HEALTHCARE IT IN 2016 5-6 (2016), http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf [hereinafter ICIT REPORT] (noting that hackers will "expend significant resources"

"obtain[ing] prescription medicine [using] the victim's identity."[33] Many victims of health-related fraud experience critical issues, such as "life-threatening inaccuracies in their medical records," "misdiagnosis," and inaccurate prescriptions.[34] In 2013, consumers paid nearly twelve-billion dollars of out-of-pocket costs.[35]

Classic attacks on retailers and the financial sector using point-of-sale (POS) attacks or credit-card skimmers have not substantially abated.[36] In 2013, Target and Neiman Marcus faced similar sophisticated attacks on their systems.[37] And though the Neiman Marcus attack was smaller, it was more sophisticated, resulting in more than 9,000 credit cards being fraudulently used.[38]

A common theme for many cybersecurity incidents is that they were preventable had sound security measures and practices been in place prior to

---

to find and obtain healthcare records because hospitals have more private information on and individual than any bank or employer).

[33] *See* Brian Krebs, *A Day in the Life of a Stolen Healthcare Record*, KREBS ON SECURITY (Apr. 28, 2015, 12:46 AM), http://krebsonsecurity.com/2015/04/a-day-in-the-life-of-a-stolen-healthcare-record/ [hereinafter *Krebs on Healthcare*] (tying tax return fraud reported by physicians to data breaches in the healthcare sector).

[34] *Medical ID Fraud Costs Consumers $12bn in Out-of-Pocket Costs*, INFO SECURITY (Sep, 16 2013), http://www.infosecurity-magazine.com/news/medical-id-fraud-costs-consumers-12bn-in-out-of/.

[35] *See id.*; *see also* BARBARA FILKINS, SANS INST., HEALTH CARE CYBERTHREAT REPORT 5 (2014) (emphasizing that unlike credit-card fraud, consumers generally cannot recover costs for health-care-related fraud).

[36] *See* DBIR 2015, *supra* note 3, at 35-38 (discussing trends in POS and credit-card skimming exploits). POS and credit-card skimming are specific exploits designed to capture credit-card numbers and other financial data at the when the vendor or customer swipes a credit card. SYMANTEC, SPECIAL REPORT: ATTACKS ON POINT-OF-SALE SYSTEMS, V.2.0 5 (2014). Credit card systems handle a variety of transactions today, and although all vendors are required to comply with PCI-DSS, a security standard, there are vulnerabilities that can be exploited by attacking associated networks. *Id.* at 6-7.

[37] *See* Rip Empson, *Neiman Marcus Breach Could Be Part Of Larger Holiday Cyberattack On U.S. Retailers*, TECHCRUNCH (Jan 11, 2014), http://techcrunch.com/2014/01/11/following-attack-on-target-neiman-marcus-confirms-its-own-breach-and-could-be-just-the-tip-of-the-iceberg/; *see also* Victoria Wagner Ross, *Target Cyber Breach Extends, Neiman Marcus Reports a Cyber-Theft*, EXAMINER (Jan 11, 2014, 12:35 PM), http://www.examiner.com/article/target-cyber-breach-extends-neiman-marcus-reports-a-cyber-theft-attack.

[38] Benjamin Elgin et al., *Neiman Marcus Hackers Set off 60,000 Alerts with Card Thefts*, BLOOMBERG (Feb. 21, 2014, 9:44 PM), http://www.bloomberg.com/news/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-in-bagging-card-data.html.

(and during) an attack.[39] Many companies, organizations, and agencies are often criticized for mishandling large-scale breaches and for failing to implement an effective cybersecurity program.[40] For instance, OPM failed to encrypt PII information in the system, which is an "industry best practice."[41] Target also missed many warning signs that, if acted on, could have prevented the breach from becoming a serious problem.[42] Often, warnings do not help. In 2014, the FBI warned the healthcare industry that its systems were vulnerable to cyberattacks, but hackers, nevertheless, made several dozen successful attacks.[43] Another trend is that companies, especially healthcare providers, have access to greater and greater amounts of data.[44] Consequently, a single compromise has greater effects.

Even worse, most companies do little to mitigate vulnerability risks or make substantial security investments pre- and post-attack.[45] This is partially

---

[39] *See* U.S. COMPUTER EMERGENCY RESPONSE TEAM, TA15-119, TOP 30 TARGETED HIGH RISK VULNERABILITIES (2015), https://www.us-cert.gov/ncas/alerts/TA15-119A [hereinafter US-CERT] (finding that "[eighty-five] percent of targeted attacks are preventable").

[40] *See* DBIR 2015, *supra* note 4, at 15 (noting that 99.9% of breaches involving a vulnerability exploit "were compromised more than a year after the [Common Vulnerability & Exposure (CVE)] was published"). See generally COMMON VULNERABILITIES & EXPOSURES, http://cve.mitre.org/about/faqs.html (last visited Apr. 9, 2016), (A CVE "is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cybersecurity issues.). *See also* OFFICE OF THE INSPECTOR GENERAL, OPM U.S. OFFICE OF PERSONNEL MANAGEMENT, SEMI ANN. REP. TO CONGRESS 7-11 (2015) (noting several security gaps among healthcare providers under an OPM administrated health program).

[41] David Perera, *Agency Didn't Encrypt Feds' Data Hacked by Chinese*, POLITICO (last updated Jun. 5, 2015, 9:03PM), http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655.

[42] *See A "Kill Chain" Analysis of the 2013 Target Data Breach*, MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER i (Mar. 26, 2014).

[43] *See* Jim Finkle, *FBI Warns Healthcare Sector Vulnerable to Cyber Attacks*, REUTERS (Apr. 23 2014, 3:15 PM), http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423; *see also* Munro, *supra* note 30 (listing the top ten healthcare data breaches in 2015); *see generally* FILKINS, *supra* note 35, at 4-5, 7-11 (analyzing malicious traffic patterns and concluding there is massive security non-compliance and vulnerabilities across the healthcare sector).

[44] *See* FILKINS, *supra* note 35, at 12.

[45] *See* US-CERT, *supra* note 39; *see also* J. Craig Anderson, *Identity Theft Growing, Costly to Victims*, USA TODAY (Apr. 14, 2013, 4:38 PM), http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/ (noting that corporations are not investing in security and that law enforcement finds it difficult to investigate, leaving victims to fend for themselves).

because most companies or agencies are not sustaining any major financial loss from data breaches:[46] the majority of the risk is borne by the consumer and credit-card issuers.[47] Furthermore, many suggest that current legislative proposals would not fix the problem.[48] And though the Federal Trade Commission (FTC) has taken affirmative steps to impose additional costs on companies that disregard modern-day security practices, there is still a substantial cost-to-risk imbalance.[49]

---

[46] *See* Erik Sherman, *The Reason Companies Don't Fix Cybersecurity*, CBS NEWS (Mar. 15, 2015, 5:30 AM), http://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/ (arguing that companies do not absorb any substantial financial damages and that the majority of the damage is, instead, absorbed by the economy); *see also* Benjamin Deen, *Why Companies Have Little Incentive to Invest in Cybersecurity*, THE CONVERSATION (Mar. 4, 2015, 2:26 PM) (noting that target's total losses were only $105 million, approximately 0.1% of 2014 sales); DBIR 2015, *supra* note 3, at 63 (noting that "time to market" for software development is critical and is prioritized over security concerns); William Roberds & Stacey L. Schreft, *Data Breaches and Identity Theft*, FED. RES. BANK OF ATLANTA 24-31 (Sep. 2008) (Working Paper No. 2008-22), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1296131 (suggesting, through modeling, a steady-state imbalance between corporate liability and the cost of identity theft).

[47] *See* Robin Sidel, *Cost of Credit-Card Fraud Is Set to Shift*, WALL ST. J. (Sep. 29, 2015, 6:59 PM) (noting that, historically, credit-card issuers covered fraudulent transactions).

[48] *See, e.g.*, DBIR 2015, *supra* note 3, at 26 (cautioning that information-sharing is "less than optimal" and that understanding the "true effects" of proposed legislation is essential); *see also* Benjamin Dean, *Sorry Consumers, Companies Have Little Incentive to Invest in Better Cybersecurity*, QUARTZ (Mar. 05, 2015), http://qz.com/356274/cybersecurity-breaches-hurt-consumers-companies-not-so-much/ (suggesting that governments may prioritize intelligence gathering over data security, creating incentives to maintain vulnerabilities).

[49] *See generally* Press Release, Fed. Trade Comm'n, *Enforcing Privacy Promises*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (listing FTC enforcement actions). After a data breach occurs, many companies will offer credit monitoring and identity theft protection services to those affected for a specified period. Jamie White, *Retailers Offer Free Credit Monitoring, ID Theft Protection*, LIFELOCK (Jan. 30, 2014). https://www.lifelock.com/education/retailers-offering-free-credit-monitoring-id-theft-protection/. But these victims are often re-victimized by these very credit-monitoring services, who disregard basic safeguards for data security. *See* Press Release, Fed. Trade Comm'n, Lifelock to Pay $100 million to Consumers to Settle FTC Charges it Violated 2010 Order (Dec. 17, 2015) (noting that Lifelock failed to meet basic security standards by establishing and maintaining an information security plan). Ironically, Lifelock was given the contract to monitor OPM data breach victims. Jennifer van der Kleut, *White House Awards Contract for Identity Theft Protection for Millions of Victims of OPM Data Breach*, LIFELOCK (Sep. 4, 2015).

B. Standing and HRIT pre-Clapper

Data-breach victims alleging a HRIT have historically faced various standing thresholds, with modern standing inquiry arguably being more stringent on imminent injuries. Prior to *Clapper*, the circuits split on whether HRIT was a sufficiently imminent injury for standing purposes, with the Ninth and Seventh Circuits saying yes and the Third Circuit saying no.[50] In doing so, The Ninth and Seventh Circuits used more lenient thresholds, while the Third Circuit required that imminent injuries be "certainly impending."[51]

1. Modern standing law and imminent injuries

Article III limits federal courts' jurisdiction to "cases" and "controversies."[52] This constitutional floor to jurisdiction has been described as standing law.[53] However, the requirements for constitutional standing have expanded and contracted over time.[54] Historically, standing law required a plaintiff to have, at the very least, a "personal stake in the outcome of the

---

[50] *See infra* Part I.B.2.

[51] *See infra* Part I.B.2.

[52] Lujan v. Defenders of Wildlife, 504 U.S. 555, 559-60 (1992). The Constitution limits courts to the exercise of "strictly judicial" powers. *See* Muskrat v. United States, 219 U.S. 346, 355-57 (1911) (noting that the judicial power "implies the existence of present or possible adverse parties, whose contentions are submitted to the court for adjudication") (quoting *In re* Pac. Ry. Comm'n, 32 Fed. 241, 255).

[53] *See Lujan*, *supra* note 53, at 560 (noting that the standing requirement exists partially because the court's jurisdiction is constitutionally limited to "cases" and "controversies"). The Court acknowledges that the "cases" and "controversies" requirement, as articulated through standing law, is vague, so the Court often compares prior case law with a current case-in-question. *See also* Allen v. Wright, 468 U.S. 737, 750-52 (1984) ("the standing inquiry requires careful judicial examination of a complaint's allegations."). There are, however, general guidelines in many cases. *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377, 1386 (2014) (holding that Article III standing generally precludes third-party lawsuits, lawsuits raising generalized issues that are better resolved by other branches, and lawsuits that fall outside the "zone-of-interests" under the particular law it seeks relief from).

[54] *See*, *e.g.*, Whitmore v. Arkansas, 495 U.S. 149, 155 (1990) (acknowledging that the Court does not have a consistent and complete definition for Article III standing); Valley Forge Christian Coll. v. Ams.' United for Separation of Church and State, Inc., 454 U.S. 464, 471 (1982) (noting vagueness in "whether particular features [of standing are] required by Art[icle] III *ex proprio vigore,* or whether" they are self-imposed).

controversy."[55] But after *Lujan v. Defenders of Wildlife*, [56] the modern "irreducible constitutional minimum" for standing is more stringent;[57] a plaintiff must demonstrate an (1) "injury-in-fact"[58] that is (2) "fairly . . . trace[able]" to the defendant's actions[59] and (3) is likely to be "redressed by a favorable decision."[60] *Lujan* also holds that the "injury-in-fact" must be "concrete and particularized" and "actual or imminent, not 'conjectural' or 'hypothetical'"[61]

Contemporary standing law has tied its Article III purposes to the separation-of-powers; to this extent, standing prevents the courts from encroaching on the political branches.[62] A deeply rooted implication of separation-of-powers doctrine and standing law is that Article III prohibits advisory opinions.[63] There are also prudential reasons for standing law.[64]

---

[55] Baker v. Carr, 369 U.S. 186, 204 (1962); *see* United States v. Richardson, 418 U.S. 166, 181 (1974) (Powell, J. concurring) (reemphasizing the requirement for "a personal stake" as the "controlling definition" for constitutional standing).
[56] 504 U.S. 555 (1992).
[57] *Id.* at 560.
[58] *Id.* The three-pronged test solidified from the Court's opinion in *Allen*, 468 U.S. 737, 751 (1984) (holding that personal injury, traceability, and redressability are the core constitutional components of standing), which borrowed from *Valley Forge Christian Coll.*, *supra* note 55, at 472 (holding that an "actual or threatened injury," traceability, and redressability is an "irreducible minimum").
[59] *Lujan*, *supra* note 53, at 560-61 (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41-42 (1976)).
[60] *Id.* at 560 (quoting *Simon*, *supra* note 60, at 38).
[61] *Id.* (quoting *Whitmore*, *supra* note 55, at 155).
[62] *See* Ariz. State Legis. v. Ariz. Indep. Redistricting Comm'n, 135 S. Ct. 2652, 2695 (2015) (Scalia, J. dissenting) (discussing separation-of-powers and standing law); *see also Muskrat*, *supra* note 53, at 352-56 (1911) (discussing various holdings emphasizing that federal-court jurisdiction is limited to 'cases' by the Constitution and cannot be expanded by the legislature); *see also Allen*, *supra* note 54, at 752 (1984) ("[S]tanding is built on a single basic idea – the idea of separation of powers."); F. Andrew Hessick, *Probabilistic Standing*, 106 NW. U.L. REV. 55, 85-86 (2012) [hereinafter *Probabilistic Standing*] (noting that "separation-of-powers . . . has significantly influenced standing doctrine"). The *Lujan* standing requirements incorporate both Article III and separation-of-powers concerns. *Lexmark*, *supra* note 54, at 1386.
[63] *See Muskrat*, *supra* note 53, at 357-58 (acknowledging that Marbury v. Madison precludes advisory opinions).
[64] *See Lexmark*, *supra* note 54, at 1386 (noting "prudential," non-Article III standing generally bars third-party lawsuits, lawsuits raising generalized issues that are better resolved by other branches, and lawsuits falling outside the "zone-of-interests" under the particular law it seeks relief from); *see also Valley Forge Christian Coll.*, *supra* note 55, at 473-75 (1982) (noting "prudential principles" where plaintiffs must "generally assert [their] own legal rights and interests" (quoting Warth v. Seldin, 422 U.S. 490, 499 (1975)); Sierra Club v. Morton, 405 U.S.

Although Article III requires a concrete and particularized injury, it need not have already occurred; an imminent or threatened injury is sufficient.[65] But "fear-based" and heightened-risk cases are an emerging field post-*Lujan's* imminent-injury requirements.[66] Because this area creates situations where an alleged injury may not occur, some courts are reluctant to find standing.[67] Yet, all courts have made exceptions for sufficiently imminent injuries, reasoning that "plaintiffs should not have to wait for an injury to occur before seeking a remedy."[68] But the circuits have split over *how* "imminent" an injury should be to satisfy Article III standing requirements.[69]

2. *Pisciotta*, *Krottner*, and *Reilly*, the three Pre-*Clapper* HRIT circuit cases

Prior to *Clapper*, there were three similar circuit cases involving HRIT: the Seventh and Ninth Circuits found standing for data-breach victims in both *Pisciotta v. Old National Bancorp*[70] and *Krottner v. Starbucks*,[71] while the

727, 731-32 (1972) (requiring that the Plaintiff have a "personal stake in the outcome of the controversy," (quoting Baker v. Carr, 369 U.S. 186, 204 (1962)).

[65] *See* Massachusetts v. Mellon, 262 U.S. 447, 488 (1923) (holding that a plaintiff has a sufficient injury when she demonstrates that she is "immediately in danger of" a direct injury from a statutes' operation).

[66] *See generally* Brian Calabrese, Note, *Fear-Based Standing: Cognizing an Injury-in-Fact*, 68 WASH. & LEE L. REV. 1445, 1447-51, 1464-72 (2011) (noting that heightened risk or "anticipatory harm" is a subset of fear-based injury).

[67] *See Probabilistic Standing*, *supra* note 62, at 61-65 (acknowledging the Court's concerns about expanding its powers under imminent injuries but pointing out that the courts have traditionally "exercise[ed] jurisdiction over claims for prospective relief."); *see also* Diana R. H. Winters, *False Certainty: Judicial Forcing of the Quantification of Risk*, 85 TEMP. L. REV. 315, 337 (2013) (noting the D.C. Circuit's concerns about expanding the courts' role by allowing "increased-risk claims" (quoting Pub. Citizen, Inc. v. Nat'l Traffic Highway Safety Admin., 489 F.3d 1279, 1295 (D.C. Cir. 2007))).

[68] *See* Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2343 (2014) (holding that plaintiffs facing a "credible threat" need not wait for "prosecution" before "seeking relief" (quoting Holder v. Humanitarian Law Project, 561 U.S. 1, 15 (2010)).

[69] *See*, *e.g.*, *Winters*, *supra* note 67, at 335-46 (comparing the Second Circuit's and D.C. Circuit's standards for imminent injuries). The Supreme Court recognizes that imminence is a "somewhat elastic concept." *Clapper*, *supra* note 10, at 1147 (quoting Lujan, *supra* note 53, at 565 n.2).

[70] 499 F.3d 629 (7th Cir. 2007).

[71] 638 F.3d. 1139 (9th Cir. 2010).

Third Circuit denied standing in *Reilly v. Ceridian Corp.*[72] Whether a HRIT was sufficiently imminent for standing depended on the different thresholds each circuit applied.

Pisciotta, decided in 2007, was the first Seventh Circuit case discussing whether a HRIT is a sufficiently imminent injury; although the Seventh Circuit held that the Plaintiffs did have Article III standing, it nonetheless concluded that the Plaintiffs failed to state any "compensable injury" under Indiana law.[73] Old National Bancorp's (ONB's) servers were breached by an external actor, who stole bank-applicant information, including "name[s], address[es], [SSNs], driver's license number[s], [birthdays], mother's maiden name[s], and credit card" numbers.[74] The court found that the "intrusion was sophisticated, intentional, and malicious."[75] And ONB notified its customers of the breach.[76] After obtaining credit-monitoring services to protect themselves, ONB's customers sued in district court, alleging ONB was negligent and breached their contract.[77] The district court dismissed for lack of a cognizable injury under Indiana law because none of the Plaintiffs could show instances of financial loss or identity theft.[78]

The Seventh Circuit reversed on the standing issue, but it affirmed the district court's holding that Indiana law would not permit credit-monitoring services as a compensable injury.[79] The Seventh Circuit held that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the

---

[72] 664 F.3d 38 (3d Cir. 2011).
[73] *Pisciotta*, *supra* note 71, at 633-35, 640.
[74] *Pisciotta*, *supra* note 71, at 631-32.
[75] *Id.* at 632.
[76] *Id.*
[77] *Id.*
[78] *Id.* at 633-34 (noting that the district court "relied on several cases from other district courts . . . conclud[ing] that the federal courts lack jurisdiction because plaintiffs whose data has been compromised, but not yet misused, have not suffered an injury-in-fact . . .").
[79] *Pisciotta*, *supra* note 71, at 633-34.

plaintiff would have otherwise faced, absent the defendant's actions."[80] Consequently, the Seventh Circuit concluded that the Plaintiffs' HRIT met the constitutional burden.[81]

Similarly, *Krottner*, decided in 2010, was the Ninth Circuit's first opportunity to consider the same issue, and the Ninth Circuit, borrowing from *Pisciotta*, held that the Plaintiffs had stated a sufficiently imminent injury.[82] This case did not involve a malicious hacker; rather, it involved an opportunist who stole a Starbucks laptop containing "unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees."[83] Starbucks notified its employees of the theft and provided free credit monitoring for all affected employees for a fixed term.[84] Several employees sued Starbucks, alleging negligence and breach of contract for the loss of their PII.[85] Although the district court held that the employees had alleged a sufficiently imminent injury, it dismissed for a lack of a "cognizable injury under Washington law."[86] The Ninth Circuit affirmed and held that a

---

[80] *See id.* at 634, 638-39 (comparing HRIT with other types of heightened-risk cases, such as medical monitoring and toxic tort liability, where courts have found a sufficiently imminent injury. The similarity between other types of heightened-risk cases and data-breach cases has been extensively argued as a basis for granting standing); Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. L. REV. 1365, 1387-96 (2013) (arguing that data- breach cases are "analogous" to classic-tort cases involving imminent harm from toxic exposure, defective medical devices, and environmental damage); *but see Reilly*, *supra* note 73, at 44-46 (distinguishing toxic exposure, defective-medical device, and environmental damage cases because they often involve human health (as opposed to economic) and cannot often be resolved entirely through "monetary compensation"); Galaria v. Nationwide Mutual Ins. Co., 998 F. Supp.2d 646, 656 (S.D. Ohio 2014) (distinguishing medical monitoring cases).

[81] *Pisciotta*, *supra* note 71, at 633-34.

[82] Krottner, supra note 72, at 1142-43.

[83] *Id.* at 1140.

[84] *Id.* at 1140-41.

[85] *Id.* at 1141.

[86] *Id.* at 1141. The Plaintiffs in *Krottner* ran into the same problem as *Pisciotta* because they did not allege a cognizable injury under state law. *See Pisciotta*, supra note 71, at 639-40 ("Plaintiffs have not come forward with a single case or statute [allowing credit monitoring costs] from any jurisdiction, authorizing the kind of action they now ask . . . to recognize . . . under Indiana law"); *Krottner*, *supra* note 72, at 131 ("Under Washington law, '[a]ctual loss or damage is an essential element . . . [and] [t]he mere danger of future harm . . . will not support a negligence action.'" (quoting Gazija v. Nicholas Jerns Co., 543 P.2d 338, 341 (Wash. 1975) (en banc)); *but see* Lone Star Nat'l Bank v. Heartland Payment Sys., 729 F.3d 421, 423, 425-26 (5th Cir. 2013) (holding that the economic loss doctrine did not bar recovery in tort under New Jersey law

HRIT is a sufficient injury for standing because a "threatened injury constitutes injury in fact."[87]

In contrast, the Third Circuit decided, in *Reilly,* that a HRIT alone was too "speculative" to be a sufficient injury.[88] Like ONB, "Ceridian's Powerpay system" was breached, giving the attacker access to "first name[s], last name[s], social security number[s] . . . birth dates[s] and/or … bank account [information]."[89] The victims sued Ceridian for "an increased risk of identity theft," relying on *Pisciotta's* and *Krottner's* holdings.[90] However, the district court held that HRIT, alone, was insufficient injury for standing purposes; and even if it was, the Plaintiffs still had no cognizable injury under state law.[91]

The Third Circuit affirmed on appeal, holding that the Constitution requires an imminent injury be "certainly impending," and a HRIT is a "possible future injury" that is "too speculative" to be "certainly impending."[92] Furthermore, the Third Circuit found that the Plaintiffs' injury rested on a series of "ifs," making the claim "attenuated."[93] Also, the Third Circuit held that an injury is unlikely to be "certainly impending" when it rests

---

when the Defendant could reasonably foresee that card issuers would be injured by its failure to secure payment-card transactions).

87 *Krottner*, *supra* note 72, at 1142.

88 *Reilly*, *supra* note 73, at 46. *Clapper* seems to borrow heavily from *Reilly's* reasoning since they both apply the "certainly impending" standard. Both rest heavily on *Whitmore v. Arkansas*. *See infra* Part I.E.1.

89 *Reilly*, *supra* note 73, at 40.

90 *Id.* at 40, 44.

91 *Id.* at 40-41.

92 *Id.* at 42-43 (quoting *Whitmore*, *supra* note 55, at 158).

93 *See Reilly*, *supra* note 73, at 43 ("we cannot now describe how Appellants will be injured .in this case .without beginning our explanation with the word 'if': *if* the hacker read, copied, and understood the hacked information...and *if* the hacker attempts to use the information, and *if* he does so successfully, . . .only then will Appellants have suffered an injury."). For the "if test," the Third Circuit cited, *Storino v. Point Pleasant Beach*, 322 F.3d 293 (3d Cir. 2003). In *Storino* the owners of a "rooming house" in the Point Pleasant Boroughs challenged the constitutionality of a recently passed zoning ordinance that prohibited "rooming/boarding" use. Despite acknowledging that New Jersey provides "vested" properties with the right to continuing "non-conforming" uses, the owners argued that the ordinance would eventually harm them because it would deprive them of their current uses. *Id.* at 297. The court held that the alleged injury was "conjectural" because it required an "if" condition. *Id.* at 297-98.

on "future actions of an unknown third-party."[94] Specifically, the Third Circuit held that the hacker's intent was unknowable, so the Plaintiffs in *Reilly* fell even shorter than *Lujan's* Plaintiffs.[95]

The Third Circuit also distinguished both *Pisciotta* and *Knotter,* noting that both cases considered more "immediate" risks and that both cases simply analogized and did not discuss the constitutional threshold for imminent injuries.[96] As the Third Circuit noted, it was undisputed in *Pisciotta* that the hack was "sophisticated, intentional, malicious,"[97] also there were already identity theft attempts in *Krottner.*[98] Furthermore, the Third Circuit rejected the defective medical device and toxic exposure analogies advanced by both cases because, unlike identity theft, those harms "had undoubtedly occurred."[99] Moreover, environmental-damage cases could not always be resolved by monetary compensation.[100] Ultimately, the Third Circuit concluded that *Pisciotta* and *Krottner* did not follow the "certainly impending" standard for imminent injuries and, thus, were not persuasive.[101]

C. Four standards for imminent injury and two from the Clapper majority

The Supreme Court introduced several thresholds for imminence.[102] *Clapper*, the most recent case, introduced four distinct thresholds for *how*

---

[94] *See Reilly*, *supra* note 73, at 42 (observing that the Plaintiffs in *Lujan* had "control" over whether the injury was sufficiently "imminent" because "all [they] needed to do was [state an intention to] travel to the site").
[95] *See id.* at 42 (concluding that Plaintiffs' injury was "even more speculative than those . . . in *Lujan*").
[96] *See id.* at 43-44 (noting that the *Pisciotta* court did not discuss the "certainly impending" threshold and how it relates to data-breach cases).
[97] *Id.* at 43-44 (quoting *Pisciotta, supra* note 71, at 632.
[98] *Id.*
[99] *See id.* at 44-46 (noting that the victims in toxic-exposure cases have the immediate concern of preventing further harm to their health).
[100] *Id. at 44-45.*
[101] *See id.* at 44 (describing *Krottner's* and *Pisciotta's* rationale as "skimpy").
[102] *See* Andrew C. Sand, Note, Standing Uncertainty: An Expected-Value Standard for Fear-Based Injury in *Clapper v. Amnesty International USA*, 113 MICH. L. REV. 711, 712-15, 726-33 (2015) (arguing that *Clapper* created three separately different standards for injury-in-fact).

imminent an injury must be. Specifically, the Court rejected the Second Circuit's "objective reasonable likelihood" threshold,[103] reemphasized the "certainly impending" threshold,[104] and acknowledged the "substantial risk" threshold.[105] Alternatively, the dissent argued for a "reasonable probability" threshold.[106] Yet, *Clapper* left lower courts wondering whether the "certainly impending" threshold only applies to surveillance cases and whether the "substantial risk" threshold would be used.

1. The district court finds no present or future injury

A coalition of human-rights attorneys and organizations challenged the constitutionality of Section 702 of the 1978 Foreign Intelligence Surveillance Act (FISA), arguing that the authorization of warrantless government surveillance on foreign nationals overseas violated their First and Fourth Amendment rights.[107] The Plaintiffs alleged an imminent injury because they had an "actual and well-founded" fear (or there was a "realistic danger") that

---

[103] *Clapper, supra* note 10, at 1147.
[104] *Id.* at 1147-48.
[105] *Id.* at n.5.
[106] *See id.* at 1160-65 (Breyer, J. dissenting) (rejecting the certainly impending as an absolute floor to standing and arguing that the court has used lower thresholds for granting standing, concluding that the constitutionally required threshold is something closer to "reasonable probability" or "high probability").
[107] Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633, 634-35 (S.D.N.Y. 2009) *rev'd sub. nom.*, Amnesty Int'l USA v. Clapper, 638 F.3d 118, 119 (2d Cir. 2011) *rev'd and rem.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013). Section 702 was added to the 1978 FISA by Section 101(a)(2) of the 2008 FISA Amendments Act (FAA). *Id.* at 634; 50 U.S.C. § 1881(a)1881a (2015). Section 702 allows warrantless interception and collection of communications by non-U.S. persons residing outside of the United States when either exigent circumstances exist or by a favorable finding by the Foreign Intelligence Surveillance Court (FISC). 50 U.S.C. § 1881(a)1881a (2015); *see McConnell*, 646 F. Supp.2d at 635-41 (describing surveillance procedures under Section 702); *see generally* EDWARD C. LIU, CONG. RESEARCH SERV., R42725, REAUTHORIZATION OF THE FISA AMENDMENTS ACT (2013) (discussing the impacts of section 702). Section 702 is particularly controversial because the government does not need to show probable cause or "specify the nature and location" of the surveillance. *Clapper*, *supra* note 10, at 1144.

their confidential communications with their clients would be monitored under Section 702.[108]

The district court held that the Plaintiffs lacked standing because their surveillance fears were "abstract."[109] Specifically, the district court found that Section 702 did not actually target the Plaintiffs and that it was "completely speculative" whether the government would surveille the Plaintiffs' communication.[110] Furthermore, the district court noted that its conclusion was consistent with those in previous monitoring cases, which all similarly held that the fear was speculative without specific language targeting a plaintiff.[111]

2. The Second Circuit finds standing using an "objectively reasonable likelihood" threshold

The Second Circuit reversed, holding that Plaintiffs had standing because there was an "objectively reasonable likelihood" that Section 702 would target their communications.[112] Relying on the Court's rationale in *City of Los Angeles v. Lyons*,[113] the Second Circuit held that a plaintiff can "obtain

---

[108] *See McConnell*, *supra* note 108, at n.12 (hinting there is little difference between the Second Circuit's "actual and well-founded fear" and "realistic danger" tests except that the former is only used when analyzing First Amendment challenges).
[109] *Id.* at 645.
[110] *Id.*
[111] *See id.* at 645-47 (discussing United Presbyterian Church in the U.S v. Reagan, 738 F.2d 1375 (D.C. Cir. 1984) and Am. Civil Liberties Union v. Nat'l Sec. Agency, 493, 403 F.3d 644 (6th Cir. 2007) and noting that both monitoring cases required the Plaintiffs to be specifically targeted for there to be standing).
[112] Amnesty Int'l USA v. Clapper, 638 F.3d 118, 134-39 (2d Cir. 2011) *rev'd and rem*, Amnesty Int'l USA v. Clapper, 133 S. Ct. 1134 (2013). The Second Circuit avoided opining on whether the required threshold was different when a plaintiff claims avoidance costs against a future injury versus when a plaintiff only claims a future injury. *Id.* at 134. Consequently, the Second Circuit analyzed both the Plaintiffs' present-injury and future-injury under a reasonable likelihood standard. *Id.* at 135. But the Second Circuit hints that standing for present injuries based on future-anticipated harm requires a lower threshold. *Id.* at 135 n.17 ("[W]e do not suggest that actual present injuries may only be traced to governmental action when the causal connection is as strong as the likelihood of injury required to base standing on contingent future harms.").
[113] 461 U.S. 95 (1983).

standing" when they allege facts showing a "sufficient likelihood of future injury."[114] Moreover, the Second Circuit emphasized that the likelihood inquiry was "qualitative, not quantitative"[115] and that "the risk of that harm need not be particularly high."[116]

Applying the threshold to the Plaintiffs' future injury, the Second Circuit found a reasonable likelihood that Plaintiffs' communications with their clients would be monitored under Section 702.[117] In finding an objectively reasonable likelihood, the Second Circuit noted that intelligence agencies would likely use Section 702 authorities.[118] Additionally, the Second Circuit agreed that the Plaintiffs' clients were the type of individuals that Section 702 aimed to monitor.[119] Consequently, the Plaintiffs had standing because their fear of future monitoring was "reasonably likely to occur".[120]

3. The *Clapper* Court emphasizes the "certainly impending" threshold and acknowledges a "substantial risk" threshold

The Supreme Court rejected the "objectively reasonable likelihood" threshold for imminent injuries as too permissive.[121] Instead, the Court reemphasized that imminent injuries must be "certainly impending"[122] and held that the Plaintiffs' alleged future and present injuries fell far short of that threshold.[123] Additionally, the Court held that the Plaintiffs' claims failed to

---

[114] *Clapper*, *supra* note 108, at 135-36; *see Lyons*, *supra* note 114, at 107 n.8 (emphasizing that the threat's "*reality*" determines standing, "not the plaintiff's subjective apprehensions").
[115] *Clapper*, *supra* note 108, at 137 (quoting Baur v. Veneman, 352 F.3d 625, 637 (2d Cir. 2003)).
[116] *Id.* at 137 (citing Massachusetts v. EPA, 549 U.S. 497, 525 n. 23 (2007)). The Second Circuit further held that the "totality of the circumstances" governed reasonability, and that the probability threshold "varies with the severity of the . . . harm." *Id.* at 137-38 (quoting *Baur*, *supra* note 116, at 637).
[117] *Id.* at 138-40.
[118] *Id.* at 138.
[119] *Id.* at 138-39.
[120] *Id.* at 140.
[121] Clapper, *supra* note 10, at 1143, 1147.
[122] *Id.* at 1143, 1147.
[123] *Id.* at 1143.

even meet the "substantial risk" standard because their claim was too attenuated.[124] Finally, the Court held that, since Plaintiffs' fear was speculative, their avoidance costs could not create standing.[125]

Like *Reilly*, the Court emphasized that an injury must be "*certainly impending*" for Article III standing.[126] And the "certainly impending" threshold does not allow for "[a]llegations of *possible* future injury."[127] Moreover, injuries that rest on "speculative fear[s]" or a "highly attenuated chain of possibilities" are not sufficiently imminent under the "certainly impending" threshold.[128]

As applied, the Court held that the Plaintiffs' future injury was speculative because they could not show that their communications would be imminently targeted.[129] Furthermore, the Court held that even if the Plaintiffs' communications were targeted, their injury was still speculative because it rested on a "highly attenuated chain of possibilities."[130] Specifically, the chain started with a government decision to target the communications of foreign contacts with whom the Plaintiffs' communicate under Section 702 authority and ended with a successful interception.[131] Also, the Court agreed with the Plaintiffs' analysis that Section 702 "at most *authorizes* – but does not *mandate* or *direct*" surveillance against Plaintiffs.[132] Thus, since the Plaintiffs' fear of

---

[124] *Id.* at 1150, n.5.
[125] *Id.* at 1150-52.
[126] *Id.* at 1147.
[127] *Clapper*, *supra* note 10 (quoting Whitmore, *supra* note 55, at 158).
[128] *Id.* at 1148.
[129] *See id.* at 1148-49 (noting further that the Plaintiffs failed to allege that their communications were even brought to a Foreign Intelligence Surveillance Court (FISC) for approval).
[130] *Id.* at 1148, 1150.
[131] *See id.* at 1148 The Court raises concerns about Plaintiffs' theory because there is a string of probabilities from targeting to collection, where the interception fails, an alternate authority is used, or the interception does not include Plaintiffs' communication with the client. *Id.*; *accord Reilly*, *supra* note 73, at 42 (holding that the Plaintiffs did not have standing because their claim of future injury required that the hacker successfully collect their personal information, intend to commit crimes with such information, and actually be able to use it to the detriment of the Plaintiffs).
[132] *Id.* at 1149.

injury was highly speculative, the Court found that the future injury failed to meet the stringent "certainly impending" threshold.[133]

In explaining the "certainly impending" threshold, the Court's implied that the threshold precluded probabilistic analysis for imminent injuries.[134] However, the Court acknowledged that it had previously found standing for some injuries using a "substantial risk" threshold.[135] But in doing so, the Court neither reaffirmed nor defined the threshold.[136] Yet, the Court held that the Plaintiffs failed to meet the "substantial risk" threshold because their claim was highly attenuated.[137]

4. The *Clapper* dissent argues the right balance is between a "high" and a "reasonable probability"

The *Clapper* dissent disagreed with the majority that "certainly impending" was the constitutional threshold and argued, instead, that the Plaintiffs had a "high likelihood" of being surveilled under Section 702.[138] Justice Breyer argued that the standing threshold is "elastic," ranging from a fair probability to a certainly impending threshold.[139] For instance, the Court found standing for "probabilistic injuries" – something less than certainty.[140]

---

[133] *Clapper*, *supra* note 10, at 1150.
[134] *See id.* at 1147-48 (noting that Plaintiffs' "fail[ure] to offer any evidence that their communications have been monitored . . . substantially undermines their standing theory"). By requiring evidence of interception and holding that injury theories requiring "if" statements speculative, the Court implies that the injury must be literally certain. *See infra* part II.B.1.
[135] *Id.* at 1150 n.5. The D.C. Circuit's substantial risk test relies on probability determinations; specifically, it examines whether an alleged injury has a substantial chance of occurring. *See infra* part II.B.3.
[136] *See id.* The Court affirms the "substantial risk" threshold a year later in *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). But the Court has not provided definitive guidance on when "substantial risk" applies. *See* Bradford C. Mank, *Clapper v. Amnesty International: Two or Three Competing Philosophies of Standing Law?* 81 TENN. L. REV. 211, 268-69 (2014) (noting lower courts' confusion about when to apply "substantial risk" analysis).
[137] *Clapper*, *supra* note 10, at 1150 n.5.
[138] *Clapper*, *supra* note 10, at 1157-58, 1160-61 (Breyer, J. dissenting).
[139] *See id.* at 1160 (recognizing that "imminence" is an "elastic concept" (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 565 n.2 (1992)).
[140] *See id.* at 1160-61 (noting that the court has allowed standing, in many case, on "probabilistic injuries" and emphasizing that "certainly" should not "literally define[] . . . impending").

In *Monsanto Co. v. Geertson Seed Farms*[141] found standing on a "substantial risk" of injury.[142] Thus, imminent injuries do not require "literal certainty," only a sufficient likelihood of occurrence.[143] Thus, Justice Breyer argued that the constitutional threshold was closer to a "'high probability' or 'reasonable probability.'"[144]

When determining that the Plaintiffs had a "high likelihood" of being surveilled, Justice Breyer pointed to several factors that raised the likelihood of Plaintiffs being harmed under Section 702.[145] He noted that the "Government has a strong *motive* to listen to" these ongoing discussions,[146] and that the Government has previously intercepted similar types of communications.[147] Taking in these factors as a whole, Justice Breyer concluded that Plaintiffs' fear was not "speculative."[148]

D. District courts disagree as to whether HRIT injuries are precluded under Clapper

After *Clapper*, data-breach litigation has increased as more companies are compelled by state laws to report any exposure or loss of PII.[149] Different district courts resolving such cases have reached two conflicting conclusions from *Clapper, Pisciotta, Knotter,* and *Reilly*: the first is that *Clapper* now requires a

---

141 561 U.S. 139 (2010).
142 *Id.* at 1160-63 (quoting *Monsanto Co.*, *supra* note 142, at 153); *see, e.g., id.* at 1161 (noting that the Court in Blum v. Yaretsky, 457 U.S. 991 (1982), found standing when nursing home residents faced a "sufficiently substantial" risk of being transferred to a "less desirable home" under a new regulation (quoting *Blum*, 457 U.S. at 999-1001).
143 *Id.* at 1160, 1162. 1165.
144 *See id.* at 1165 (arguing the Courts deny standing when an injury is "*less* likely" to occur). Substantial risk could be akin to high probability of occurrence and objectively reasonable likelihood could be likened to a mere possibility of occurrence. *Compare* notes 112-116 and accompanying text (discussing the Second Circuit's test) *with* notes 296-301 and accompanying text (discussing D.C. Circuit's substantial risk test).
145 *Id.* at 1157, 1159 ("The upshot is that (1) similarity of content, (2) strong motives, (3) prior behavior, and (4) capacity all point to a very strong likelihood the Government will intercept...at least some of the . . .plaintiffs' communications.").
146 *Id.* at 1158.
147 *Id.*
148 *Id.* at 1160.
149 *See* DAVID ZETOONY ET AL., 2015, DATA BREACH LITIGATION REPORT 4 (2015) (showing that the number of class action complaint filings over an eighteen-month period has grown).

higher threshold for imminent injuries, in all cases and, consequently, older circuit opinions no longer control;[150] the second is that *Clapper* can be reconciled with previous cases because either (a) *Clapper* only emphasized heightened scrutiny for government surveillance[151] or (b) *Clapper* acknowledged the "substantial risk" threshold and, therefore, did not foreclose probabilistic future-injuries.[152]

Many courts consistently hold that *Clapper* forecloses all HRIT cases by rejecting the "objectively reasonable likelihood" test and by emphasizing that "possible future injur[ies]" are insufficient for Article III standing.[153] For instance, the court in *In re Science Applications International Corporation (SAIC) Backup Tape Data Theft Litigation* interpreted the "certainly impending" threshold to bar risk-based (probabilistic) analysis, holding that the "degree by which the risk of harm has increased is irrelevant."[154] Similarly, other courts do not consider the amount or sensitivity of the information stolen, the intent of the hacker (to the extent it is known), or whether anyone in the class had

---

[150] *See In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25-26, 28 (D.D.C. 2014) (noting that *Clapper* rejected the "objectively reasonable likelihood" threshold and holding that *Clapper* has overruled pre-*Clapper* circuit opinions using lower thresholds for imminent injuries).

[151] *See In re* Sony Gaming Networks, 996 F. Supp.3d 2d 943, 960-63 (S.D. Cal. 2014) (holding that *Clapper* "reiterated an already well-established framework" and that victims can still sue under a theory of heightened risk when their personal information is wrongfully disclosed).

[152] *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1211-16 (N.D. Cal. 2014) (holding that *Clapper* did not change standing law and that injuries causing a "substantial risk" of harm are still allowed).

[153] *Clapper*, *supra* note 10, at 1147; *see Peters*, *supra* note 11, at 855 (holding that under *Clapper,* an increased risk of harm from data breaches, alone, does make an injury "certainly impending"); *see also Storm*, *supra* note 11, at 364-68 (noting that even if the identity-theft risk was "likely or probable," it would still fail to meet the certainly-impending threshold); *see also* Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 875-79 (N.D. Ill. 2014) ("*Clapper* compels rejection . . . that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing."); *In re* Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588, at *2, *5 (N.D. Ill. Sep. 3, 2013) ("the increased risk of identity theft is insufficient to convey standing . . . .").

[154] *See In re SAIC*, *supra* note 151, at 25 (responding to the Plaintiffs' assertion that they are "9.5 times more likely . . . to become victims of identity theft"); *but see* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 654 (S.D. Ohio 2014) ("An injury can hardly be said to be 'certainly impending' if there is less than a [twenty] percent chance of it occurring.").

already suffered identity theft.[155] However in other instances, the courts have quantified the "certainly impending" threshold by requiring that the probability of harm rise to a particular level before it finds a sufficiently imminent injury.[156]

In denying standing under the "certainly impending" threshold, many courts apply *Reilly's* and *Clapper's* "if test" to HRIT cases.[157] Specifically, the injury is speculative under the "certainly impending" threshold when it requires an 'if' condition to be satisfied.[158] For instance, in a data-breach case, a future injury occurs only "*if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information and *if* he does so successfully."[159] Since many data-breach victims cannot demonstrate an identity theft without using the word "if," many courts have found their injury speculative.[160] Additionally, the courts have also expressed concerns about the uncertainty of the hacker's actions as an "independent third party," as noted in both *Reilly* and *Clapper*.[161] Because the court cannot

---

155 *See Peters*, *supra* note 11, at 856 (noting that *Clapper* resolved the circuit split from *Knotter*, *Pisciotta*, and *Reilly*, and denied Plaintiffs standing even though there were some instances of attempted identity theft); *In re Barnes & Noble*, 2013 WL 4759588 at *2, *5 (declining to grant standing even though there was instance of identity theft).

156 *See Galaria*, *supra* note 155, 654 (requiring at a least twenty percent chance of occurring).

157 *See infra* notes 281-289 and accompanying text; *see also* Green v. eBay Inc., CIV.A. No. 14-1688,. 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) (noting that whether the Plaintiff suffers an injury "depends on numerous variables"); *Peters*, *supra* note 11, at 854 (noting the Plaintiff "cannot describe [her] injurie[s] without . . . the word 'if." (quoting Storino v. Point Pleasant Beach, 322 F.3d 293, 298 (3d. Cir. 2003))); *Storm*, *supra* note 11, at 365 (discussing *Reilly's* "if" test and applying it to a data breach case); *cf. In re Horizon Healthcare Services, Inc. Data Breach Litig.*, CIV.A. No. 13–7418, 2015 WL 1472483, at *6 (D.N.J. Mar. 31, 2015) *appeal field* (noting *Reilly's* holding that physical theft (as opposed to intrusion) creates an even more attenuated injury because the abilities of the "crook" to take advantage of the theft are unknown).

158 *Clapper*, *supra* note 10, at 1148 (2013); *Reilly*, *supra* note 73, at 43.

159 *Reilly*, *supra* note 73, at 43.

160 *Storm*, *supra* note 11, at 365.

161 *See Clapper*, *supra* note 10, at 1150, 1164 n.5 (declining to support standing when injuries rely on "independent actors"); *Lujan*, *supra* note 53, at 562 (noting the court's reluctance to find standing when the "asserted injury arises from the government's . . . regulation . . . of *someone else*" who is not "before the courts" because the courts cannot "control" or "predict" their actions); *Reilly*, *supra* note 73, at 42 (noting that the injury "is dependent on entirely speculative, future actions of an unknown third-party"); *See In re* SAIC, *supra* note 151, at 25-26 ("Courts . . . are reluctant to grant standing where the alleged future injury depends on . . .the actions of. an independent party.").

find an injury without first assuming that the hacker, thief, or other actor will have the knowledge and the will to exploit the stolen information, the court relying on *Clapper* and/or *Reilly* will find no standing.[162] The reasoning behind the court's reluctance for standing when the injury depends on third-party actions is also a basis for distinguishing analogies to medical devices, toxic exposure, and environmental damage.[163]

On the other hand, other courts disagree that *Clapper* found Article III standing under a HRIT by relying on previous circuit holdings and distinguishing *Clapper* because *Clapper* the constitutionality of surveillance law and, thus, did not change standing law.[164] To some extent, this is because *Clapper* partially relied on *Laird v. Tatum*.[165] Consequently, there were conflicting views about how far *Laird*'s holding went in framing what kinds of "fear-based injur[ies]" or imminent injuries are acceptable.[166] Because *Clapper* relies partially on *Laird*'s holdings, there is reasonable confusion as to whether *Clapper*'s interpretation of a stringent "certainly impending" standard for imminent injuries is more specific towards surveillance law, or whether it covers all cases concerning imminent injury.[167] This premise is further

---

[162] *See In re Horizon Healthcare Services*, 2015 WL 1472483 at *6 (holding that injures depending on a "third party bandit" are "inadequate" for Article III standing); *see* also *Galaria*, *supra* note 155, at 655 (holding that the Plaintiffs' future injury is speculative because it depends on third-party actors); Polanco v. Omnicell, Inc. 988 F. Supp. 2d 451, 466-67 (D.N.J. 2013) (discussing *Reilly* and assumed third-party actions).

[163] *See supra* note 99 and accompanying text.

[164] *See In re Adobe Sys., supra* note 153, at 1211-14 (N.D. Cal. 2014) (declining to adopt Adobe's argument that *Clapper* "intended a wide reaching revision" of standing and noting that the circumstances in *Clapper* were more sensitive because they concerned whether the government had violated the Constitution); Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *3-5 (N.D. Ill. Jul. 14, 2014) (disagreeing that *Clapper* overruled *Pisciotta* and noting that *Driehaus* upholds a lower standing threshold); *In re* Sony Gaming Networks and Customer Data Sec. Litig., 996 F. Supp. 2d 942, 961-62 (S.D. Cal. 2014) (holding that *Krottner* and *Clapper* can be reconciled because "real and immediate" and "certainly impending" are essentially the same standard).

[165] 92 S. Ct. 2318, 2321-23 (1972). *Laird* also concerned surveillance law.

[166] *See Sand*, *supra* note 102, at 716-21 (discussing *Laird* and arguing that three interpretations of *Laird* emerged on the Supreme Court).

[167] *See Clapper*, *supra* note 10 at 1152 (discussing *Laird*); John L. Jacobus & Benjamin B. Watson, *Clapper v. Amnesty International and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?* 21 RICH. J.L. & TECH. 3, 5, 48-51, 81 (2014) (noting that courts remain split on *Clapper*'s implication in data-breach cases); *see also Moyer*, *supra* note 165, at *6 (distinguishing

supported by *Clapper*'s language, holding that the court is wary of granting standing where intelligence and "foreign affairs" are involved.[168]

Some courts acknowledge that *Clapper* reemphasized the stringent "certainly impending" threshold for imminent injuries, but note *Clapper*'s willingness to accept some imminent injuries where there is a "substantial risk" of harm. And these courts analyze data-breach cases under both standards with various outcomes.[169] However, other courts acknowledge a "substantial risk" threshold but do not offer any discussion on how the threshold affects a Plaintiffs' HRIT case.[170] Still other courts, like the court in *SAIC*, have quantified the "substantial risk" threshold of harm because eighty percent of the victims may not experience identity theft.[171]

One crucial discriminating factor that district courts do look to when finding standing is whether some victims, within a class, have *already* experienced successful or attempted identity theft.[172] Other courts consider the time between the lawsuit and the actual breach, arguing that the longer a victim goes without experiencing any attempted or actual identity theft, the

---

Clapper to "national security and constitutional issues"); *Strautins*, *supra* note 154, at at 878 n.11 (noting that the court makes closer examinations of standing when Plaintiffs challenge actions "by the Legislative or Executive branches of government").

168 *Clapper*, *supra* note 10 at 1147.

169 *See Remijas*, *supra* note 12, at 693-694 (arguing the Supreme Court did not "jettison" the "substantial risk"' standard); *see also In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 956-57 (D. Nev. 2015) (noting that "substantial risk" and *Krottner*'s standard for imminent injury are the same); *In re SAIC*, 45 F. Supp. 3d at 25-26 (noting that a Plaintiff can plead a sufficient risk if the "risk of harm" is "substantial); *Moyer*, *supra* note 165, at *4, *5 (relying on the "substantial risk" standard to find standing).

170 *See* Enslin v. Coca-Cola Co., 136 F. Supp. 3d 654, 663-65 (E.D. Pa. 2015) (acknowledging the "substantial risk" standard but granting standing based on previous instances of identity theft); *Strautins*, *supra* note 154, at 876, 876 n.8 (acknowledging "substantial risk" but, nevertheless, holding that Plaintiffs do not meet the "certainly impending" threshold); *In re Barnes & Noble*, *supra* note 156, at *3, *5 (acknowledging "substantial risk" as a standard but holding that an "increased risk of identity theft" is not enough for standing).

171 *In re SAIC*, *supra* note 151, at 26 (holding that the probability is insufficient to meet the D.C. Circuit's requirement that there is "(i) a substantially increased risk of harm and (ii) *a substantial probability of harm* with that increase taken into account" (quoting Public Citizen, Inc. v. Nat'l Highway Traffic Safety Admin., 489 F.3d 1279, 1295 (D.C. Cir. 2007)).

172 *See Enslin*, *supra* note 171, at 664-65 (distinguishing *Reilly* and *Clapper* because the Plaintiff had to spend "time, effort, and money" to mitigate actual identity theft); *In re SAIC*, *supra* note 151, at 33-34 (allowing two of thirty-three identity theft cases to proceed because they alleged actual injury).

less likely she has a sufficiently "immediate" injury.[173] There are, yet, other courts that distinguish between the sophisticated hacker and the physical thief, arguing that it is more plausible that a sophisticated hacker can successfully exploit the PII.[174] Also, on the administrative side, the courts have supported federal agencies' claims on mere allegations that a data breach could potentially cause millions of dollars in loss from fraud and identity theft.[175]

E. Remijas recognizes that previous and subsequent Supreme Court cases have not consistently applied Clapper's "certainly impending" threshold.

The *Clapper* decision created confusion amongst the circuits about how far its heightened threshold went in other contexts. There were several major points of confusion. First, the "certainly impending" standard was never uniformly applied in every case. Second, many previous and subsequent cases had found standing on lower thresholds that did not focus on immediacy and certainty. Third, the *Driehaus* Court reaffirmed that "substantial risk" threshold for determining standing was valid. Consequently, the *Remijas* Court recognized these discrepancies and found standing for HRIT victims on the "substantial risk" standing. In doing so, the *Remijas* Court reminded courts not to "overread" *Clapper*.

---

[173] *See Remijas*, *supra* note 170, at 693 (disagreeing that the Plaintiffs claim to standing falls as "more time passes between a data breach and an instance of identity theft" (quoting *In re Adobe*, 66 F. Supp. 3d at 1215, n.5)); *In re Zappos*, *supra* note 170, at 957-59 (noting that Plaintiffs claim that injury was imminent may have been credible in 2012, but cannot confer standing after "three-and-a-half-years" pass without actual evidence of identity theft).

[174] *See In re Adobe Sys.*, *supra* note 153, at 1215-16 (rhetorically questioning why a sophisticated hacker would "target and steal" personal information "if not to misuse it").

[175] FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 622-24 (D.N.J. 2014).

1. *Whitmore v. Arkansas* establishes the "certainly impending" threshold for imminent injuries

In *Clapper*, Justice Breyer noted in his dissent that "'imminence' is . . . a somewhat elastic concept." [176] Along those lines, Justice Breyer correctly noted that in *Clapper* the "certainly impending" language was not always used as a constitutionally minimum threshold.[177] The Court in *Whitmore v. Arkansas*[178] transformed the "certainly impending" requirement from a *sufficient* threshold to a *necessary* condition.[179]

After *Whitmore*, the language changed to require "[a] threatened injury must be '"certainly impending."'"[180] From there, the "certainly impending" threshold later appeared in *Lujan*, where Justice Scalia explicitly relates the standard to a time dimension and the certainty of injury.[181] From *Lujan* and *Whitmore*, the "certainly impending" threshold became the requirement for the *Clapper* Plaintiffs.[182]

---

[176] *Clapper*, *supra* note 10, at 1160 (Breyer, J. dissenting).
[177] *Id.*
[178] 495 U.S. 149 (1990).
[179] *Clapper*, 133 S. Ct. at 1160; *see Whitmore*, 495 U.S. at 158 ("A threatened injury must be "certainly impending"' to constitute injury in fact" (quoting Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979))). But *Pennsylvania v. West Virginia*, which was quoted in *Babbitt*, used "certainly impending" as a sufficient standard, not a necessary one. *See* Pennsylvania v. West Virginia, 262 U.S. 554, 593–95 (1923) (noting if the harm "is certainly impending, that is enough"). A review of cases prior to *Whitmore* used the sufficient standard. Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979); Blanchette v. Conn. Gen. Ins. Corps., 419 U.S. 102, 143 (1974).
[180] *Id.* at 158 (quoting *Babbitt*, 442 U.S. at 298).
[181] *See* Lujan v. Defenders of Wildlife, 504 U.S. 553, 566 n.2 (1992) (holding that the imminence requirement is exceptionally important when the "acts necessary to make the injury happen are at least partly within the plaintiff's own control" to prevent the courts from deciding cases without an injury-in-fact). Justice Scalia also emphasized that "imminence" is not limited to situations where an injury is dependent on a third-party actor. *Id.*
[182] *See supra* Part I.C.3. and accompanying notes.

2. Prior Supreme Court cases have applied lower thresholds in different contexts

Although the Court insisted that imminent injuries must meet the "certainly impending" threshold, the Court has previously found standing under lower thresholds. For instance, cases involving environmental regulation or First Amendment challenges have not invoked the "certainly impending" threshold.

The Court has found standing where a party is at "substantial risk" of falling within the scope of an allegedly unconstitutional criminal statute and does not require an inevitable conflict between a statute's operation and a party's activity.[183] For instance, the Court found standing in *Babbitt v. United Farm Workers National Union*[184] when there was a "realistic danger" that United Farm Workers (UFW) would face prosecution under a state statute that made it unlawful to use "dishonest, untruthful, and deceptive publicity" when influencing agricultural consumers.[185] And where there is a "credible threat," a plaintiff "should not be required to await and undergo a criminal prosecution as the sole means of seeking relief."[186]

The Court has also applied "substantial risk" thresholds when deciding environmental regulatory challenges. For instance, the Court granted standing in *Massachusetts v. EPA*,[187] holding that the EPA's "refusal to regulate greenhouse gas emissions"[188] created both an "'actual' and [an] 'imminent'"

---

[183] *See* Steffel v. Thompson, 415 U.S. 452, 459 (1974) ("[I]t is not necessary that petitioner first expose himself to actual arrest or prosecution to be entitled to challenge a statute that he claims deters the exercise of his constitutional rights.").
[184] 442 U.S. 289 (1979).
[185] *See id.* at 297–99, 301–02 (quoting Ariz. Rev. Stat. Ann. § 23-1385(B)(8) (2016)) (finding standing when a plaintiffs' fear of prosecution is not "imaginary or wholly speculative," even if the "criminal penalty provision . . . may never be applied").
[186] *Id.* at 298 (quoting Doe v. Bolton, 410 U.S. 179, 188 (1973)).
[187] 549 U.S. 497 (2007).
[188] *Id.* at 521. The Court creates some ambiguity within the standing issue by holding that Massachusetts has "special solicitude." *See id.* at 520 (emphasizing that "States are not normal litigants [when] invoking federal jurisdiction" (quoting Georgia v. Tennessee Copper Co., 206 U.S. 230, 237 (1907); *Id.* at 518.

injury to the Plaintiffs.[189] The EPA had interpreted that "air pollutants," within the meaning of Clean Air Act, did not include motor- vehicle carbon emissions, so the agency had no authority to regulate it.[190] Conversely, Massachusetts argued that if the EPA did not regulate "greenhouse gas emissions," the sea level could rise and potentially damage coastal lands.[191] The Court agreed, pointing to "objective and independent assessment[s]"[192] concluding that greenhouses gases have already caused "significant harms."[193] The Court also acknowledged testimony that "[fourteen] acres of land per miles of coastline" could be lost "by [the year] 2100."[194] Thus, the Court concluded that Massachusetts had a "remote" risk of "catastrophic" injury, which is sufficient for Article III standing.[195]

Another example is *Monsanto Co. v. Geertson Seed Farms* where the Court found standing when Geertson sued the Animal and Plant Health Inspection Service (APIHS) when it failed to conduct an environmental impact assessment prior to deregulating genetically engineered alfalfa seeds, as required by the 1969 National Environmental Policy Act.[196] Geertson argued that by failing to issue an Environmental Impact Statement (EIS), there was high risk that non-modified alfalfa seeds would be contaminated by genetically modified seeds, and conventional famers would have to raise prices to cover for testing and contamination control.[197] The district court

---

[189] *Id.* at 521 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).
[190] *See id.* at 521, 528 (noting EPA's conclusion that "climate change was so important" it could not "address it" without some explicit guidance from Congress).
[191] *Id.* at 499.
[192] *Id.* at 521 (quoting Control of Emissions From New Highway Vehicles and Engines, 68 Fed. Reg. 52922-02, 52930 (Sept. 8, 2003)).
[193] *Id.* at 521.
[194] *Id.* at 523 n.20.
[195] *Id.* at 526. The Court, at least in this case, supported two additional theories. The first is that "even a small probability of injury . . . create[s] a case or controversy." *Id.* at 525 n.23 (quoting Village of Elk Grove v. Evans, 997 F.2d 328, 329 (7th Cir. 1993)). The second theory is that the more severe an alleged future injury could be, the less likely it needs to be for standing purposes. *Id.* (citing Mountain States Legal Foundation v. Glickman, 92 F.3d 1228, 1234 (D.C. Cir. 1996)).
[196] 561 U.S. 139, 144, 153 (2010).
[197] *Id.* at 153–56.

held there was a "reasonable probability" of contamination, and the Supreme Court affirmed, holding that there was a "significant" or "substantial risk of gene flow" to non-modified alfalfa.[198] In doing so, the Court acknowledged that Geertson's expenses to avoid contamination were reasonable.[199]

3. *Driehaus* reaffirms the "substantial risk" test as a valid threshold for imminent injuries

Although the Court had arguably left the question of whether "substantial risk" was still a valid threshold, it reaffirmed the "substantial risk" test in *Susan B. Anthony List v. Driehaus*.[200] In *Driehaus*, the Court held that Susan B. Anthony List (SBAL), an anti-abortion advocacy group, had standing to challenge an Ohio statute criminalizing "false statement[s]" about the "voting record of a candidate or public official" during any "nomination or election" campaign.[201] SBAL had publically accused a congressional candidate, Driehaus, of voting for the Affordable Care Act (ACA), which "includes taxpayer-funded abortion."[202] In response, Driehaus went to the Ohio Elections Commission, which investigated whether SBAL had made false statements about his voting record.[203] Consequently, SBAL challenged the

---

[198] *See id.* at 141, 151–52 (rejecting the argument that there was no imminent injury because there was no way of knowing how the environmental impact analysis would turn out).
[199] *See id.* at 154–55 (noting that the additional costs to test crops is a valid injury "even if their crops are not actually infected").
[200] 134 S. Ct. 2334 (2014).
[201] *Id.* at 2338 (quoting OHIO REV. CODE ANN. § 3517.21(B) (Lexis 2013)). Ohio's statute allowed anyone with "personal knowledge" to "file a complaint with the Ohio Elections Commission." *Id.* (citing OHIO REV. CODE ANN. § 3517.153(A) (Lexis Supp. 2014)). Once a complaint was filed, the Commission would create a panel and hold a hearing to determine whether there was probable cause of a violation. *Id.* (citing OHIO REV. CODE ANN. §§ 3517.156(B)(1), (C) (Lexis 2013)). If there was probable cause, the full Commission held a more extensive hearing, and if there was "clear and convincing evidence" of a violation, the Commission was required to either "refer the matter to the relevant county prosecutor" or "issue a reprimand." *Id.* at 2339 (quoting OHIO REV. CODE ANN. §§ 3517.155(D)(1) (2) (Lexis Supp. 2014)) (citing OHIO ADMIN. CODE 3517-1-10(E) (2008); § 3517-1-14(D)).
[202] *Driehaus*, 134 S. Ct. at 2339 (citing Susan B. Anthony List v. Driehaus, 525 Fed. Appx. 415, 416 (6th Cir. 2013) (unreported) *rev'd*, *Driehaus*, 134 S. Ct.).
[203] *Id.*

statute as a violation of the First and Fourteenth Amendments.[204] But before anything could proceed, Driehaus lost the election and withdrew his SBAL complaint.[205] Still, SBAL moved forward with its constitutional claim, arguing that the statute "chill[s]" First Amendment speech because SBAL intends to operate similarly in the future, and that modus operand would likely trigger the statute's criminal provisions.[206] But the district court dismissed for a lack of concrete injury.[207] And the Sixth Circuit affirmed, holding there is no imminent injury because SBAL did not have any "plans to lie . . . in the future."[208]

The Supreme Court reversed and agreed with SBAL and COAST, holding that both organizations faced an imminent injury.[209] The Court found standing on three points: (1) SBAL's expressed intent to continue activities that would likely trigger the statute;[210] (2) the added threat of

---

[204] *Id.* at 2339–40. The SBAL suit alleged that the Ohio statute is unconstitutional on its face and as-applied. *Id.* at 2340. There have been a number of First Amendment challenges under a theory that the statute "chills" free speech because the statute is overbroad; the courts have been more willing to grant standing in these cases. *See* Richard H. Fallon, Jr., *As-Applied and Facial Challenges and Third-Party Standing*, 113 HARV. L. REV. 1321, 1321–22 (2000) (noting that the courts will allow facial challenges, involving the First Amendment, when the statute has "too many unconstitutional applications" and that the courts are sensitive about this doctrine because it bypasses traditional third-party standing rules). For non-First Amendment overbreadth challenges, the court has been fairly restrictive on facial challenges. *See* United States v. Salerno, 481 U.S. 739, 746 (1987) (holding that, outside of First Amendment challenges, overbreadth challenges require a showing that the statute is unconstitutional in *every* case); *see also* Marc E. Isserles, *Overcoming Overbreadth: Facial Challenges and the Valid Rule Requirement*, 48 AM. U.L. REV. 359, 360–67 (1998) (discussing overbreadth facial challenges and *Salerno*). *But see* Richard H. Fallon, Jr., *Fact and Fiction About Facial Challenges*, 99 CAL. L. REV. 915 (2011) (arguing that in many Supreme Court terms, facial challenges had a higher success rate than as-applied challenges).

[205] *See Driehaus*, 134 S. Ct. at 2340 (noting that SBAL adjusted its pleading to a theory of imminent injury, arguing that it faces future financial burdens in defending itself should another complaint arise under the statute); *see also* Susan B. Anthony List v. Driehaus, Nos. 11-3894, 11-3925, 2013 WL 1942821, at *3 (6th Cir. May 13, 2013) (noting that there was no "final decision" on SBAL).

[206] *Driehaus*, 134 S. Ct. at 2340.

[207] *Id.*

[208] *Id.* at 2340–41 (quoting *Driehaus*, 2013 WL 1942821, at *7).

[209] *Id.* at 2347.

[210] *Id.* at 2343–44.

criminal prosecution;[211] and that (3) the "threat of future enforcement . . . [was] substantial."[212]

The court relied on *Babbitt*[213] and held that SBAL's expressed intent to continue discussing candidates' voting records fell within the statute's scope.[214] Moreover, the Court found that, in addition to "administrative action," both organizations faced criminal prosecution from the statute's operation, and this layered threat created a sufficiently imminent injury.[215] More importantly, the Court found that the "threat of future enforcement of the false statement statute is substantial."[216] In doing so, the Court made a direct comparison to *Clapper* and noted that the Commission's probable-cause finding implies past enforcement, which is "good evidence that the threat . . . is not 'chimerical.'"[217]

---

[211] *Id.* at 2346.
[212] *Id.* at 2345.
[213] *See* Babbitt v. United Farm Workers, 442 U.S. 289, 298 (1979) ("When the plaintiff has alleged an intention to engage in a course of conduct arguably affected with a constitutional interest, but proscribed by a statute, there exists a credible threat of prosecution [and] he 'should not be required to await and undergo a criminal prosecution as the sole means of seeking relief.'" (quoting Doe v. Bolton, 410 U.S. 179, 188 (1973))).
[214] *Driehaus*, 134 S. Ct. at 2343–45.
[215] *Id.* at 2345–46. For standing under a threatened prosecution theory, the plaintiff must show that her behavior will likely lead to criminal prosecution under a challenged statute; it is not enough that the plaintiff is pleading a possible future injury based on "[p]ast exposure to illegal conduct" that does not have "present adverse effects." *See* O'Shea v. Littleton, 414 U.S. 488, 495–97 (1974) (noting a lack of any "allegations that any relevant criminal statute . . . is unconstitutional"). This slightly distinguishes pre-enforcement challenges with heightened risk arguments. *See* Calabrese, *supra* note 67, at 1460–71 (distinguishing "pre-enforcement fear" and "anticipatory harm); *compare* Los Angeles v. Lyons, 461 U.S. 95, 105(1983) (denying standing to challenge anticipatory fear of police chokeholds because it was speculative that it could happen again) *with* Holder v. Humanitarian Law Project, 561 U.S. 1, 14–16 (2010) (granting standing in a pre-enforcement challenge when a statute outlawed assisting certain organizations).
[216] *Driehaus*, 134 S. Ct. at 2345.
[217] *Id.* (quoting Steffel v. Thompson, 415 U.S. 452, 459 (1974). In *Steffel*, the Court found a sufficient injury-in-fact when Plaintiff challenged a Georgia statute prohibiting "handbilling" after he was told by police on two different occasions that he would be arrested if he continued to handbill at a shopping center, and after his associate was actually arrested. *Steffel*, 415 U.S. at 454–56, 459, 471–72.

4. The *Remijas* Court finds standing for HRIT victims under the "substantial risk" standard

Remijas is the first circuit court case on standing in HRIT post-*Clapper*.[218] The Seventh Circuit found standing for Neiman Marcus breach victims, reversing the District Court's judgment and holding that *Clapper* did not foreclose HRIT cases under the "substantial risk" threshold.[219] Additionally, *Remijas* cautioned that *Clapper* should not be "overread" to have changed standing law.[220] Specifically, *Remijas* distinguished *Clapper* on its facts, noting that the Court did not find standing because the Plaintiffs claims were highly attenuated in that specific case.[221]

Neiman Marcus announced on January 23, 2014 that its servers were breached by malware.[222] The malware had allowed attackers to skim nearly 1.1 million payment cards between July 16 and October 30, 2013, more than six months prior.[223] Immediately following the attack, many Neiman Marcus customers reported credit-card fraud.[224]

Shortly afterwards, Neiman Marcus reported another successful second attack on January 29, 2016, where hackers used brute-force[225] attempts to

---

218 794 F.3d 688 (7th Cir. 2015).
219 *Id.* at 696–97.
220 *Id.* at 694.
221 *Id.* at 693.
222 Byron Acohido, *Timeline: Target, Neiman Marcus Disclosures*, USA TODAY (Feb. 6, 2014, 11:33 AM), http://www.usatoday.com/story/cybertruth/2014/01/23/timeline-target-neiman-marcus-disclosures/4799153/.)
223 *Id.* The disclosure occurred shortly after an outside security analyst had suspected a breach. Brian Krebs, *Hackers Steal Card Data from Neiman Marcus*, KREBS ON SECURITY (Jan. 10, 2014, 6:56 PM), https://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus; *see* Lily Hay Newman, *A 17-Year Old Was Behind the Target, Neiman Marcus Credit Card Hacks*, SLATE (Jan. 20, 2014, 1:30 PM), http://www.slate.com/blogs/future_tense/2014/01/20/target_neiman_marcus_credit_card_number_hacks_were_caused_by_a_17_year_old.html) (noting that the timing of Neiman Marcus' disclosure was controversial).
224 Tracy Kitten, *Neiman Marcus Reports New Breach*, BANK INFO SECURITY (Feb. 4, 2016). http://www.bankinfosecurity.com/new-neiman-marcus-breach-authentication-must-change-a-8843.
225 Brute Force is a basic technique where an attacker randomly guesses a targets' username and password to gain access. *See* MILES TRACY ET AL., NAT'L INST. OF SCI. & TECH., DEPT. OF COMMERCE, SPECIAL PUB. 800-44, VERSION 2, GUIDELINES ON SECURING PUBLIC WEB

access 5,200 accounts. Neiman Marcus reported that there were nearly seventy successful breaches with subsequent fraudulent purchases.

The victims sued Neiman Marcus under "negligence, breach of implied contract . . . unfair and deceptive business practices," and other common law tort theories.[226] The district court acknowledged that some 9,200 payment cards belonging to 350,000 customers were fraudulently used.[227] Although the District Court used the "certainly impending" threshold, it distinguished *Clapper's* analysis as "especially rigorous" because it implicated national security and constitutional issues.[228] Instead, the District Court reconciled *Pisciotta* and *Clapper* by holding that the line between imminent and speculative injury was confirmed data theft.[229] But this did not save the plaintiffs' case because they did not have a HRIT, only a risk for future fraudulent charges.[230] And fraudulent charges is not sufficiently "concrete" because the victims were reimbursed for the fraudulent transactions.[231]

The Seventh Circuit reversed, holding that all 350,000 class members had standing at the pleading stage.[232] The Seventh Circuit held that probabilistic injuries, such as HRIT, were still allowed under the "substantial risk" threshold.[233] The Seventh Circuit further held that HRIT victims "should not

---

SERVERS 7-12, 7-13 (2007) (defining brute force attacks). Even though the technique is time-tested, there are many ways to harden systems against brute-force attacks, and there was skepticism among some experts as to whether this was a brute-force attack. Kitten, *supra* note 224.

226 Remijas v. Neiman Marcus Grp., 2014 WL 4627893, No. 14 C 1735, *1 (N.D. Ill. Sep. 16, 2014) (unreported) *rev'd*, Remijas v. Neiman Marcus Grp., 794 F.3d 688 (7th Cir. 2015).

227 *Id.*

228 *Id.* at *2, *3

229 *See id.* at *3 (distinguishing various cases on the likelihood of data misuse).

230 *See id.* at *3–4 (acknowledging that the 350,000 victims may be at imminent risk of future fraudulent charges but holding that this translated to a "certainly impending risk of identity theft" was "a leap too far"). Although the District Court did not explain its rationale for drawing the distinction, it was probably discussing the differences between identity theft and identity fraud. *See* KRISTIN FINKLEA, CONG. RES. SERV., R40599, IDENTITY THEFT: TRENDS AND ISSUES 3 (2014) (describing identity theft as a specific form of identity fraud). This distinction may have been drawn because the only data exposed was credit card information. Acohido, *supra* note 222.

231 *Id. Remijas*, 2014 WL 4627893, at *3.

232 Remijas v. Neiman Marcus Grp., 794 F.3d 688, 690 (7th Cir. 2015).

233 *Id.* at 693 (noting "*Clapper's* recognition that a substantial risk will sometimes suffice" for standing).

have to wait [for] . . . credit-card fraud" to occur if there is an "'objectively reasonable likelihood'" of it occurring.[234] Finally, the Seventh Circuit raised concerns that requiring identity theft to actually occur before finding standing could create "more latitude" for defendants to argue traceability.[235]

As applied, the Seventh Circuit found a concrete injury in both the time required to resolve fraudulent transactions and the possibility of new-account fraud in the future.[236] The Seventh Circuit also recognized that "fraudulent use . . . may continue for years."[237] And emphasized that 9,200 accounts have already been stolen and experienced fraudulent charges.[238] Furthermore, the Seventh Circuit held that it was a reasonable inference that the hackers intended to commit credit-card and identity fraud.[239]

II. ANALYSIS

The Supreme Court emphasizes that an "actual" or "imminent" injury is the constitutional minimum to satisfy Article III's "case" or "controversy" requirement.[240] But even if the Constitution, in theory, mandates

---

[234] *Id.* (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)).
[235] *Id.* (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215, n.5 (N.D. Cal. 2014)). Many courts use the time element to show why a data-breach victim does not have any substantial risk of harm. *See, e.g.*, *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 108 F. Supp. 3d 949, 958 (D. Nev. 2015) ("Even if Plaintiffs' [HRIT] was substantial and immediate in 2012, the passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something.").
[236] *Remijas*, 794 F.3d at 692–93, 696.
[237] *Id.* at 694 (quoting U.S. GOVT'T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007)).
[238] *Id.* at 692.
[239] *See id.* at 693 ("Why else would hackers break into a store's database and steal consumers' private information?")
[240] *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013) (recognizing a "constitutional limitation of federal-court jurisdiction" to "cases" or "controversies") (quoting DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006)); O'Shea v. Littleton, 414 U.S. 488, 493, n.2 (1974) (A plaintiff "must show actual or threatened injury" for constitutional standing); R.S. v. D., 410 U.S. 614, 616–17 (1973) (noting that "federal plaintiffs must allege some threatened or actual injury" for standing).

a sufficient injury, it is silent on *how* imminent the injury must be.[241] Consequently, the Court has varied the threshold requirement when it contemplates the separation-of-powers doctrine and the severity of the potential.[242] More specifically, the Court has relaxed the standing threshold the more severe the injury and has heightened its standing requirements the more the separation-of-power concerns are present. The "certainly impending" threshold used in *Clapper* reflected both the Court's perspective that there were heightened separation-of-powers concerns in the Court interfering with national security and intelligence-related matters, and the Court's possible perspective Plaintiffs' did not face severe consequences flowing from government surveillance. Within this context, data-breach case victims raise little separation-of-powers concerns because it does neither affects, nor questions the constitutionality of, government activity. Furthermore, data-breach victims face a range of potential consequences, ranging from life-threatening discrepancies in their medical records to spending notable hours fixing fraudulent transactions.

Yet, many courts have applied the rigorous "certainly impending" standard to almost all post-*Clapper* cases of heightened risk, defending this practice as applying the constitutionally minimum threshold.[243] In doing so, those courts forget the primary purpose of standing law: the reluctance, of the courts, to decide whether the actions of the coordinate branches are constitutional without some certainty that a private injury would occur.[244] Thus, the courts should not apply such rigorous thresholds in HRIT cases. Instead, the courts should recognize the Supreme Court's willingness, both

---

[241] *Cf. Probabilistic Standing*, *supra* note 62, at 66–70 (arguing that Article III does not require the court to base standing on the probability that the harm will occur).
[242] *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 559, 560 (1992) (noting that although standing is "essential" to Article III, some of the elements are "merely prudential"); Flast v. Cohen, 392 U.S. 83, 97 (1968) (noting that the justiciability doctrine "has become a blend of constitutional requirements and policy considerations" and that the two are not "always clearly distinguished" (quoting Barrows v. Jackson, 346 U.S. 249, 255 (1953)).
[243] *See supra* Part I.D.
[244] *See supra* Part I.B.1.

pre- and post-*Clapper*, to consider probabilistic injuries under a "substantial risk" or "reasonably likely" threshold. And as part of a "substantial risk" analysis, courts should consider several risk factors within data breach cases that raise or lessen the chances that victims will face identity theft in the near future.

A. The Standing Threshold is Context-Specific; "Substantial Risk" is Used When the Separation of Powers Concerns is Low or the Severity of the Injury is High

Although the Supreme Court has expanded and restricted standing law over time, it has also applied standing law differently to different contexts.[245] First, the Court has emphasized that imminent harms must be "certainly impending," a stringent standard that has been applied to prevent the Court from interfering with the other political branches. Second, the Court has indicated some willingness to relax standing rules when the imminent harm is severe. Applying these two factors, the Court demands that an injury be "certainly impending" when there are heightened separation-of-powers concerns and the anticipated harm is not substantial. However, the Court should only require a plaintiff have a reasonable or "substantial" risk of injury when there are little separation-of-powers concerns and the anticipation harm is catastrophic. Data-breach lawsuits generally have little separation-of-powers concerns, but, depending on the circumstances, the consequences can range from financial to life-threatening issues.

---

[245] *See* F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORN. L. REV. 275, 275–90 (2008) [hereinafter *Standing and Private Rights*] (discussing the history of the Court's approach to standing law).

1. Separation-of-powers concerns abate when government activity is not involved

Modern and historical standing law reflects the Courts' reluctance to usurp the political branches by entertaining constitutional challenges to government actions without some certainty of a particularized injury.[246] But whether a case has heightened separation-of-powers concerns should turn on the type of issue, not on the likelihood of injury.[247] Otherwise stated, if standing law preserves the separation-of-powers, the imminence threshold would rise when a wide range of government activities are implicated.[248] But likewise, the imminence threshold should be relaxed where a case does not require a court to decide on the constitutionality of government activities. For instance, most data-breach victims sue on common-law tort claims, e.g. negligence or breach of contract, where the courts need not opine on a statutes' constitutionality. Conversely, the *Clapper* Court had to decide on the constitutionality of government surveillance within a national security framework. Even if, hypothetically, the likelihood of injury was similar in both cases, the data-breach cases would not have the same separation-of-powers concerns.

Taken to the extreme, the constitutional minimum for standing should be minimal when the courts are not required to decide on the constitutionality of legislation, regulation, or government action because there are no separation-

---

[246] *See, e.g.*, Ariz. State Legis. v. Ariz. Indep. Redistricting Comm'n, 135 S. Ct. 2652, 2695 (2015) (Scalia, J. dissenting) (arguing that standing doctrine is "built on a single basic idea – the idea of separation of powers"); Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013) (noting that constitutional standing is "built on separation-of-powers principles"); Laird v. Tatum, 408 U.S. 1, 15 (1972) (noting that it is Congress' responsibility, not the courts,' to rule on the "soundness of Executive action"); *see also Probabilistic Standing*, *supra* note 62, at 68–80 (discussing the historical basis for requiring imminent or threatened injuries to be at least "probable")

[247] Flast v. Cohen, 392 U.S. 83, 99–101 (1968).

[248] *See supra* note 246 and accompanying text; *cf.* Lujan v. Defenders of Wildlife, 504 U.S. 555, 564, n.2 (1992) (noting that the "certainly impending" threshold reduces the likelihood a Court would opine a case without injury). *But see Flast,* 392 U.S at 101 (emphasizing that it is "substantive issues . . . to [be] adjudicated" that creates the separation-of-powers concerns).

of-powers concerns.[249] The D.C. Circuit noted its concerns about "increased-risk" cases because "[m]uch *government regulation* slightly increases [the] risk of injury," and courts must, therefore, limit cases to those involving actual or imminent harm.[250] But if the D.C. Circuit is the correct, then the injury requirement, and arguably much of constitutional standing, rests on whether government action is being challenged. Anything more rests on more policy and prudential concerns, which are flexible.[251]

Within this framework, *Clapper,* at most, re-emphasized existing requirements *for plaintiffs who challenge government action on constitutional grounds,* objecting to these cases where lower courts apply an "objectively reasonable likelihood" standard.[252] Furthermore, a review of almost *every* subsequent Supreme Court case (after *Pennsylvania*) *explicitly* referencing the "certainly impending" standard involved a challenge to statute, regulation, or government action on constitutional grounds.[253] Also, *Clapper* emphasized

---

[249] *See* Golden v. Zwickler, 394 U.S. 103, 110 (1969) (holding that "constitutional question[s]" about congressional acts require a live controversy); *Flast*, 392 U.S. at 107 (Douglas, J. concurring) ("The case or controversy requirement comes into play *only* when the Federal Government does something . . . .") (emphasis added); *see also Flast,* 392 U.S. at 100–02 (per curium) (holding that the minimum requirement of Article III standing is that the plaintiff has "a personal stake in the outcome of the controversy" (quoting Baker v. Carr, 369 U.S. at 204) and that "the dispute touches upon 'the legal relations of parties having adverse legal interests'" (quoting Aetna Life Ins. Co. v. Haworth, 300 at 240–41)); Massachusetts v. Mellon, 262 U.S. 447, 488 (1923) (holding that "acts of Congress" are only reviewable on constitutional grounds when the party can show actual or threatened injury).

[250] Pub Citizen, Inc. v. Nat'l Highway Traffic Safety, Admin., 489 F.3d 1279, 1295 (D.C. Cir. 2007) (emphasis added).

[251] *See Probabilistic Standing*, *supra* note 62, at 91–92 (arguing that prudential rules help to advance many of the courts objectives, such as reducing "potential plaintiff" and ensuring that the issue is sharply presented for good resolution).

[252] *See Clapper*, 133 S. Ct. at 1146–49 (noting heightened scrutiny when passing on the constitutionality of government activities is inconsistent with the "objectively reasonable likelihood" test); Laird v. Tatum, 408 U.S. 1, 13 (1972) ("[T]o invoke the judicial power to determine the *validity of executive or legislative* action he must show that he . . . is immediately in danger of sustaining a direct injury) (emphasis added); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015) (cautioning courts not to "overread *Clapper*").

[253] *See*, *e.g.*, Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2338 (2014) (challenging Ohio statute on First Amendment grounds); *Clapper*, 133 S. Ct. at 1142 (challenging the constitutionality of government surveillance); DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 337–38 (2006) (declining to grant taxpayer standing when they challenged Ohio law providing tax credits); McConnell v. FEC, 540 U.S. 93, 224–26 (2003) (challenging an amendment to the 1934 Federal Communications Act) (overruled on other grounds); *Whitmore*, 495 U.S. at 151 (challenging constitutionality of a death penalty where defendant waives appeal); Pac. Gas and

that the standing threshold is "especially rigorous" when the court must decide on the constitutionality of federal government actions.[254] But when threatened injuries are premised on a private party's negligence, breach-of-contract, or other common law theory, not implicating any statute or government action, these concerns arguably abate.

Regardless, some imminent injury is required to satisfy Article III's case-or-controversy requirement,[255] but the courts should apply a lower threshold, e.g. "substantial" or "reasonable risk," when the government's role is de minimis. The threshold should vary with how much court's opinion impacts coordinate branches. This is directly related to the "certainly impending" threshold, which is intended to minimize the chances that the Court pass judgments where the injury is not immediate .[256] To this extent, consider a scenario where a private party alleges a federal statute is unconstitutional, either as-applied or on its face, because the statute will injure the party

---

Electr. Co. v. State Energy Res. Conservation & Dev. Comm'n, 461 U.S. 190, 198 (1983) (challenging California nuclear laws as preempted by federal regulation); *see also* Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 292–94 (1979) (challenging the constitutionality of an Arizona employment law); Blanchette v. Conn. Gen. Ins. Corps., 419 U.S. 102, 121–22 (1974) (challenging the Rail Act). But there are three notable environmental cases that are exceptions, including *Lujan*, where the plaintiffs (in those cases) challenged regulatory interpretations and administrative decisions; yet, the court used slightly different standards in some of these cases. *See* Massachusetts v. EPA, 549 U.S. 497, 504–05 (2007) (challenging EPA's non-regulation of greenhouse gases); Lujan v. Defenders of Wildlife, 504 U.S. 555, 557–59 (1992) (challenging Fish and Wildlife Service's interpretation of the 1973 Endangered Species Act); Friends of the Earth v. Laidlaw Env't Servs.' (TOC), Inc., 528 U.S. 167, 173–74 (2000) (discussing a citizen-suit under the Clean Water Act).

[254] *See Clapper*, 133 S. Ct. at 1147 ("[O]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional") (quoting Raines v. Byrd, 521 U.S. 811, 819–20 (1997)); Blum v. Holder, 744 F.3d 790, 795–99 (1st Cir. 2014) (arguing that *Clapper* makes the standing requirement more rigorous when the courts must decide whether actions that are taken by the other branches of federal government are constitutional).

[255] *See* R.S. v. D., 410 U.S. 616, 616–17, n.4 (1991) (noting a longstanding and consistent requirement that "federal plaintiffs must allege some threatened or injury"). *But see, e.g.*, *Standing and Private Rights*, *supra* note 245, at 279–90 (arguing there is no constitutional basis for an injury-in-fact requirement and that the injury requirement was first "developed . . . to expand standing").

[256] In theory, the more time that passes, the less of certainty that injury could occur. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 n.2 (1992) (describing imminence as the cornerstone of certainty).

between twenty-and-thirty years from now.[257] If the private party now sues, the court would need to decide the constitutionality of a statute or government action for a harm twenty years from now, which reflects the federal court's concern for separation of powers.[258] In contrast, consider a private party that sues because she is likely to sustain an injury, because of the actions (or inactions) of another party at some point, or continuously, over the next twenty years. In this case, there are far less concerns over the separation-of-powers doctrine because the court is merely resolving the legal rights of the parties without a high risk of making constitutional declarations.

2. The Court varies the threshold when considering an injury's severity

The Court has also varied the standing threshold based on the severity and types of injuries, effectively making the inquiry context based.[259] And the Court has never explicitly said that the *Clapper* standing threshold overruled any of the previous cases.[260] For example, the Court has allowed standing when a plaintiff is at "substantial risk" of coming under the threat of criminal penalties.[261] The Court has also related the severity of harm to the threshold

---

[257] *See, e.g.*, Addington v. U.S. Airline Pilots Ass'n, 606 F.3d 1174, 1185 (9th Cir. 2010) (Bybee, J., dissenting) (arguing that ripeness or an imminent injury "'coincides squarely with standing's injury' [requirement] [and is] 'standing on a timeline'" (quoting Stormans, Inc. v. Selecky, 586 F.3d 1109, 1122 (9th Cir. 2009)). Bybee's dissent argued that ripeness turns on whether there remain any "contingent future events" in the plaintiffs' theory of injury; and if there are no further contingencies, and the plaintiff would suffer hardship if judicial review was denied, then standing should be granted. *Addington*, 606 F.3d at 1187–88. Thus, in Bybee's conclusion, "certainly impending" is about the absence of contingencies, rather than the proximity in time. *Id.* This is similar to the "if" test. *See infra* notes 281–289 and accompanying text.

[258] Although there was no constitutional challenge to the Clean Air Act in *Massachusetts v. EPA*, Judge Roberts' dissent addressed these particular facts for a possible injury "*by the year 2100*." 549 U.S. 497, 542 (2007) (Roberts, C.J., dissenting).

[259] *See* Flast v. Cohen, 392 U.S. 83, 100–02 (1968) ("[I]n ruling on standing, it is both appropriate and necessary to look to the substantive issues").

[260] In fact, the Court still cites previous cases where they applied such exceptions. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013) (citing *Monsanto* and *Babbitt* as good law).

[261] *See* Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014); *see also supra* notes 183–186 and accompanying text.

inquiry, allowing for a relaxed likelihood when determining whether an injury is sufficiently imminent.[262]

Both *Babbit* and *Driehaus* were examples where the Court found standing, even though the threat of harm was not certain or immediate.[263] Both cases involved a plaintiff who faced a risk of criminal prosecution if they continued their allegedly protected activities.[264] In finding standing for both plaintiffs, the Court did not require that such harm be immediate, only that there was a reasonable likelihood of enforcement in the future.[265] The Court in *Driehaus* especially pointed to the risk of *criminal* prosecution as a basis for providing standing.[266] The Court in *Babbitt* came to similar conclusions.[267]

Similarly, the Court has implied that the likelihood inquires varies with the severity of the injury in *Massachusetts v. EPA* and *Monsanto*. For instance, the Court in *Massachusetts v EPA* pointed to the "catastrophic" nature of rising sea levels to justify standing even when the likelihood was "remote."[268] Likewise, the Court in *Monsanto* noted the "substantial risk" of "contamination" of "non-genetically-engineered alfalfa," but did not mandate that such harms be essentially immediate, a cornerstone of "certainly impending."[269] In doing so, the Court pointed to "significant environmental

---

[262] *See supra* notes 193–195, 215 and accompanying text. Most established risk-management practices mandate that a potential threat be analyzed from both their severity and probability of occurrence. Specifically, the risk is a function of both likelihood and severity. *See, e.g.*, DEP'T OF THE ARMY, TECHNIQUES PUB. ATP 5-19, RISK MANAGEMENT 1–7, Table 1.1 (2014) (noting that "catastrophic" harms that "seldom" occur are considered to be "high risk").
[263] *See Driehaus*, 134 S. Ct. at 2345 (noting that the "threat of future enforcement . . . is substantial"); *supra* notes 213–215 and accompanying text.
[264] *See supra* notes 183–186, 209–217 and accompanying text.
[265] *See Driehaus*, 134 S. Ct. at 2345–46 (noting the "substantial risk" of enforcement but falling short of noting that the risk is immediate); Babbit v. United Farm Workers Nat'l Union, 442 U.S. 289, 300, n.12 (1979) ("Challengers to election procedures often have been left without a remedy in regard to the most immediate election because the election is too far underway").
[266] *See Driehaus*, 134 S. Ct. at 2346 ("The burdensome Commission proceedings here are backed by the additional threat of criminal prosecution.").
[267] *See Babbitt*, 442 U.S. at 302 (holding that although the criminal provision "may never be applied," the Plaintiffs do not need to wait for prosecution to bring their challenge).
[268] Massachusetts v. EPA, 549 U.S. 497, 526 (2007).
[269] *See* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–56 (2010) (noting the various ways farmers would have to react to the possibility of contamination).

concern[s]" emanating from cross-contamination.[270] Also, the Court agreed that the Plaintiffs suffered an injury by expending cost to avoid the prospective risk of harm, *even when* they had not yet done so.[271]

This type of harm was also *Reilly's* basis for distinguishing between identity theft cases with toxic-exposure and defective-medical devices cases.[272] However, as discussed previously, many identity-theft victims face more than just financial losses, they can potentially face life-threatening or harmful issues when their medical records made inaccurate.[273] Depending on the type and amount of PII stolen, a data-breach victim faces a wide range of potential injuries, many being health-related.

These cases not only demonstrate the Court's willingness to make exceptions on the rigorous "certainly impending" standard, but the Court, in doing so, illustrates that the constitutional floor for imminent injuries is something less than "certainly impending."

B. The "Substantial Risk" Threshold Should Emphasize the Victim's Relative Risk in Heightened-Risk Injuries

The *Clapper* and *Driehaus* Courts have never described in detail *how* likely a harm must be to meet the "substantial risk" threshold. As discussed above, this is likely because the threshold is sensitive to separation-of-powers concerns and the severity of harm, which are context-specific. But some circuit and district courts have quantified the "substantial risk" threshold in various degrees. However, many such tests do little to account for the relative risk a victim faces. Specifically, the tests largely ignore the degree the

---

[270] *Id.* at 155–56.
[271] *See id.* at 153–54 (noting that measures farmers *would have to take* if the injunctions were lifted, but finding that such measures were injuries).
[272] *See* Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011) ("[S]tanding in medical-device and toxic-tort cases hinges on human health concerns); *see also supra* note 99 and accompanying text.
[273] *See supra* notes 30–35 and accompanying text.

victims' risk-profile changes by the defendant's actions. They should not. The "certainly impending" threshold covers the immediacy aspect, ignoring relative risk. To have any merit as a distinguishable test, the "substantial risk" threshold must.

1. The "certainly impending" threshold asks whether an injury will immediately occur, and not whether an injury will occur

Any imminent-injury theory should not require the injury to have already occurred or is because, otherwise, half of the "actual or imminent" requirement in *Lujan* would be meaningless.[274] It would also contradict *Clapper's* acknowledgement of a substantial risk threshold.[275] For instance, consider a breach victim alleging a HRIT, with identity theft being the ultimate injury; if the court forecloses any "possibility of future injury" and that must be certain to occur, then the probability is, essentially, one. And given that that the identity theft would be more properly characterized as an actual injury.[276] But many possibilities can become certainties over sufficient time: "On a long enough timeline, the survival rate for everyone will drop to zero."[277] Hypothetically, if an event, A, has a one-percent chance of occurring year-over-year, then, over a long enough period of time, the probability it will happen is one.[278] Similarly, if the same event A has a

---

[274] *See* Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) ("Allegations of possible future injury do not satisfy . . . Art[icle] III. A threatened injury must be 'certainly impending.'"). Many courts use *Whitmore*'s language to compel dismissal of HRIT claims. *See*, *e.g., In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 19, 24 (D.D.C. 2014) (dismissing most claims within the class for lack of ongoing identity theft). But, again, *Whitmore* used the "certainly impending" standard in deciding a case involving government activity. *Whitmore*, 495 U.S. at 151, 158.

[275] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150, n.5 (2013)

[276] *See In re SAIC*, 45 F. Supp. 3d 14, 28 (D.D.C. 2014) (holding that HRIT was not an injury under neither the certainly impending nor substantial risk threshold). The Court sought to root out class members that did not have a previous or ongoing identity theft attempt, but found actual injuries for members with previous identity theft attempts. *Id.* at 31–32.

[277] CHUCK PALAHNIUK, FIGHT CLUB 17 (1996).

[278] As proof: if event, A, has a 0.01 (or one percent) chance of occurring each year, then the chance that it does not occur in any particular year is 0.99 (or ninety-nine percent). Let *n* be

heightened risk of a nineteen percent chance of occurring in a year, then the likelihood (assuming the year-over-year risk is the same) that A would occur within eight years is eighty percent.[279] Consequently, any imminent injury theory cannot rest its threshold on a simple probability of occurrence; there should also be a time consideration.[280]

"Certainly impending" incorporates the time consideration discussed above and requires that an injury not only have a near certainty of occurring, but that the certainty occurs immediately.[281] In other words, it is not a question of whether; it is a question of when. And this often expressed by the "if test" in *Reilly* and *Clapper*: if a threatened or imminent injury cannot be described without using the word "if," or a series of "ifs," then the injury is speculative and too attenuated for Article III standing.[282] Thus, the harm must be essentially "certain" because a party cannot have any conditional statements attached to the alleged injury.[283] In other words, if a plaintiff requires that a conditional statement be satisfied to show injury, then the condition becomes an "if" within the "certainly impending" threshold.[284]

---

the number of years; as *n* approaches infinity, the probability (P) that A would not occur is characterized by $P(\sim A) = \lim_{n\to\infty} (0.99)^n = 0$. In other words, P(A) = 1.

[279] As proof: let P(A) = .19 for any year, then P(~A) = 1-P(A) = 1-0.19 = 0.81 for any year. Let *n* be the number of years required for P(A) to approach eighty percent, i.e. where $1 - P(\sim A)^n > 0.80$. $n > \frac{\log(0.2)}{\log(0.81)} = 7.64$ years.

[280] *Cf.* Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 n.2 (1992) (noting that "certainly impending" requires a "high degree of immediacy").

[281] *Id.*

[282] *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1157–58 (2013) (demonstrating the series of "ifs"). Though *Reilly* cites *Storino* as a basis for the "if test," the reasoning likely formulated from a reading of *Whitmore*, as it characterized the plaintiffs' pleading in *O'Shea* as a series of if statements. *See* Whitmore v. Arkansas, 495 U.S. 149, 157–58 (1990) ("*[I]f* respondents proceed to violate an unchallenged law and *if* they are charged . . . they will be subjected to discriminatory practices" (quoting O'Shea v. Littleton, 414 U.S. 488, 497 (1974))); Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d. Cir. 2011) (holding injuries speculative when "one cannot describe how the [plaintiffs] will be injured without beginning the explanation with the word 'if.'" (quoting Storino v. Pleasant Beach, 322 F.3d 293, 297–98 (3d Cir. 2003))).

[283] *See Clapper*, 133 S. Ct. at 1160 (Breyer, J. dissenting) (rejecting the premise that the Constitution requires imminent injuries to be "absolutely certain.").

[284] The D.C. Circuit has an alternative way of expressing the "certainty" within "certainly impending" by holding "future predictions" that "are not normally susceptible of labeling as 'true' or 'false'" as speculative. *See* United Transp. Union v. Interstate Commerce Comm'n, 891 F.2d 908, 912 (D.C. Cir. 1989) (holding that the court "reject[s] as overly speculative those

But even if the Court were to follow its own threshold for imminent injuries, then the outcome of subsequent cases to *Clapper* would be different. For instance, in *Driehaus*, SBAL could not claim the harm was "certainly impending" because there is no way it could construe the harm without using the word "if." Regardless of how SBAL constructs its theory of injury, it must *condition* it on a candidate (or other party) filing a complaint sometime in the future and on the commission panel finding probable cause; those *conditions* transform to "ifs" for the purposes of "certainly impending."[285] Consequently, the Court confers standing in *Driehaus* case on something less than "certainly impending."

Nevertheless, this construction makes sense as a heightened standard if the Court is concerned about separation-of-powers because it limits the Court from passing constitutional questions without an immediate injury.

2. Substantial risk tests should emphasize relative-risk injuries

If "certainly impending" occupies the immediate time dimension,[286] then substantial risk theory must turn on some other factor to have any meaning; and shown previously, it cannot simply be the probability of occurrence.[287] One possibility is that the substantial-risk test examines a conditions' strength or reasonableness, rather than its *existence*. For example, the Court in *Driehaus* could determine whether the condition "*if* a candidate files a complaint" is

links which are predictions of future events"). Under the above framework, a condition is speculative if there is uncertainty – not "true" or false" – in whether it will occur. It then follows that the "certainly impending" threshold requires an injury to be essentially certain to happen.

[285] *Id.*

[286] *See supra* note 181.

[287] There seems to be a difference. *Compare Clapper*, 133 S. Ct. at 1148 (essentially requiring that the Plaintiffs produce evidence of monitoring before granting standing) *with* Monsanto v. Geertson Seed Farms, 130 S. Ct. 2743, 2754–55 (2010) (requiring a showing that deregulation creates a substantial risk for cross-contamination).

substantially or reasonably likely to occur, all factors considered.[288] Similarly, the *Massachusetts v. EPA* Court examined whether global warming would be substantially worsened if the EPA didn't regulate greenhouse gas emissions from new vehicles.[289] This would be the essence of heightened risk analysis – deciding whether an event or condition occurring in the future is likely to occur. But, even so, this runs into the same problems on an expanded timeline because the condition having a sustained, nonzero likelihood will certainly happen at some point in the distant future.[290] Yet, if the Court binds substantial-risk theory with an immediacy requirement, there is little difference to the "certainly impending" threshold. Consequently, the next logical step would be to examine a condition's strength or likelihood over a 'reasonable' period of time, 'reasonable' being more relaxed than immediate.[291] But admittedly, this would raise an additional complexity of defining a "reasonable time period."

On the other hand, if the substantial-risk theory examines plaintiffs' harm using a time as the indicator, then a distinguishable test emerges. As a concrete example, consider a victim whose baseline risk of experiencing an event, *E*, to be one percent year-over-year. Next, consider that a defendant's action causes a sustained ten-fold increase (ten percent year-over-year) to the victim's baseline risk of experiencing *E*. Under the heightened risk, the victim has nearly an eighty percent chance she will experience *E* within fifteen

---

[288] *See supra* notes 200–208 and accompanying text. The Court held that it standing did not turn on whether Driehaus would seek reelection because SBAL would discuss other candidates' seeking reelection sometime in the future. Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2344–45 (2014).

[289] *See* Massachusetts v. EPA, 549 U.S. 497, 522–24 (2007) (discussing the effects of global warming).

[290] *See supra* notes 276–279 and accompanying text.

[291] For example, if an event A having a heightened risk of thirty percent per year, it might fail the certainly impending threshold because it is unlikely to be imminent; on the other hand, there is more than a seventy-five percent chance A could occur within the next four years, which may be acceptable under substantial risk. *Cf.* Massachusetts v. EPA, 549 U.S. 497, 526 (2007) (granting standing because global warming will have "catastrophic" effects at an unspecified point in the future); *Driehaus,* 135 S. Ct. at 2343–45 (granting standing because SBAL may be charged under the Ohio statute in some future election).

years; however, under her baseline risk, she would not reach an eighty percent chance of experiencing *E* until more than *160* years from now.[292] In contrast, a victim with a ten-percent baseline risk of experiencing *E*, but an eleven-percent heightened risk of *E*, would only experience a year-and-a-half's difference before hitting an eighty percent threshold. Thus, under this approach, both the underlying risk and the relative increase in risk are considered over time, but the relative risk impacts are better accounted for.

Also, cases where the harm is conditional on an independent third-party actor are doomed under the "certainly impending" standard on traceability grounds.[293] However, the "substantial" or "reasonable" risk standard would allow standing if the strength of the assumption on the third-party actor is substantial.[294] That is, if it is reasonable to assume that a third-party actor, either through probability or stated intent, then there should be a sufficient basis for injury-in-fact, especially if the emphasis is on the relative risk. Also, many security experts argue that finding out where the stolen data came from is fairly easy for investigators.[295]

---

[292] *N*, number of years, is given by $N > \frac{\log(0.80)}{\log(1-P(E))}$, where *P(E)* is either 0.99 for baseline risk or 0.90 for heightened risk.

[293] *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (holding that the injury cannot result from third-party actions).

[294] A good example is the Court's reasoning in *Bennett v. Spear*, 520 U.S. 154 (1997). In *Bennett*, the Court noted that if there are "determinative or coercive" effects on the third-party, then it can be fairly traceable. *Id.* at 168–69. But this reasoning presupposes that the third-party actor will act in accordance with the coercive effect, essentially making the analysis probabilistic. *See id.* at 169 ("[W]hile Service's Biological O[pinion theoretically serves an 'advisory function,' . . . in reality it has a powerful coercive effect on the action agency.").

[295] *See Krebs on Healthcare*, *supra* note 33 (noting that value is not as easily derived from healthcare records since they are largely handled by third parties who don't have a direct connection to the patients).

3. Current substantial-risk tests that emphasize overall risk do not do enough to account for relative risk

The D.C. Circuit has proposed two ways to determine whether an imminent injury exists: the first way is to treat the "ultimate alleged harm . . . as the concrete and particularized injury and then … determine whether the increased risk of such harm [is] sufficiently 'imminent;'"[296] the second is to treat the heightened risk as an actual injury.[297] The second approach is arguably cleaner because it keeps the courts from having to make difficult, and sometimes subjective, determinations about which injuries are sufficiently imminent;[298] however, the D.C. Circuit has argued that such an approach also renders the "actual or imminent" meaningless and opts for the first approach.[299]

Given the first approach, several courts have advanced a substantial risk test. *Galaria's* theory that the heightened risk, alone has no significant bearing on the likelihood of an injury-in-fact and that the proper question is whether the plaintiff has an *overall* "substantial risk" of injury.[300] The D.C. Circuit solidifies this reasoning further by requiring that an alleged injury result in "(i) a *substantially* increased risk of harm and (ii) a *substantial* probability of harm with that increase taken into account."[301] In other words, not only does the victim have to show that a defendant's actions have caused a measurable

---

[296] *See* Public Citizen, Inc. v. Nat'l Highway Traffic Safety Admin., 489 F.3d 1279, 1297–98 (D.C. Cir. 2007) (rejecting the approach to characterize heightened risk as an injury and, instead, presenting an approach using probability-of-harm as the measure).
[297] *See id.* (arguing that if heightened risks were actual injuries, then the imminence requirement would be meaningless); *see also In re SAIC*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (declining to characterize heightened risk as an actual injury).
[298] *See Probabilistic Standing*, *supra* note 62, at 75–77 (noting that courts would not need to rely on "precise calculations of probabilities" if all imminent injuries had standing); *see also* Winters, *supra* note 67, at 365 (arguing the "quantify[ing] risk" mixes "threshold determination[s]" with "merits analysis").
[299] *See Public Citizen*, 489 F.3d at 1297–98 (holding that treating heightened risk as an injury would lead to standing in every case).
[300] *See* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 654 (S.D. Ohio 2014) (distinguishing between relative risk of injury and absolute risk).
[301] Public Citizen v. Nat'l Highway Traffic Safety, 489 F.3d 1279, 1295 (D.C. Cir. 2007).

increase in the risk of injury, but also that measurable increase has now placed the victim at substantial risk of injury.

But both tests fail to account for relative risk, especially across time, which is arguably what the whole issue is.[302] As an example, consider a victim whose baseline risk of developing a particular type of cancer is fifty out of every 100,000 (0.05 percent), but because of defendant's actions, his risk is twenty-five fold (1.25 percent). In terms of time to reach an eighty-percent risk threshold, the victim moves from 3,218 years to 128 years! The relative risk is twenty-five times greater, but the overall risk is still less than two percent, and would likely lead to a rejection of standing by the D.C. Circuit. Yet, it is unlikely that few societies today would conclude that the victim was not injured in some way, especially when the result is spread over a class or a group.[303] As a result, the "substantial risk" threshold should rely more heavily on the relative risk, the first prong of the D.C. Circuit's test, rather than the second prong.

III. APPLYING THE CONTEXT-SPECIFIC THRESHOLD FOR IMMINENT INJURIES TO DATA-BREACH CASES

In Part II, this Article proposes a framework for a context-specific standing threshold that varies its likelihood requirement based on separation-of-powers concerns and the severity of harm. It also proposes that the

---

[302] For instance, consider P, whose ordinary chances of suffering an injury are one percent, but because of D's actions, P's chances of injury increase by one percent year over year. Under the rigorous D.C. test, P would not have standing until one day, perhaps fifty years from now, which at that point the injury is more likely than not to occur. A concrete example would be fingerprint data exposure. *See* David Alexander, *5.6 Million Fingerprints Stolen in U.S. Personnel Data Hack: Government*, REUTERS (Sep. 23, 2015 3:50pm), http://www.reuters.com/article/us-usa-cybersecurity-fingerprints-idUSKCN0RN1V820150923 (noting OPM's acknowledgement that although the technology to exploit fingerprint data is "currently limited," "the threat could increase over time").

[303] *See* Amanda Leiter, *Substance or Illusion? The Dangers of Imposing a Standing Threshold*, 96 GEO. L.J. 391, 411–15 (2009) (discussing the D.C. Circuit's substantial risk test and arguing that it fails to account for the population size and an injury's magnitude).

relaxed "substantial risk" threshold focuses on the increase in relative risk that the victim suffers from the defendant actions. Given that a data-breach victim usually sues on a theory of negligence, fraud, breach o contract, or unjust enrichment,[304] separation-of-powers concerns are minimal, and the courts should be comfortable in applying a lower threshold of injury.[305] Moreover, if the courts were to require apply the "substantial" or "reasonable" risk standard as a threshold, analyzing the victim's relative-risk of harm, then a good balance is drawn between caseload and ensuring the victim's get their day in court.[306] After all, several companies have settled after the courts found standing in their respective cases.[307]

A. Factors to Consider for Substantial Risk Analysis

To determine whether a breach victim alleging a HRIT should have standing, the courts should begin with identity theft as the ultimate injury; next, the court should determine how the defendant's actions have changed the victim's risk profile compared to the victim's baseline risk.[308] If the relative-risk is substantial in that it changes the victim's risk profile in a meaningful way, then the court should find standing.[309] Most importantly, when "substantial risk" is applied, the courts should not fixate on whether the harm will occur within a fixed timeframe; instead, the courts should look at empirical data and other factors to inform its analysis.

---

304 *See supra* Part I.D.
305 *See supra* Part II.A.1.
306 *See supra* Part II.B.3.
307 *See e.g.* TARGET BREACH SETTLEMENT, https://targetbreachsettlement.com/ (last updated Dec. 2015) (notifying victims of a settlement and a chance to file a claim); Anne Bucher, *Adobe to Settle Data Breach Class Action Lawsuit*, TOP CLASS ACTIONS (Apr. 24, 2015), http://topclassactions.com/lawsuit-settlements/lawsuit-news/54519-adobe-to-settle-data-breach-class-action-lawsuit/ (noting that Adobe has a reached a proposed settlement with data-breach victims).
308 *See supra* Part II.B.3.
309 Supra Part II.B.3.

Fortunately (or unfortunately), cybersecurity and protecting sensitive information (to include PII) have taken a front seat in national politics.[310] Consequently, there is increasing data on the effects of identity theft, trends on cyber intrusion, and on the risks victims often face in these situations.[311] Recent trends from Javelin Research suggest that "two-thirds of identity fraud victims" had previously received a data-breach notice "in the same year."[312] Identity theft has been a sixteen-to-twenty-one billion dollar industry over the past five years, affecting more than ten million Americans annually.[313] In 2014, fourteen percent experienced out-of-pocket losses of $1,000 or more.[314] Sadly, many experts conclude that most data breaches were preventable, with one analysis noting the number to be as high as ninety percent.[315]

1. Active or Recent Cases of Actual Identity Theft

In analyzing data-breach cases, the courts should consider a combination of the following factors when determining whether there is a substantial or a reasonable risk of injury. Generally, the courts do find standing when there have been previous or ongoing identity thefts.[316] It is arguable that most

---

310 *See* EXECUTIVE OFFICE OF THE PRESIDENT, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (discussing various initiatives for strengthening cybersecurity); DHS, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 14–15 (2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf)(noting confidentiality as a priority).

311 DBIR 2015, *supra* note 3, at 3; FINKLEA, *supra* note 230.

312 Press Release, *$16 Billion Stolen from 12.7 Million Identity Fraud Victims in 2014*, JAVELIN STRATEGY & RESEARCH (Mar. 3, 2015), https://www.javelinstrategy.com/press-release/16-billion-stolen-127-million-identity-fraud-victims-2014-according-javelin-strategy.

313 Tamara E. Holmes, *Credit Card Fraud and ID Theft Statistics*, CREDITCARDS.COM (Sep. 16, 2015), http://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

314 HARRELL, *supra* note 7, at 6.

315 *See* SECURITY AND PRIVACY ENHANCING BEST PRACTICES, ONLINE TRUST ALLIANCE 1 (2015), https://otalliance.org/system/files/files/resource/documents/ota2015-bestpractices.pdf.

316 *See supra* notes 172–173 and accompanying text; *see also In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1158–59 (D. Minn. 2014) (noting that many of the Plaintiffs "actually incurred unauthorized charges").

cases involving some class members who experienced recent or ongoing identity theft attempts creates a substantial risk of identity theft for all members.[317] But the inquiry should not end there.[318] The whole point of imminent injury standing is that it allows for those injuries that have not yet occurred.[319] Moreover, there are many instances where breach victim are injured in ways that are not apparently linked.[320] Often, this occurs because companies retain significant amounts of historical, redundant, or excessive PII, and consumers are unaware that a breach may have affected them.[321] More importantly, the substantial risk standard demands more.[322] Thus, the courts should consider additional factors that weigh upon a victim's relative risk.

---

317 This is not because the probability that any given victim experiencing identity theft directly influences the probability that any other victim would experience the same thing. But it does demonstrate both technical competency and intent by the hackers or thieves to utilize the stolen data for financial crimes or other purposes. *See*, *e.g.,* Reilly v. Ceridian Corp., 664 F.3d 38, 43–44 (3d Cir. 2011) (distinguishing the attack in *Pisciotta*).

318 *See*, *e.g*, Peters v. St. Joseph Servs.' Corp., 74 F. Supp. 3d 847, 854–55 (S.D. Tex. 2015) (applying the "if" test and noting that Plaintiffs cannot have standing until their theory of injury actually happens); *see also In re SAIC*, 45 F. Supp. 3d 14, 25–28 (D.D.C. 2014) (allowing only one litigant to proceed because the other litigants had no actual injuries).

319 *See supra* part II.B.2.

320 For instance, when Anthem Blue Cross disclosed a massive breach, the company and government officials noted that there was no evidence of identity theft. Rick Jurgens, *A Year Later, Impact of Anthem Data Breach Still Debated*, VALLEY NEWS (Feb. 24, 2016), http://www.vnews.com/Archives/2016/02/a1-anthembreach-rj-vn-022116. But the victims allege that they have had "fake tax returns filed in their names," along with fraudulent credit cards and loans in their names. *Id.* Victims in *Storm* had also faced fraudulent tax-return issues near the time of Paytime's data breach. *See* Barbara Miller, *Paytime Data Breach Could Reach an Estimated 216,000 in U.S.*, PENN LIVE (last updated Jun. 8, 2014, 9:24AM), http://www.pennlive.com/midstate/index.ssf/2014/06/paytime_data_breach_reaches_an.html (noting that the victim had not used Paytime "since 2008" but believes that Paytime retained his old information). *But see* Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 365–66 (M.D. Pa. 2015) (noting that none of the class members actually experienced any injury from data misuse).

321 Nicholas Elliott, *Cyber Compliance: Data Excess Magnifies Risk*, RISK & COMPLIANCE, WALL ST. J. (May 14, 2013, 3:41 PM), http://blogs.wsj.com/riskandcompliance/2013/05/14/cyber-compliance-data-excess-magnifies-breach-risks/; *see* Miller, *supra* note 320.

322 *See supra* part II.B.

2. Other Factors

Encryption secures data from being accessible by third-parties.[323] There are several industry standards and readily available encryption software, making this important protection widely implement across multiple industries today.[324] Disk and server encryption greatly lowers potential victims' risks, particularly in physical-theft cases where a laptop or hard-disk is stolen.[325] If a stolen laptop or hard-disk has encryption, the hacker must defeat the encryption to even access the information. On the other hand, anyone could exploit the information where there is no encryption.[326] Surprisingly, many corporations and agencies fail to follow this basic practice.[327] Thus, the courts should consider whether the data is encrypted in its substantial risk calculus.

Also, as some courts have hinted that the sophistication of an attack provides some insight as to the probability that victims of a data-breach will face a successful identity theft in the future.[328] A sophisticated and targeted

---

[323] *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1206–07 (N.D. Cal. 2014) (noting that the hackers were able to decrypt the personal data in Adobe's servers); *see generally* KAREN SCARFONE ET AL., NAT'L INST. OF SCI. & TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800-111, GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES 2-3, 2-4 (2007), http://www.hhs.gov/sites/default/files/nist800111.pdf [hereinafter NIST SP800-111] (discussing encryption).

[324] *See* NIST SP800-111, *supra* note 323, at 3-1 (discussing various encryption options such as disk-based or system-based encryption))).)

[325] *See Avoid Identity Theft: Protecting Social Security Numbers*, U.S. SOCIAL SEC. ADMIN., https://www.ssa.gov/phila/ProtectingSSNs.htm (recommending encryption to prevent theft of social-security numbers).

[326] *See In re SAIC*, 45 F. Supp. 3d 14, 20 (D.D.C. 2014) (noting that the personal information on the stolen laptop required specialized hardware and software).

[327] *See*, *e.g.,* Robert Westervelt, *Coca-Cola Laptop Breach A Common Failure of Encryption, Security Basics*, CRN (Jan. 27, 2014, 4:55 PM), http://www.crn.com/news/security/240165711/coca-cola-laptop-breach-a-common-failure-of-encryption-security-basics.htm; *see also* Eric Chabrow, *Why Organizations Fail to Encrypt*, BANK INFO SECURITY (Dec. 22, 2012), http://www.bankinfosecurity.com/interviews/encryption-i-1740/op-1; Rick Robinson, *The Impact of a Data Breach Can be Minimized Through Encryption*, SECURITY INTELLIGENCE (Oct. 21, 2014), https://securityintelligence.com/the-impact-of-a-data-breach-can-be-minimized-through-encryption/ (comparing Adobe's data breach with Target's data breach and how encryption would have minimized the cost).

[328] *See Reilly*,F.3d at 44 (recognizing that the attacker in *Pisciotta* was "sophisticated"); *In re Adobe Sys.*, 66 F. Supp.3d at 1206–07 (describing a highly sophisticated attack where hackers spent

attack requires time, money, and skill, and there is a higher likelihood that with the investment of resources, the damage is greater.[329] Furthermore, the more time that passes between the actual attack, the discovery of the attack by either the victim or the server operators, and the notification to all potential victims, the more likely that a successful identity theft is possible.[330]

As previously discussed, attackers sometimes make announcements of a successful breach and will also state their intentions, sometimes in the form of a demand.[331] The court need not speculate about an attacker's intentions if an attacker includes threats of subsequent actions, such the use or disclosure personal information. Thus, if there is a stated intent, then the courts should take such intentions as true and analyze whether the victims face a heightened risk based upon such intentions.

Courts should also consider whether there is any clear evidence that data was actually stolen. In 2015, there were nearly 80,000 data breach incidents; however, only a little more than 2,100 had confirmation that data was stolen.[332] It is less likely that victims are at a risk of identity theft if there is no confirmed report that the exposed personal information was stolen.

Finally, not all data is equal. Some captured information can be used within a short period of time and only one time. On the other hand, other

---

weeks breaching Adobe's servers). *Contra* Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 365–68 (M.D. Pa. 2015) (dismissing highly sophisticated attacks as indicative of risk and insisting on an actual injury prior to standing).

[329] *See* Graeme R. Newman, *The Problem of Identity Theft*, CENTER FOR PROBLEM-ORIENTED POLICING (2004), (http://www.popcenter.org/problems/identity_theft/) (distinguishing between highly organized identity theft operations and opportunistic ones, finding that the more organized the scheme, the higher chance of success).

[330] *See* SYNOVATE, FEDERAL TRADE COMMISSION - IDENTITY THEFT SURVEY REPORT 8 (2003), http://www.popcenter.org/problems/identity_theft/PDFs/FTC_2003a.pdf (discussing the benefits of a "quick discovery" and noting that the amount of time and money a victim needs to resolve identity theft cases is correlated with the length of time between breach and discovery).

[331] *See* David Robb, *Sony Hack: A Timeline*, DEADLINE (Dec. 22, 2014, 1:25 PM), http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ (noting that the hackers in Sony threatened to release personal information, emails, and other data if Sony did not comply with their demands). The attack on Ashley Madison also resulted in a ransom letter. Krebs, *supra* note 18.

[332] DBIR 2015, *supra* note 3, at 3.

information, such as SSNs, birthdates, and health information have lesser value when separate, but when aggregated, can create a complete profile of the victim for future exploitation.[333] Such "permanent" PII creates longer-term risk for a victim compared with shorter-term information, such as credit and debit card numbers. Yet, some studies have shown that stolen credit card or debit card information is a clear indicator of substantial risk.[334] Consequently, the court should consider the amount and type of personal information that was potentially collected about a given individual or organization. For instance, healthcare information was the most coveted data in 2015 because sizable profits could be obtained from insurance fraud.[335] Also hackers who obtain large quantities of PII on individuals have multiple opportunities to exploit that information.[336]

The relationship between time and the type of information can help courts considerably. For instance, if debit and credit card numbers were compromised, as in *Zappos*, and a few years pass without any substantial identity theft within the affected class, then there is likely no meaningful heightened risk.[337] On the other hand, when a victim loses control of her health records, biographical data, and SSN, she may not realize the full effect of the injury until several years have passed.

All of these factors play into a "substantial risk" analysis. If courts apply these factors to standing law in data-breach cases, several cases would have

---

333 *See* U.S. COMPUTER EMERGENCY RESPONSE TEAM, PROTECTING AGGREGATED DATA 4–6 (2005) (defining data aggregation and discussing the associated inherent risks).
334 *See* Kathy Kristof, *Fraud Risk Soaring for Data Breach Victims*, CBS NEWS (Feb. 5, 2014, 2:27 PM), http://www.cbsnews.com/news/fraud-risk-soaring-for-data-breach-victims/ (noting a study that indicated that, in 2013, "[forty-six] percent of consumers with a breached debit card" were "fraud victims in the same year").
335 RECORD BREAKING HEALTHCARE DATA BREACHES IN 2015 MAY BE ECLIPSED IN 2016, HIPPA JOURNAL (Dec. 10, 2015) http://www.hipaajournal.com/healthcare-data-breaches-in-2015-2016-worse-2012/.
336 *See*, *e.g.*, Peters v. St. Joseph Servs.' Corp., 74 F. Supp. 3d 847, 850–51 (S.D. Tex. 2015) (noting that victim's "[SSN], birthdate, address, medical records and bank account information" was stolen and that the victim experienced everything from telemarketing for medical devices to attempted hacks on her Amazon account);
337 *See In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958 (D. Nev. 2015) (suggesting that three years without incident may not qualify as an imminent injury).

come out differently. For instance, The Texas branch of St. Joseph Health Network's data systems were attacked sometime in December 2013.[338] The hackers had accessed patients' SSNs, birthdates, medical records, and financial data.[339] St. Joseph discovered the breach and notified potential victims; the victims sued St. Joseph, arguing they have a HRIT.[340] However, the district court held that the victims lacked standing because a HRIT is not "certainly impending."[341] And *Clapper* does not allow mitigation expenses for 'hypothetical' injuries.[342] But the district court did not apply any meaningful "substantial risk" analysis.[343] Under "substantial risk" the court would have considered that the substantial amount of permanent PII stolen, which created the potential for medical and identity fraud. In doing so, the court would acknowledge the strong possibility that the victims may face serious injuries in the future stemming from the data breach.

Moreover, the California branch of the St. Joseph Health System recently settled with data-breach victims in a separate case for twenty-eight million dollars.[344] The settlement stemmed from a mishandled security configuration in January 2011 that allowed tech-savvy individuals to access a "patient[s'] names, diagnoses list, medication allergies, body mass index, blood pressure,

---

338 David F. Carr, *Texas Hospital Discloses Huge Breach*, INFORMATION WEEK (Feb. 5, 2014, 2:00 PM), http://www.informationweek.com/healthcare/security-and-privacy/texas-hospital-discloses-huge-breach-/d/d-id/1113724.

339 *Id.*

340 *Peters*, 74 F. Supp. 3d at 850–51.

341 *See id.* at 854–55 (noting that Plaintiffs' identity theft injury rests on a series of "ifs").

342 *See id.* at 855–56 (acknowledging *Clapper*'s holding that plaintiffs cannot create standing by "making an expenditure based on a nonparanoid fear") (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2015)).

343 *Id.* at 854–55. Although the district court acknowledges "substantial risk," it neither applies a distinct test nor explains why the Plaintiffs do not meet it. *See id.* at 855 ("The allegation that risk has been increased does not transform that assertion in to a cognizable injury.").

344 Marianne Kolbasuk McGee, *'Egregious' Breach Results in Hefty Settlement*, HEALTH INFO SECURITY (Mar. 16, 2016), http://www.healthcareinfosecurity.com/egregious-breach-results-in-hefty-settlement-a-8974.

lab results, smoking status, and advanced directive status," along with "birth date, race, and gender."[345]

B. Remijas Correctly Applies Standing Law and Substantial Risk Factors When Considering Data-Breach Risks

In deciding whether the class of victims had standing to bring a lawsuit against Neiman Marcus under a common-law theory of negligence and other claims, the *Remijas* Court concludes that they did using the standards discussed in Part II.B.1.[346] Moreover, the Court distinguished *Clapper* on its facts and relaxed the standing requirement to allow a heightened risk of injury under the substantial risk standard.

The victims sued Neiman Marcus under "state breach laws" and other common tort claims; they did not allege the unconstitutionality of a statute or regulation, nor did they challenge government action. Consequently, the Court considered their injury claims under a relaxed imminent injury threshold of "substantial" or "reasonable" risk.[347]

In analyzing the risk, the Court considered three factors: (1) 9,200 of the 350,000 "potentially exposed cards" were already "used fraudulently;" (2) malware was found in the system that resulted from a fairly sophisticated attack; (3) and the hack occurred around three to six months before the discovery. The court also noted that the hack and subsequent downloading of consumer records created a fair presumption that the hackers intended to commit fraud. And Neiman Marcus confirmed that data was actually stolen when it investigated the data breach. Moreover, the type of information (debit and credit accounts) was the type of information that has value in the

---

345 *See* Howard Anderson, *Glitch Exposes Medical Record Online*, HEALTHCARE INFO SECURITY (Feb. 17, 2012), http://www.healthcareinfosecurity.com/glitch-exposes-medical-records-online-a-4515 (noting that the information was accessible via Internet for nearly a year).
346 *See* Part I.E.4. and accompanying text.
347 *See* Part I.E.4. and accompanying text.

immediacy, so some evidence of existing identity fraud was to be expected. The *Remijas* Court understood that there were little separation-of-powers concerns, as compared to *Clapper*. And although the main issue in *Remijas* was credit-card fraud, the Court correctly applied a substantial risk test to arrive at standing.

CONCLUSION

Ms. Edith Ramirez, Federal Trade Commission Chairwoman, testified shortly after the Neiman Marcus breach that "companies continue to make very fundamental mistakes when it comes to security" and that she did not "believe the burden should be placed on consumers."[348] Currently the burden is.[349] And the courts should not preclude data-breach victims who have a realistic and credible potential for identity and medical fraud. The *Remijas* Court agreed. And the *Remijas* acknowledged that *Clapper* did not foreclose all data-breach victims from suing corporations who mishandle their PII.[350]

Cybersecurity is an emerging area that requires serious attention across all sectors of industry, government, and the greater society. Cybersecurity is no less important than physical security, something that many corporations take seriously. But sound practices are best developed and improved when the cost and risk allocations are distributed properly across all sectors. They currently are not. Data breach victims have little recourse and little power in compelling corporations and agencies to protect their PII, yet it is a priority (and a concern) for many.

---

[348] Grant Cross, *Target and Neiman Marcus Execs Defend Security Practices*, COMPUTERWORLD (Feb. 5, 2014, 3:16 PM), http://www.computerworld.com/article/2487386/cybercrime-hacking/target-and-neiman-marcus-execs-defend-security-practices.html.
[349] *See supra* notes 44–49 and accompanying text.
[350] *See supra* Part I.E.4.

Standing law has been a major impediment to data-breach victims.[351] But it does not have to be. This Article argued that *Clapper* does not compel non-justiciability in all heightened-risk cases; the separation-of-powers doctrine does not either. And case-load concerns can be mitigated by applying a lower, but sensible, substantial-risk threshold that accounts for the relative-risk increase of HRIT that many face. The costs are not trivial; many victims spend months resolving outstanding financial and credit issues caused by identity theft.[352] To make matters worse, less than three percent of these victims note that they were saved by credit-monitoring service. Many have reported becoming distraught; a few have committed suicide.

This Article presented a framework for imminent injuries that can help give victims the much-needed redress without flooding the courts with a tidal wave of data-breach litigation. By using an imminent injury framework sensitive to separation-of-powers doctrine and severity of the injuries, the courts adhere to Article III principles without needlessly shutting the door for victims who have little recourse. Additionally, a "substantial risk" threshold that focuses on relative risk can help in correcting the unbalanced cost-risk allocation that exists within these situations. In doing so, corporations will invest more in cybersecurity and embrace current best practices, stemming the billions of dollars that society incurs yearly.

---

[351] *See supra* Part I.D.
[352] *See supra* notes 55–60.