The Struggle to Define Privacy Rights and Liabilities in a Digital World and the Unfortunate Role of Constitutional Standing

JUAN OLANO*

Today's world runs on data. The creation and improvement of technological products and services depend on the exchange of data between people and companies. As people's lives become more digitized, companies can collect, store, and analyze more data, and in turn, create better technology. But, because consumer data can be very sensitive (think Social Security numbers, GPS location, fingerprint recognition, etc.) this cyclical exchange comes with serious privacy risks; especially in light of more frequent and sophisticated cyberattacks. This creates a face-off between technological growth and privacy rights. While it makes sense that people should be willing to subside some of their privacy in exchange for technological enhancements to things like communication, health, and entertainment, companies should also be doing their best to prevent and respond to cyberattacks.

This Note highlights the urgency created by the combination of the digitization of consumer lives, sophisticated hackers, and inadequate data privacy laws. It explains that,

* J.D. Candidate 2018, University of Miami School of Law; B.A. with Distinction 2015, University of North Carolina at Chapel Hill. I want to thank Professor Stephen J. Schnably for his guidance, mentorship, and support in writing this Note and for challenging me every step of the way; Alfred J. Saikali for giving me the first glimpse at the critical merger between cybersecurity and the law; and the members of the University of Miami Law Review who influenced this Note. I especially want to thank my parents and my siblings for their relentless love and support—thank you for always believing in me and my pursuits.

because Congress is yet to legislate and the Supreme Court's findings in Clapper v. Amnesty International USA and Spokeo, Inc. v. Robin created federal circuit splits, data privacy laws are either non-existent or muddled. As a result, it is increasingly difficult for companies or consumers to know their rights, responsibilities, and liabilities in this sphere. Moreover, this Note calls for Congress to establish federal compliance measures with respect to corporate use of consumer data and handling of cyberattacks. However, this Note argues that Congress will continue to remain silent and, therefore, the Supreme Court, by revisiting the constitutional standing issues presented in Clapper and Spokeo, can be the one—for now—to provide much needed guidance with respect to data privacy.

INTRODUCTION

"If we're going to be connected, then we need to be protected . . . we shouldn't have to forfeit our basic privacy when we go online to do our business," President Barack Obama stated in a 2015 National Public Radio interview.[1] He was calling for the federal government

[1] Scott Horsley, *Obama: 'If We're Going To Be Connected, Then We Need To Be* Protected,' NAT'L PUBLIC RADIO (Jan. 12, 2015), http://www.npr.org/sections/alltechconsidered/2015/01/12/376788871/obama-if-were-going-to-be-connected-then-we-need-to-be-protected.

to help improve security systems to prevent cyberattacks.[2] Ironically, and underscoring the urgency of Obama's remarks, cybercriminals hacked the United States Central Command's Twitter account later that day.[3]

The President's declarations were well-grounded: in 2016 alone, there were at least 980 reported[4] data breaches through which more than 35,233,317 records were exposed.[5] Most recently, Equifax reported that a data breach hit 143 million user accounts.[6] Juniper research predicted that data breaches will cost at least $2.1 trillion globally by 2019.[7]

We are living in a vulnerable era where our personal and financial data is stored in everyday devices, gadgets, and appliances that are susceptible to cyberattacks.[8] The technological revolution has spurred an unprecedented increase in companies' collection of per-

---

[2] *Id.*

[3] Everett Rosenfeld, *FBI Investigating Central Command Twitter Hack*, CNBC (Jan. 12, 2015), http://www.cnbc.com/2015/01/12/us-central-command-twitter-hacked.html.

[4] Most breaches are not reported or even detected. Steve Morgan, *Cyber Crime Costs Projected To Reach $2 Trillion by 2019*, FORBES (Jan. 17, 2016), https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7108068e3a91. "The World Economic Forum (WEF) says a significant portion of cybercrime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot." *Id.*

[5] This number only reflects reported breaches involving more than an email, user name, and password, meaning that in actuality, there were probably many more breaches. *See Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout*, ITRC (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html.

[6] *See* Matt Burgess, *That Yahoo Data Breach Actually Hit Three Billion Accounts*, GUARDIAN (Oct. 4, 2017), http://www.wired.co.uk/article/hacks-data-breaches-2017.

[7] Morgan, *supra* note 4.

[8] *See generally Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, KREBSONSECURITY (Oct. 22, 2016), https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/. Unlike the days when operating systems were only on computers, now they are in our phones, on our TVs, in our Wi-Fi networks, in our speakers, and in our home appliances. *Why Your Chances of Getting Hacked Could Increase This Year*, CBS (Jan. 2, 2017), https://www.cbsnews.com/news/protect-yourself-from-email-hacking-cyber-threats/ [hereinafter *Hacked*].

sonally identifiable information ("PII"), which is defined as anything that can be used to identify, locate, or contact a person.[9] PII is endlessly provided by consumers and collected by companies online through the typical use of technology (think mouse-clicks, social media likes, mobile apps, GPS updates, etc.).[10] Juniper research calls this the "digitization of consumers' lives and enterprise records."[11]

As PII increases, so does the vulnerability of consumer data theft or data misuse.[12] In this Note, "data theft" will refer to situations of lost or stolen PII resulting from a data breach. This involves situations where companies (e.g., retailers, technology companies, health systems, or financial institutions) are hacked and thereby lose consumer PII.[13] On the other hand, "data misuse" will refer to the wrongful or inaccurate exposure of PII on behalf of companies; this involves situations where companies violate a consumer protection statute. For example, by violating the Video Privacy Protection Act of 1988 ("VPPA"),[14] a company endangers the integrity of consumer PII. Put simply, data theft will deal with data breaches and data misuse with a company's violation of a consumer protection statute.

Despite the increased threat of data theft by hackers and data misuse by companies, the law and the governmental mechanisms that create and enforce it (e.g., Congress, federal agencies, and the Supreme Court) have struggled to adapt. The government must step in to push for clearer privacy rights and liabilities, and to ensure that the law catches up. "Fundamentally, the law is a powerful tool to

---

[9] John Stringer, *Protecting Personally Identifiable Information: What Data is at Risk and What You Can Do About It*, SOPHOS (Oct. 2011), https://www.sophos.com/en–us/medialibrary/pdfs/other/sophosprotectingpii.pdf.

[10] *Id.*

[11] Morgan, *supra* note 4.

[12] Irina Raicu, *Loss of Online Privacy: What's the Harm?*, MARKKULA CENTER FOR APPLIED ETHICS (Feb. 4, 2013), https://www.scu.edu/ethics/privacy/loss–of–online–privacy–whats–the–harm/.

[13] *See e.g.*, Rick Robinson, *The Top 5 Retail Breaches*, SECURITY INTELLIGENCE (Oct. 7, 2014), https://securityintelligence.com/the-top-5-retail-breaches/ (discussing data theft and breaches against retail stores).

[14] 18 U.S.C. § 2710 (2012). The VPPA, among other functions, protects against the unconsented dissemination a consumer's personally identifiable rental information. *Id.*

assist with setting a . . . standard in data protection, [and in] providing a degree of security alongside flexibility for [companies] to approach their policies . . . ."[15]

While agencies such as the Federal Trade Commission ("FTC") have increased their limited efforts to protect consumers,[16] Congress and the Supreme Court have been slower to react. There is "no overarching framework legislation in place [for cybersecurity], but [instead] many enacted statutes [that] address various aspects of cybersecurity."[17] Therefore, there is a growing consensus that "the current legislative framework for cybersecurity might need to be revised to address needs for improved cybersecurity, especially given the continuing evolution of the technology and threat environments."[18] Crucially, this also means that some cybersecurity harms are statutorily addressed, while some are not—a distinction between data theft and data misuse.

The Supreme Court's efforts are not much different, as the Court has not provided anything more than minimal guidance regarding privacy rights and liabilities. In its decisions in *Clapper v. Amnesty International USA*[19] (a quasi-data theft suit) and *Spokeo, Inc. v. Robins*[20] (a data misuse suit), the Supreme Court "failed to articulate an intellectual framework that can satisfactorily explain the results in

---

[15] Liam Lambert, *Cyber Security – Attacks, Effects and the Role of the Law*, MARKET MOGUL (Jan. 5, 2017), http://themarketmogul.com/cyber–security–attacks–effects–role–law/.

[16] *See e.g.*, *FTC Testifies on Efforts to Protect Privacy and Security of Consumer Health Information*, FED. TRADE COMM'N (Mar. 22, 2016), https://www.ftc.gov/news–events/press–releases/2016/03/ftc–testifies–efforts–protect–privacy–security–consumer–health.

[17] ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 2 (2014), https://fas.org/sgp/crs/natsec/R42114.pdf. The congressional report cites acts enacted from 1987 to 2002, demonstrating the need for new acts. *Id.*

[18] *Id.* at 1.

[19] 568 U.S. 398 (2013).

[20] 136 S. Ct. 1540 (2016).

[privacy] cases that are already decided, or that can be usefully employed to shape legal analysis in cases yet to come."[21] This has resulted in two federal circuit court splits, a post-*Clapper* and a post-*Spokeo* split, which add to the chaos regarding consumer rights and corresponding liabilities where PII is stolen or misused.[22]

This Note argues that the increased collection, exchange, and dissemination of consumer PII, coupled with an upward trend in cyberattacks, requires congressional action. Though Congress should act to define privacy rights and protections, if its silence continues to drive the conversation, the Supreme Court may soon (again) be in the unique position to provide guidance. When it has the chance, considering what is at stake, the Court must be clearer than it was in *Clapper* and *Spokeo*, which have led to uncertainty over the state of litigation, consumers' availability of redress, and adequate cybersecurity thresholds.[23]

Part I highlights the urgency created by the frightening combination of technological innovations, the digitization of consumer lives, sophisticated hackers, and governmental inadequacy. It also explains the role of the law in defining consumer privacy through the FTC, Congress, and the Supreme Court, which either create or enforce such laws. Part II briefly explains the constitutional standing requirements with a focus on the injury-in-fact requirement, which is the crux of consumer protection suits like *Clapper* and *Spokeo*. Parts III and IV, respectively, discuss the story of data theft and data misuse in the court system. Specifically, each Part explains what led to *Clapper* and *Spokeo*, the flawed analyses used to determine each decision, and the resulting chaotic state. Part V demonstrates the complexities of what is at stake for consumers and for companies, with the goal of showing why Congress and the Court may be too afraid to take a stance on anything privacy-related. Finally, Part VI urges Congress to legislate, but anticipating congressional silence, calls for the Supreme Court to clarify its position in data theft cases and to defer to Congress in data misuse cases.

---

[21] William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 290 (1988). While this Note speaks of standing in general, it reflects where privacy standing currently stands as well.

[22] *See infra* Parts III, IV.

[23] *Id.*

I. URGENT TIMES KNOCKING AT THE DOOR: SEARCHING FOR LEADERSHIP

Today, "virtually every organization acquires, uses and stores personally identifiable information."[24] As mentioned, PII includes anything that can be used to identify, locate, or contact a person.[25] While some may argue this information is not necessarily private,[26] if it ends up in the wrong hands, it can be quite harmful.[27] Cyberattacks leading to data theft or made possible by company misuse of PII may cause consumers personal harm (e.g., a sense of insecurity about one's private affairs) or financial harm (e.g., fraudulent credit card expenses or identity theft).[28] According to a Norton study, as of 2010, roughly three-quarters of U.S. web surfers had fallen victim to cybercrimes including computer viruses, credit card fraud, and identity theft.[29]

A. *A Lingering Threat Left Unsolved*

Hackers do not discriminate. Many of the most prominent companies in the United States and abroad have been hacked over the past three years. This includes extramarital affairs site Ashley Madison (37 million users exposed),[30] Yahoo (three billion user accounts

---

[24] Stringer, *supra* note 9.

[25] *Id.*

[26] *See* U.S. SECURITIES AND EXCHANGE COMMISSION, PRIVACY IMPACT ASSESSMENT (PIA) GUIDE 2 (2007), https://www.sec.gov/about/privacy/piaguide.pdf ("PII should not be confused with 'private' information. Private information is information that an individual prefers not to make publicly known, e.g., because of the information's sensitive nature. Personally identifiable information is much broader in scope and includes all information that can be used to directly or indirectly identify individuals.").

[27] *What Are the Dangers of PII*, PENN ARTS & SCIENCES (2010), http://yourdata.sas.upenn.edu/content/what–are–dangers–pii.

[28] *Id.*

[29] Eli Talmor, *Cybercrime Victims Feel Ripped Off*, INFOSEC ISLAND (Sept. 20, 2010), http://www.infosecisland.com/blogview/8042–Cybercrime–Victims–Feel–Ripped–Off.html.

[30] Frank Jennings, *You've Been Hacked. What Are You Liable For?*, THE REGISTER (Oct. 14, 2016), https://www.theregister.co.uk/2016/10/14/been_hacked_what_are_you_liable_for/.

exposed), Deloitte, Equifax, Chipotle, Verizon,[31] the Federal Reserve,[32] law firms like Cravath, Swaine & Moore LLP[33] and Mossack Fonseca,[34] JPMorgan Chase,[35] and even the United States Presidential election (via the Democratic National Convention).[36]

With the expansion of smart technology and use of mobile platforms, the trend will probably only increase.[37] As a consequence, consumer trust is dropping and insecurity concerns are rising.[38] Despite the increase in cybersecurity threats and the influx of PII, "companies appear unaware of the growing trend in both the scale and sophistication of cyber security threats."[39] For example, a Ponemon Institute study revealed that "40 [percent] of companies do not scan their mobile apps for security vulnerabilities"; almost "40 percent of the more than 400 organizations surveyed do not review code for security weaknesses, and 33 percent never even test their apps before release"; organizations do not have policies in place for acceptable mobile app use; and most companies have not

---

[31] *See* Burgess, *supra* note 6.

[32] Jose Pagliery & Patrick Gillespie, *Federal Reserve Under Attack by Hacker Spies*, CNN (June 2, 2016), http://money.cnn.com/2016/06/01/technology/federal–reserve–hack/.

[33] Sara Randazzo & Dave Michaels, *U.S. Charges Three Chinese Traders With Hacking Law Firms*, WALL ST. J. (Dec. 27, 2016), http://www.wsj.com/articles/u–s–charges–three–chinese–traders–with–hacking–law–firms–1482862000.

[34] This is the law firm that was breached in the "Panama Papers" scandal of 2016. Jessica Durando, *Panama Papers: What We Know Now*, USA TODAY (May 9, 2016), http://www.usatoday.com/story/news/world/2016/05/09/panama–papers–leak–documents–tax–shelters/84132964/.

[35] Kevin Dugan, *New Rule Would Require City Firms to Hire Cybersecurity Officers*, N.Y. POST (Sept. 13, 2016), http://nypost.com/2016/09/13/new–rule–would–require–city–firms–to–hire–cybersecurity–officers/.

[36] Associated Press, *Top US Intelligence Officials to Testify on Russian Hacking*, CNBC (Jan. 5, 2017) http://www.cnbc.com/2017/01/05/top–us–intelligence–officials–to–testify–on–russian–hacking.html.

[37] *See Hacked*, *supra* note 8 ("'If you haven't been hacked yet, the chances are even greater in 2017.'").

[38] *New Study Shows Public Does Not Trust Social Media Privacy, Supports Stronger Privacy Laws*, ELECTRONIC PRIVACY INFO. CTR. (Oct. 19, 2016), https://epic.org/2016/10/new–study–shows–public–does–no.html. In a survey supported by the Craig New Mark Foundation, a majority of Americans "expressed concern about the lack of safety online, including fears over identity theft, email hacking, and non–consensual online tracking." *Id.*

[39] Lambert, *supra* note 15.

or do not know if they have inspected their cloud services for malware.[40] This study is alarming, and to make matters worse, "[m]any Americans think privacy laws are too weak," including millennials, who "are increasingly aware of the need for stronger privacy laws."[41]

What makes data theft cases so complicated (and data misuse so potentially detrimental), is that hackers are often not caught.[42] "Catching hackers remains a tough, tough job," and "the police can't keep up."[43] This means the liability for data theft or misuse shifts away from the culprit and to the companies and consumers. On one end, companies should adapt their business practices to the changing times.[44] According to Garnet, an information technology research company, "[o]rganizations should focus on how to detect and respond to malicious behaviors and incidents instead of trying to prevent every threat," as they are doing now.[45] On the other end, con-

---

[40] Christine Kern, *Ponemon Study Reveals Startling Lack of Security In Mobile Apps*, INNOVATIVE RETAIL TECHS. (Mar. 30, 2015), https://www.innovativeretailtechnologies.com/doc/ponemon-study-reveals-startling-lack-of-security-in-mobile-apps-0001; *Netskope and Ponemon Institute Study: Majority of Businesses Have Not Inspected Cloud Services for Malware*, NETSKOPE (Oct. 12, 2016, https://www.netskope.com/press-releases/netskope-ponemon-institute-study-majority-businesses-not-inspected-cloud-services-malware/ [hereinafter *Netskope*].

[41] *Id.*

[42] James Andrew Lewis, the Senior Vice President and Director at Center for Strategic International Studies, and an ex–Foreign Service officer, stated, "We don't catch most cybercriminals and we don't catch the most successful . . . [s]o far there is impunity for cybercriminals." Tom Risen, *Study: Hackers Cost More Than $445 Billion Annually*, U.S. NEWS (June 9, 2014), http://www.usnews.com/news/articles/2014/06/09/study–hackers–cost–more–than–445–billion–annually.

[43] Charles Orton-Jones, *Catching Hackers is Not Getting Easier*, RACONTEUR (Mar. 8, 2016), https://www.raconteur.net/technology/catching-hackers-is-not-getting-easier.

[44] *See* Lambert, *supra* note 15 ("The scale and vitriolic nature of attacks are becoming more profound. Even with the well documented adverse effects of a hack, many companies do not have sufficient policies in place to protect against this threat nor do they possess an adequate response plan for an attack.").

[45] Christy Pettey & Rob van der Meulen, *Gartner Says By 2020, 60 Percent of Digital Businesses Will Suffer Major Service Failures Due to the Inability of IT Security Teams to Manage Digital Risk*, GARTNER (June 6, 2016), http://www.gartner.com/newsroom/id/3337617.

sumers must also bear some sort of burden of knowing how to handle sensitive information—who to give it to, when to expect its safekeeping, and knowing the risks of voluntarily handing it over.[46]

Though it is clear that these things must happen, the question then becomes, which party, governmental or otherwise, should ensure that they do?

B. *An Absence of Congressional Efforts*

At a time where consumers and companies are pitted against each other—because hackers are typically not caught—Congress' legislative efforts have failed to keep up.[47] To its credit, some existing statutes protect consumers from risky business practices and regulate the exchange of sensitive information—to an extent.[48] Currently, there are several prominent statutes:

- the Fair Credit Reporting Act of 1970 ("FCRA"),[49] designed to regulate the collection of credit information;

- the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"),[50] designed to increase credit and debit card protection;

- the Federal Debt Collection Practices Act of 1977 ("FDCPA"),[51] designed to battle abusive debt collection practices;

---

[46] *Computer Security*, FED. TRADE COMM'N (June 2017), https://www.consumer.ftc.gov/articles/0009-computer-security.

[47] Martha Wrangham & Gretchen A. Ramos, *Calls for Federal Breach Notification Law Continue After Yahoo Data Breach*, NAT'L L. REV. (Oct. 5, 2016), http://www.natlawreview.com/article/calls–federal–breach–notification–law–continue–after–yahoo–data–breach.

[48] *See Hacked*, *supra* note 8 ("[P]ersonal data has become a huge area of concern, with strict new laws regarding the sharing and dissemination of medical history (HIPAA), misinformation in credit reports (Fair Credit Reporting Act), and many others.").

[49] 15 U.S.C. § 1681 (2012).

[50] *Id.* § 1681c.

[51] *Id.* § 1962.

- the Video Privacy Protection Act of 1988 ("VPPA"),[52] designed to protect video-related disclosures;

- the Telephone Consumer Protection Act of 1991,[53] designed to restrict telephone solicitations; and

- the Health Information Portability and Accountability Act of 1996 ("HIPAA"),[54] designed, in part, to protect health information.

However, aside from HIPAA, which provides data breach notification guidelines and penalty guidelines for different types of breaches,[55] Congress has yet to pass any other statutes to incentivize threshold cybersecurity measures or to guide companies' reactions to data breaches.[56]

Congress' failed attempts at passing such data protection laws in 2014 and 2015 have stalled federal breach legislation.[57] Instead, there is an "existing spread of 47 state [breach notification] laws."[58] Even after Russia's cyberattack on the United States' 2016 Presidential election and the proposed creation of a new Senate Cybersecurity Subcommittee, there have been no more fruitful efforts on the way.[59] In the absence of such laws, the aftermath of a breach (the most recent example being the Equifax breach that affected 145 mil-

---

[52] 18 U.S.C. § 2710.

[53] 15 U.S.C. § 552.

[54] 45 C.F.R. §§ 160.103, 164.400–414; 42 U.S.C. § 1320d.

[55] *See* STEPTOE & JOHNSON LLP, COMPARISON OF US STATE AND FEDERAL SECURITY BREACH NOTIFICATION LAWS 188–92 (2016), https://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf.

[56] *See* Wrangham & Ramos, *supra* note 47.

[57] *Id.*

[58] *Id*. For more information on the different state laws see generally STEPTOE & JOHNSON LLP, *supra* note 55.

[59] Jessica Schulberg & Laura Barrón-López, *John McCain To Create New Senate Cybersecurity Subcommittee*, HUFFINGTON POST (Jan. 5, 2017), http://www.huffingtonpost.com/entry/john–mccain–cybersecurity–subcommittee_us_586ec07ae4b099cdb0fc5c1d.

lion Americans) follows a "familiar script: white-hot, bipartisan outrage, followed by hearings and a flurry of proposals that [go] nowhere."[60]

"The lack of legislative response has industry groups and lawmakers . . . uttering a familiar refrain: Wait until next year."[61] Waiting until next year means companies and consumers are left to resort to navigating forty-plus different state standards regarding data protection and breach response.[62] It also means that uncertainty over consumer rights and data protection guidelines does not seem likely to be eased by Congress any time soon. In essence, it is hard to expect anything from Congress, which only leaves what it has in place—the above-mentioned consumer protection statutes.

C. *The Limited Power of the Federal Trade Commission*

The FTC is a congressionally created federal agency empowered by the Federal Trade Commission Act of 1914 to regulate commerce.[63] It serves as the chief federal agency on privacy policy and consumer protection.[64] Among other duties, it investigates companies and takes law enforcement action to ensure that companies are keeping their promises and implementing adequate security measures.[65]

---

[60] Martin Matishak, *After Equifax Breach, Anger but No Action in Congress*, POLITICO (Jan. 1, 2018), https://www.politico.com/story/2018/01/01/equifax-data-breach-congress-action-319631.

[61] *Id.*

[62] *Id.*

[63] 15 U.S.C. § 45 (2012).

[64] *_Bureau of Consumer Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about–ftc/bureaus–offices/bureau–consumer–protection (last visited Feb. 11, 2018).

[65] *Id.* Section 5(a) of the FTC Act empowers the agency to "prevent persons, partnerships, or corporations . . . from using . . . *unfair* or *deceptive* acts or practices in or affecting commerce." 15 U.S.C. § 45 (emphasis added). Unfair practices refer to when companies employ data security practices that cause or are likely to cause substantial injury to consumers. Deceptive practices refer to when companies make materially misleading statements or omit material information about their practices (usually on their privacy policies).

While the FTC has increased focus on consumer protection,[66] its power is limited to the enforcement of laws.[67] So, while the FTC serves as a deterrent by writing privacy guidelines and fining companies, it does so only based on already established statutes.[68] "While the FTC . . . has attempted to curb harmful practices by data brokers . . . to protect consumers, there is very limited, if any, historical precedent for consumers' ability to challenge the inappropriate aggregation and disclosure of their personal information."[69] In sum, without new legislation, the FTC is limited in its fight to protect consumers against data theft and data misuse. Consumers affected by data theft or misuse would need to file suit in court to seek monetary compensation for any harm caused,[70] which means that, at least for now, the judicial branch is at the forefront of the data privacy issues.

D. *The Unfortunate Role of Constitutional Standing*

As consumers seek redress for data theft and data misuse in courts, and without any sign of congressional efforts coming, the Supreme Court may find itself in the driver's seat regarding laws for data privacy and protection. It has already spoken on the issue, albeit

---

[66] *See* Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news–events/press–releases/2012/08/google–will–pay–225–million–settle–ftc–charges–it–misrepresented. Jon Leibowitz, Chairman of the FTC, has stated that "[n]o matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place." *Id.* Also, recently the FTC increased the maximum civil penalty amount from $16,000 to $40,000 for each day of the violation. Press Release, Fed. Trade Comm'n, FTC Raises Civil Penalty Maximums to Adjust for Inflation (June 29, 2016), https://www.ftc.gov/news–events/press–releases/2016/06/ftc–raises–civil–penalty–maximums–adjust–inflation.

[67] *See Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement (last visited Feb. 11, 2018).

[68] *See* Rafae Bhatti, *Standing in Privacy Lawsuits: Is the Tide Turning in Favor of Consumers?* 5–6 (March 3, 2016) (unpublished comment), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2741514.

[69] *Id.*

[70] *Id.* ("The standing to sue . . . is part of an important framework to enable individuals allegedly harmed by data brokers to protect their own right of privacy.").

quite unclearly (as is demonstrated in Parts III and IV), in two cases that extended to the privacy sphere: *Clapper v. Amnesty International USA*[71] (a quasi-data theft suit) and *Spokeo, Inc. v. Robins*[72] (a data misuse suit).

In both *Clapper* and *Spokeo*, the Court gave blurry guidelines focused on Article III constitutional standing; specifically, its injury-in-fact requirement.[73] This created a circuit split regarding standing for both data theft and data misuse cases, with many courts unwilling to confer standing for consumer plaintiffs.[74] Standing has become such an obstacle that a federal magistrate judge has come to describe it as the "Kilimanjaro" of data privacy cases.[75]

Because of the ensuing circuit splits the Court is likely to again find itself in a position to define data privacy rights and liabilities going forward—at least until Congress speaks. Because data privacy litigation has centered on constitutional standing, Part II provides a brief background, especially as it relates to privacy cases.

II. CONSTITUTIONAL STANDING REQUIREMENTS AND THE CONFUSING INJURY-IN-FACT JURISPRUDENCE

A. *Brief Background*

The United States Constitution limits the jurisdiction of federal courts through Article III's case and controversy requirement.[76] "No principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies."[77] Where the Court finds an actual case or controversy, it gives plaintiffs standing

---

71 568 U.S. 398 (2013).

72 136 S. Ct. 1540 (2016).

73 *See infra* Parts III, IV.

74 *See* Bhatti, *supra* note 68, at 4; *see also* John Biglow, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943, 943 (2016).

75 *In re* Google, Inc. Privacy Policy Litig., 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013).

76 U.S. CONST. art. III, § 2. *See also* Summers v. Earth Island Inst., 555 U.S. 488, 492–93 (2009); DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 340–41 (2006).

77 Simon v. Eastern Ky. Welfare Rights Org., 426 U.S. 26, 37 (1976) (citation omitted).

to sue, which ensures they have "such a personal stake in the outcome of the controversy as to warrant [their] invocation of federal-court jurisdiction . . . ."[78]

To establish standing, (1) the plaintiff must have suffered an "injury-in-fact" that is "concrete and particularized"; (2) the plaintiff's injury must be traceable to the defendant's alleged conduct; and (3) the plaintiff's injury must be likely to be redressed by a favorable judicial decision.[79] This Note focuses solely on the injury-in-fact element, as it is the focus of standing in privacy cases.

B. *Injury-In-Fact Requirements and Privacy Suits*

The Supreme Court defined the characteristics of an injury-in-fact: the injury must be (1) "an invasion of a legally protected interest," (2) that is "concrete and particularized," and (3) that is "actual or imminent, not conjectural or hypothetical."[80] Unfortunately, the Court's prolonged lack of guidance for assessing these requirements has caused scholars to critique standing jurisprudence and lower courts to produce inconsistent results.[81]

The presence of an injury-in-fact is crucial in privacy litigation, as it often leads to early dismissals for a lack of standing.[82] For data theft cases, the main contention is whether the threat of future harm is sufficiently imminent.[83] A court's holding on the imminence of harm opens or closes the door to plaintiffs who seek compensation for the costs of data theft. Such expenses include mitigation costs,

---

[78] Warth v. Seldin, 422 U.S. 490, 498 (1975) (quoting Baker v. Carr, 369 U.S. 186, 204 (1962)).

[79] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

[80] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan*, 504 U.S. at 560).

[81] *See generally* Lee A. Albert, *Standing to Challenge Administrative Action: An Inadequate Surrogate for Claim for Relief*, 83 YALE L.J. 425, 492 (1974) (suggesting that the standing question should not be injury-in-fact, but cause of action); David P. Currie, *Misunderstanding Standing*, 1981 SUP. CT. REV. 41, 42 (same).

[82] *See* Amanda Fitzsimmons, et al., *Seventh Circuit: Victims of Data Breaches Have Article III Standing to Litigate Class Action Lawsuits*, DLA PIPER (July 23, 2015), https://www.dlapiper.com/en/us/insights/publications/2015/07/seventh-circuit-victims-of-data-breaches/ ("[A]n overwhelming majority of courts have dismissed data breach consumer class actions at the outset due to a lack of cognizable injury-in-fact[.]").

[83] *See infra* Part III.

like credit monitoring services to protect themselves from fraud,[84] unjust enrichment costs from the overpayment of services that they believed would keep their PII secure (e.g., credit monitoring),[85] a loss in the intrinsic value of their PII,[86] or emotional distress caused by the threat of harm.[87]

For data misuse cases (like *Spokeo*), courts examine whether an injury is sufficiently concrete by looking at whether the violated statutory provision is tied to a legally protected interest.[88] All of the same injuries alleged in data theft cases may apply, in addition to the statutory violation possibly being a constitutional harm in and of itself.[89]

1. LEGALLY PROTECTED INTERESTS AS A VIOLATION OF THE LAW

Legally protected interests may include common law rights such as those established in property, contract, and tort law, as well as constitutional rights and statutory rights created by Congress.[90] Absent an acknowledgement by the legal system and "until some

---

[84] *See, e.g.*, Lewert v. P.F. Chang's China Bistro, 819 F.3d 963, 964 (2016) (plaintiff sought compensation for the time and expense incurred to prevent and monitor fraudulent charges after a data breach).

[85] Plaintiffs allege that they overpaid for services because they paid for a certain service relying on the idea that such a payment included the adequate security of their information. *See e.g.*, Attias v. CareFirst, Inc., 199 F. Supp. 3d 193, 202 (D.D.C. 2016) (plaintiffs alleged that the payment they inherently paid in security as part of their full payment "[was] not equivalent [to] the security value" actually provided). *Id.*

[86] Plaintiffs allege that the value of their personal information has decreased as a result of a breach or misuse of their information. *See e.g.*, *Attias*, 2016 WL 4250232, at *5 (plaintiffs argued that data breach "negatively impacted [the datas] value.").

[87] *See* Reilly v. Ceridian Corp., 664 F.3d 38, 41–42 (3d Cir. 2011) (plaintiff alleged "an increased risk of identity theft, . . . costs to monitor their credit activity, and . . . *emotional distress*" as harm) (emphasis added).

[88] *See infra* Part IV.

[89] *See* Church v. Accretive Health, Inc., 654 F. App'x 990, 994–95 (11th Cir. 2016) (finding violation of the Fair Debt Collection Practices Act as sufficient for constitutional harm because it conferred a right to adequate disclosures).

[90] *See* Tenn. Elec. Power Co. v. Tenn. Val. Auth., 306 U.S. 118, 137 (1939) ("[T]he right invaded is a legal right,—one of property, one arising out of contract, one protected against tortious invasion, or one founded on a statute which confers

source of law creates a relevant legal interest and a right to bring suit," a factual injury may not typically suffice for standing.[91]

With regards to privacy and consumer protection, the question becomes whether there exists an "understanding of law"[92] sufficient to create a legally protected interest in the correct use, adequate protection, and appropriate dissemination of one's PII. In other words, while Congress and the Supreme Court have acknowledged "the right to privacy [as] a personal and fundamental right protected by the Constitution of the United States,"[93] it remains to be consistently determined whether today's privacy—the protection of personal data such as PII—is a legally conferred right.

2. THE CONCRETE AND PARTICULARIZED REQUIREMENT

Prior to *Spokeo*, courts tended to treat the concrete and particularized elements as one—now they are separately analyzed.[94] Particularity ties into the idea that federal courts do not owe protection to "generalized grievances," which are injuries "often said to be suffered 'by all or a large class of citizens.'"[95] The generalized grievance doctrine "is based on the notion that if parties seek to redress public harms, they must do so via the political branches and not the courts."[96] As for the second requirement, the definition of concreteness remains fuddled and is a major point of contention in privacy

---

a privilege.") (footnote omitted), *abrogated by* Bond v. United States, 564 U.S. 211 (2011).

[91] Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 639–40 (1999).

[92] *Id.* at 641.

[93] 5 § U.S.C. 552(a) (2012).

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

[95] Ryan Guilds, *A Jurisprudence of Doubt: Generalized Grievances As A Limitation to Federal Court Access*, 74 N.C. L. REV. 1863, 1864 (1996) (quoting Warth v. Seldin, 422 U.S. 490, 499 (1975)). "Generalized grievances are a subcomponent of standing doctrine and encompass a set of doctrinal limitations on federal court access." *Id*.

[96] Kimberly N. Brown, *Justiciable Generalized Grievances*, 68 MD. L. REV. 221, 221 (2008). For example, prior cases like *Defenders of Wildlife* stated that for standing purposes, citizens would have to show that they are affected in a personal and individual way in the sense that their grievances were not widely shared. *See* Sunstein, *supra* note 91, at 639–40. This stemmed from the idea that "the role of the courts is to protect individual rights, and that when numerous people are . . . injured, their remedy is political rather than judicial." Antonin

litigation.[97] In theory, concreteness means that an injury must be *de facto*—it "must actually exist" and be "real and not abstract."[98]

3. THE ACTUAL OR IMMINENT REQUIREMENT

Generally, the actual or imminent injury requirement means that injuries cannot be speculative or hypothetical.[99] However, a threat of injury may be sufficient "if the injury is certainly impending."[100] As with concreteness, the Supreme Court has not provided clear guidance as to when a plaintiff crosses the probability threshold for risk of harm to become certainly impending. The imminence required is unknown.[101]

To recap, privacy litigation centers around the injury-in-fact requirement of constitutional standing, which is unclear and undeveloped. In data theft cases, which invoke *Clapper*, the focus is on the concreteness and imminence of the alleged harm, and in data misuse cases, like *Spokeo*, the focus is also on whether the harm is legally cognizable.

III. CLAPPER'S FAILED ATTEMPT TO DEFINE IMMINENCE IN DATA BREACH SUITS

A. *A Necessary Disclaimer*

This Note deals exclusively with data theft cases where plaintiffs allege a risk of future harm *absent any other actual harm*.[102] In other

---

Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 882 (1983) ("I suggest that courts need to accord greater weight than they have in recent times to the traditional requirement that the plaintiff's alleged injury be a particularized one, which sets him apart from the citizenry at large."). In other words, one should turn to Congress for a remedy, which in turn can then legislate and, in theory, create standing for individuals who share any injury.

97 *See infra* Part III.

98 *Spokeo*, 136 S. Ct. at 1548.

99 Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

100 Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

101 *See, e.g.*, *id.* at 1142–45 (providing two separate standards for imminence: the certainly impending standard and the substantial risk standard).

102 *Cf.* Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 398–99 (2014) (listing two classes of data breach cases: Class I cases in which the plaintiff has suffered a financial loss stemming from a data breach, and Class II cases in which the

words, data theft means just that—data theft without anything more. This distinction is made because it is already largely settled that in cases of *actual misuse of information by hackers*, a plaintiff has suffered "ongoing, present, distinct, and palpable harms" sufficient for standing.[103] On the other hand, federal circuit courts are split on whether injuries from data theft alone, which involve *future harm* or *preventive measures to avoid future harm*, are sufficient for constitutional standing.[104]

B. *The Creation of a Circuit Split for Imminence of Harm*

At first, the threat of future harm following data theft seemed like it would be sufficient for standing. The Seventh Circuit held in *Pisciotta v. Old National Bancorp*,[105] a case of first impression, that where customers' names, addresses, social security numbers, driver's license numbers, dates of birth, and other financial information were stolen,[106] the plaintiffs had standing because of their alleged mitigation costs. They had "incurred expenses in order to prevent their confidential personal information from being used and continue to incur expenses in the future."[107] In *Krottner v. Starbucks Corp.*,[108] the Ninth Circuit held similarly that breach victims who had their "names, addresses, and social security numbers" stolen alleged a future threat of harm.[109]

---

plaintiff has taken steps to prevent future harm stemming from a data breach or they have alleged that future harm is imminent due to a data breach). This Note deals exclusively with "Class II" cases.

[103] Enslin v. The Coca-Cola Co., 136 F. Supp. 3d 654, 664 (2015) (finding an injury-in-fact where plaintiff alleged theft of funds from his bank accounts, unauthorized use of credit cards, and the unauthorized issuance of new credit cards); *see also In re* Target Corp. Data Security Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding plaintiffs to have standing where their credit cards were used to make unauthorized purchases).

[104] *See* Biglow, *supra* note 74, at 943.

[105] 499 F.3d 629, 631–34 (7th Cir. 2007).

[106] *Id.*

[107] *Id.*

[108] 628 F.3d 1139, 1140 (9th Cir. 2010).

[109] *Id.* at 1143. The court found that the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data" that was different from more "conjectural or hypothetical allegations," such as if, "[p]laintiffs had sued based on the risk that it would be stolen at some point in the future." *Id.*

However, the Third Circuit created a split in *Reilly v. Ceridian Corp.*, which denied standing on similar facts.[110] The plaintiffs "first name[s], last name[s], social security number[s] . . . birth date[s] and[] the bank account[s] that [are] used for direct deposit"[111] were stolen by hackers.[112] The court found that "an increased risk of identity theft . . . costs to monitor their credit activity, and . . . emotional distress," were hypothetical and "attenuated, because [they were] dependent on entirely speculative, future actions of an unknown third-party."[113]

C. Clapper *as the Answer?*

In 2013, the Supreme Court heard *Clapper*, which though not particularly catered to a data theft setting, would examine the future threat of harm—imminence—as to standing.[114] The case arose because Section 1881a of the Foreign Intelligence Surveillance Act allowed the Attorney General and the Director of National Intelligence to acquire intelligence through the surveillance of individuals who were not "United States persons."[115] The plaintiffs (U.S. citizen attorneys, human rights activists, media organizations, and others) alleged that, because they regularly engaged in "international communications with individuals who [were] likely targets of surveillance," they had to take costly and burdensome measures to protect the confidentiality of such communications, which would likely be acquired through the Section 1881 protocol. [116]

The Court denied standing because plaintiffs "[did not] demonstrate [that] the future injury . . . [was] *certainly impending* and because they [could not] manufacture standing by incurring costs in

---

110 664 F.3d 38, 41–42 (3d Cir. 2011).

111 *Id.*

112 *Id.*

113 *Id.* The court explained that the speculation included having to believe that the hacker "read, copied, and understood their personal information; . . . intends to commit future criminal acts by misusing the information; and . . . is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names." *Id.*

114 Clapper v. Amnesty Int'l USA, 568 U.S. 398, 407–22 (2013).

115 *Id.* at 404–05.

116 *Id.* at 406–07.

anticipation of non-imminent harm."[117] Their allegations, the Court stated, relied on a "highly attenuated chain of possibilities."[118]

On its face, this was a final blow to data theft consumers who also had to take costly precautions to avoid future harm. Many believed *Clapper* would end data theft suits solely grounded on future harm claims.[119] "While *Clapper* was not a data breach case, its analysis is particularly applicable in such cases where the plaintiff's sole allegation of harm is that he is in imminent danger of future harm by virtue of his identity having been stolen."[120]

D. *The Circuit Split Persists Through the "Substantial Risk" Standard*

While various courts agreed with *Clapper* and quickly dismissed claims,[121] the Seventh Circuit did not. In *Remijas v. Neiman Marcus Grp., LLC*, it re-established the split when it found standing in a data theft case, stating that "*Clapper* does not . . . foreclose any use whatsoever of future injuries to support Article III standing."[122] In *Remijas*, the plaintiffs had their credit card numbers stolen and alleged that, because "unreimbursed fraudulent charges and identity theft may happen," they had to incur "necessary" and "immediate preventative measures."[123] *Remijas* relied on a lower standard of imminence cited in a footnote in *Clapper*, which stated that sometimes "[the Court] found standing based on a *'substantial risk'* that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid the harm."[124]

---

[117] *Id.* at 422 (emphasis added).

[118] *Id.* at 410.

[119] S*ee Does Clapper Silence Data Breach Litigation? A Two-Year Retrospective*, INFOLAWGROUP LLP (Feb. 25, 2015), https://www.infolawgroup.com/2015/02/articles/breach-notice/does-clapper-silence-data-breach-litigation-a-two-year-retrospective/ (discussing the possibility that *Clapper* could silence data breach litigation).

[120] Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1283 (M.D. Fla. 2016).

[121] Most courts, consistent with *Clapper*, rejected the threat of future harm as insufficient. *See, e.g.*, Attias v. CareFirst, Inc., 2016 WL 4250232, at *2 (D.D.C. Aug. 10, 2016) (finding the risk of harm too speculative); *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015).

[122] 794 F.3d 688, 693 (7th Cir. 2015).

[123] *Id.* at 692.

[124] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (emphasis added). The Supreme Court acknowledged the substantial risk threshold as lower

The Seventh Circuit distinguished *Remijas* from *Clapper* because it was not speculative that the theft itself occurred: "[t]he hackers deliberately targeted Neiman Marcus to obtain [the plaintiffs'] credit-card information."[125] The court asked, "[w]hy else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[126] The Seventh Circuit reiterated its stance in *Lewert v. P.F. Chang's China Bistro*, where it held that customers whose credit and debit card data was stolen had a concrete injury composed of the time and expense spent to prevent and monitor fraudulent charges.[127] Confusingly, it applied a "certainly impending" standard.[128]

With the Ninth and Seventh Circuits conferring standing and the Third Circuit denying it, a split still exists.[129] It is also unclear if the substantial risk or certainly impending standard applies to data theft. Without any legislation on data theft and with continuing confusion in the courts, obscurity plagues data theft rights and liabilities.

IV. *SPOKEO* FAILS TO ESTABLISH AN ALTERNATE AVENUE FOR STANDING

A. *An Opportunity for Related Clarity*

Clapper left a guidance gap—consumer victims, attorneys, and courts could not predictably gauge whether post-data theft risk of harm was sufficiently imminent for standing. Consequently, these parties anticipated that *Spokeo*—which considered the related question of whether a plaintiff could overcome a standing challenge

---

than certainly impending by stating that "[Clapper] respondents [fell] short of even that standard." *Id.*

125 *Remijas*, 794 F.3d at 693.

126 *Id.*

127 819 F.3d 963, 965 (7th Cir. 2016).

128 The "increased risk of fraudulent credit- or debit-card charges, and the increased risk of identity theft" were "certainly impending" future harms. *Id.* at 966.

129 *Compare id.* (conferring standing), *and* Krottner v. Starbucks Corp., 658 F.3d 1139, 1142–43 (9th Cir. 2010) (conferring standing), *with* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (denying standing).

solely on a company's violation of a consumer protection statute[130]—could offer assistance. *Spokeo* could potentially allow victims of data misuse and some victims of data theft (if there was a statutory violation involved as well) to seek redress in federal courts through a different avenue, that of statutorily conferred standing.[131]

B. *The Creation of the Concreteness Conundrum*

Spokeo arose when Thomas Robins, the named plaintiff, discovered an inaccurate profile of himself on Spokeo, a consumer reporting agency that operates a search engine.[132] Spokeo gathers data about people and creates a profile of them.[133] Robins' profile falsely asserted that he was married (he was not), had children (he did not), was in his late 50s (he was younger), had a job (he was looking for one), was affluent (he was not), and held a graduate degree (he did not).[134] He filed suit alleging, among other claims, that Spokeo violated the FCRA by failing to "follow reasonable procedures to ensure maximum possible accuracy [of information]."[135] The harm, he alleged, was that the inaccurate profile caused him to miss out on employment opportunities because it "made him appear overqualified . . . expectant of a higher salary . . . and less mobile . . . ."[136]

In its analysis, the Court focused exclusively on the particularization and concreteness prong of the injury-in-fact analysis.[137] The Court held that Robins' claims were particularized, without much

---

130 Brandon N. Robinson & Gregory C. Cook, *One Month Later: Reflections On the Impact of Spokeo*, LAW360 (June 20, 2016), https://www.law360.com/articles/807734/one-month-later-reflections-on-the-impact-of-spokeo ("The much anticipated question that the court was asked to address revolved around whether Robins could bring a claim under the FCRA based solely on the publishing of inaccurate information alone, without evidence of any actual injury.").

131 *Id.*

132 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544–46 (2016).

133 *Id.*

134 *Id*. at 1546.

135 *Id.*

136 *Id*. at 1554 (Ginsburg, J., dissenting).

137 *Id.* at 1546–47 (majority opinion).

discussion.[138] Regarding concreteness, the Court remanded the analysis back to the Ninth Circuit.[139] In dictum, it provided limited guidance by stating that an injury must be *de facto*—it "must actually exist" and be "real and not abstract."[140] Concrete is "not necessarily synonymous with 'tangible.'"[141]

Most importantly, it stated that courts should look at history and congressional judgment to determine concreteness.[142] Regarding history, courts must consider if the "intangible harm has a close relationship to a harm that has traditionally been regarded as providing basis for a lawsuit."[143] Regarding congressional judgment, Congress is "well positioned to identify intangible harms" and may elevate the status of an injury to "concrete" by conferring statutory rights.[144] But, the Court also provided the conflicting view that a "bare procedural violation, divorced from any concrete harm," does not satisfy the injury-in-fact requirement.[145] Even more confusing, the Court also wrote that in *some* circumstances, "the violation of a procedural right granted by statute *can* be sufficient . . . to constitute injury-in-

---

[138] *See id.* at 1548. Because Spokeo violated *his* statutory rights and because he had a personal interest in the handling of his credit information, the Court found his injury sufficiently particularized. *Id.*

[139] *Id.*

[140] *Id.*

[141] *Id*. at 1549 (providing that, for example, the risk of real harm is an intangible harm that may satisfy concreteness).

[142] *Id.*

[143] *Id.*; *see, e.g.*, Vt. Agency of Nat. Resources v. U.S. *ex rel.* Stevens, 529 U.S. 765, 775–77 (2000) (justifying Article III standing for a "*qui tam* relator [claim] under the False Claims Act" because *qui tam* actions were historically prevalent in America and England).

[144] *Spokeo*, 136 S. Ct. at 1544.

[145] *Id.* As an example, the Court explains that while Congress sought to stop the "dissemination of false information" by enacting the FCRA and adopting procedures such as the one allegedly violated by Spokeo, a "bare procedural violation [of the FCRA]" would not satisfy Article III because it may result in no harm. *Id*. at 1550 ("not all inaccuracies [by FCRA regulated agencies] cause harm or present any material risk of harm"). "It is difficult to imagine how the dissemination of an incorrect zip code . . . could work any concrete harm." *Id.*

fact,"[146] and a plaintiff does not have to allege "additional harm beyond the one Congress has identified."[147]

In short, *Spokeo* left an unclear understanding of concreteness and failed to state whether a congressional statute ordering companies to safeguard or display PII in certain ways is sufficient for standing. The Court merely provided history and congressional judgment as talking points for concreteness (without actually doing the analysis itself) and vaguely differentiated between procedural and substantive statutory violations.

C. *A Post-*Spokeo *Circuit Split*

Spokeo's lack of clarity resulted in a brewing circuit split—the case has "produced divergent decisions in cases with similar fact patterns."[148] It remains unclear whether a mere statutory violation is sufficient for standing in privacy claims.[149] While the Eleventh Circuit and the D.C. Circuit demonstrated an expansive view of *Spokeo* (conferring standing), the Sixth, Seventh, and Eighth Circuits, showed a restrictive view (denying standing).[150] As demonstrated

---

[146] *Id.* (emphasis added).

[147] *Id.*; *see, e.g.*, Fed. Election Comm'n v. Akins, 524 U.S. 11, 20–25 (1998) (confirming that a group of voters' "inability to obtain information" that Congress had decided to make public is sufficient injury-in-fact to satisfy Article III).

[148] Allison Grande, *Spokeo Split: How High Court's Ruling is Being Interpreted*, LAW360 (Dec. 2, 2016), https://www.law360.com/articles/865734/spokeo-split-how-high-court-s-ruling-is-being-interpreted.

[149] David Lender, et al., *A Circuit Split Emerges As Lower Courts Weigh In On Spokeo*, LAW360 (Sept. 15, 2016), https://www.law360.com/articles/839978/a-circuit-split-emerges-as-lower-courts-weigh-in-on-spokeo.

[150] *See* Church v. Accretive Health, Inc., 654 F. App'x 990, 991–92 (11th Cir. 2016) (conferring standing where, in violation of the Fair Debt Collection Practices Act, the plaintiff received a letter by the defendant that omitted certain statutorily required disclosures causing plaintiff to get "very angry" and "cr[y] a lot."); *see also* Galaria v. Nat'l Mutual Ins. Co., 663 F. App'x 384, 385 (6th Cir. 2016) (conferring standing in a data breach case where the plaintiff alleged an FCRA violation). *But see Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 513–15 (D.C. Cir. 2016) (defendant's violation of the D.C. Consumer Identification Information Act and the D.C. Consumer Protection Procedures Act by requesting customers' zip codes in connection with credit card purchases is not a concrete Article III injury); *see also* Braitberg v. Charter Comm., Inc., 836 F.3d 925, 930–31 (8th Cir. 2016) (defendant's cable company's retention of personal information in violation of Cable Communications Policy Act does not merit standing without some other harm); Meyers v. Nicolet Rest. of De Pere, LLC, 843 F.3d 724, 728–

by the following chart (Chart 1) compiled by attorneys at Morgan Lewis & Bockius LLP, after *Spokeo*, courts have inconsistently determined standing founded on consumer protection statutes (even in cases with the same statute):

Chart 1[151]

	Standing	*No Standing*	*Totals*	*Percent Finding Standing*
FACTA	4	4	8	50%
FCRA	18	25	43	42%
FDCPA	24	3	27	89%
TCPA	23	6	29	79%
Other	36	30	66	55%
TOTAL	105	68	173	61%

While it may be that this split is due in part to the different nature and factual requirements of statutes, the courts' differing analyses demonstrate that there is more than just a factual inconsistency within these cases. While courts often employed the historical and congressional intent analysis suggested by *Spokeo*,[152] they have carried it out in a highly inconsistent manner, leading to unpredictable results. The following subsections explain how courts have been applying each prong.

1. HISTORICAL ANALYSIS INCONSISTENCIES

Courts with an expansive view of *Spokeo* (that conferred standing) typically make it a point to recognize the right to privacy as a traditional common law cause of action.[153] This recognition alone

29 (7th Cir. 2016) (the sole failure to truncate a credit card's expiration date as required by FACTA is insufficient to confer Article III standing).

151 Ezra D. Church, et al., *Spokeo 6 Months Later: An Undeniably Dramatic Impact*, LAW360 (Dec. 6, 2016), https://www.law360.com/articles/839978/spokeo-6-months-later-an-undeniably-dramatic-impact.

152 *See, e.g.*, Holderread v. Ford Motor Credit Co., LLC, 2016 WL 6248707, at *3 (E.D. Tex. Oct. 26, 2016) ("As directed by *Spokeo*, the Court should first consider the history of the intangible harm and Congress's judgment.").

153 *See* Matera v. Google Inc., 2016 WL 5339806, at *3 (N.D. Cal. Sept. 23, 2016) (finding that, for centuries, common law had recognized the *right to privacy*, which the Wiretap Act sought to protect); *see also* Yershov v. Gannet Satellite Info. Network, Inc., 204 F. Supp. 3d 353, 362 (D. Mass. 2016) (finding that

bolsters the strength of the statutory provision that has been violated because it alludes to something that the Supreme Court has recognized for standing in the past. On the other hand, courts that have rejected standing do not acknowledge the right to privacy as a cause of action.[154] Nevertheless, this is vaguely and arbitrarily applied.

2. CONGRESSIONAL INTENT INCONSISTENCIES

Courts have had difficulty differentiating between statutorily created procedural and substantive rights. While *Spokeo* clearly stated that virtually[155] all procedural violations are insufficient for standing, it only provided one example of what would qualify as a procedural right: the correct dissemination of a zip code as required by the FCRA.[156] As a consequence, lower courts have either merely compared the statutory provision in question to the dissemination of an incorrect zip code, or just assumed conclusively that a right is substantive or procedural.[157] The former method is inefficient because the FCRA's correct zip code requirement does not establish much of a guidepost,[158] and the latter method because it serves no precedential purpose.

---

the VPPA protected "an individual's *right to privacy* . . . as to certain personal information and private locations," which had long been regarded as a basis for a lawsuit) (emphasis added); Aranda v. Caribbean Cruise Line, Inc., 202 F. Supp. 3d 850, 857–58 (N.D. Ill. 2016) (finding the TCPA codifies the common law tort of right to privacy and seclusion).

[154] *See, e.g.*, *Hancock*, 830 F.3d at 511 (right to privacy not acknowledged).

[155] In some cases, such as FEC v. Akins, 524 U.S. 11 (1998), standing was merited with a mere procedural violation. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016). Akins involved "statutory rights intended to protect and promote public interests"—citizens' right to information that should have been publicly disclosed about candidates running for public office. *Id.*

[156] The Court stated that dissemination of an incorrect zip code may violate the FCRA, but that it is "difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm." *Spokeo*, 136 S. Ct. at 1550.

[157] *See Hancock*, 830 F.3d at 511; *see also* Braitberg v. Charter Comm., Inc., 836 F.3d 925, 927 (8th Cir. 2016).

[158] The only time this works well is when the case deals with extremely similar provisions as *Spokeo*, such as *Hancock*. 830 F.3d at 512. There, the defendant violated D.C.'s Consumer Identification Information Act by requesting zip codes from plaintiffs during credit card purchases, and the court found that plaintiffs "assert[ed] only a bare violation of the requirements." *Id.*

Furthermore, courts have inconsistent ways of distinguishing cases using *Spokeo*'s zip code example: some use the prohibitive language of a statute as a key to finding substantive rights,[159] and others equate procedural rights to duties.[160] Other cases, like *Matera v. Google Inc.*,[161] demonstrate how some courts apply an arbitrary and conclusive analysis to distinguishing between a procedural and a substantive right of action. There, the plaintiff alleged that Google violated the Wire Tap Act because it unlawfully intercepted the contents of Gmail messages.[162] Without giving much explanation, the court found that the Wire Tap Act created a substantive right of action.[163] This is not the only time that a court has employed this type of conclusory analysis.[164]

---

159 *See* Aranda v. Caribbean Cruise Line, Inc., 202 F. Supp. 3d 850, 857 (N.D. Ill. 2016). There, the court conferred standing, by distinguishing a TCPA provision based on the fact that it "prohibit[ed] making certain kinds of telephonic contact" without consumers' consent, instead of "requiring the adoption of procedures to decrease congressionally-identified risks." *Id.* The court stated that, unlike where an agency violates the FCRA by reporting an incorrect zip code (and, thus, the "procedural rights . . . are attenuated enough from the interests Congress identified and sought to protect through the FCRA"), "the TCPA section at issue does not require the adoption of procedures to decrease congressionally-identified risks." *Id.* Instead, it "prohibits making certain kinds of telephonic contact" without consumers' consent. *Id.*

160 *See Braitberg*, 836 F.3d at 931. There, the court equated procedural rights to duties and denied standing on the basis that the right was procedural because it created a duty. *See id.* (stating that "FCRA . . . provides that consumer reporting agencies must 'follow reasonable procedures to assure maximum possible accuracy' of consumer reports."). The plaintiff alleged that defendant, his ex-cable provider, violated the Cable Communications Policy Act when it kept his PII after he canceled the service. *Id.* at 927. The court found that a bare procedural right—the duty to destroy PII—was insufficient for standing. *Id.*

161 2016 WL 5339806, at *23 (N.D. Cal. Sept. 23. 2016).

162 *Id.*

163 *Id.* It merely stated that while the dissemination of an incorrect zip code violated a "reasonable [FCRA] procedure," the Wiretap Act created "substantive rights to privacy in one's communications."

164 *See* Yershov v. Gannet Satellite Info. Network, Inc., 204 F. Supp. 3d 353, 362 n.5 (D. Mass. 2016) (conclusively stating that the VPPA created a "substantive right to prevent and remedy" the type of disclosure performed by Gannet); Church v. Accretive Health, Inc., 654 F. App'x 990, 991–92 (11th Cir. 2016) (conclusively finding a substantive right to receive disclosures without additional explanation).

Even worse, some courts, like the Seventh Circuit in *Meyers v. Nicolet Rest. of De Pere, LLC*, do not distinguish between procedural and substantive rights and just make a blanket assumption that standing requires an additional injury to the statutory violation.[165] Through all of these different methods, courts—unsurprisingly—have interpreted the same statutes and ended up with opposite holdings on standing.[166]

3. COURTS IGNORE THE *SPOKEO* ANALYSIS AND MAINTAIN THE STATUS QUO

Finally, some courts forego the statutory analysis suggested by *Spokeo* and confer standing solely on the imminence of harm (under the *Clapper* analysis).[167] It is as if *Spokeo* did not change anything.[168] One district court even claimed that *Spokeo* "essentially affirmed" the intangible injury requirements set forth in *Clapper*.[169]

In sum, *Clapper* and *Spokeo* have done very little, if anything, to help define privacy rights and liabilities. So, why has the Supreme Court been so vague?

---

[165] 843 F.3d 724, 725 (7th Cir. 2016). There, the court denied standing because consumers showed no actual injury other than that the defendant had failed to properly truncate credit card expiration dates in accordance with the Fair and Accurate Credit Transactions Act. *See id.* (stating that "Congress enacted the FACTA in response to what it considered to be the increasing threat of identity theft."). The court concluded that regardless of whether the right was substantive or procedural, its violation required an accompanying injury. *Id.* at 728–29.

[166] *See* Church, *supra* note 151 and accompanying Chart 1.

[167] *In re Zappos.com*, a data breach case, is an example. *In re* Zappos.com, Inc. Customer Data Sec. Breach Litig., 2016 WL 4521681, at *1 (D. Nev. Aug. 29, 2016). There, the court denied standing, claiming that plaintiffs did not suffer actual damages as a result of the breach. *Id.* at *3. On the other hand, in *Galaria*, another data breach case, the court conferred standing based on the imminent risk of the harm and remanded the FCRA claim (ignoring the *Spokeo* analysis). Galaria v. Nat'l Mutual Ins. Co., 663 F. App'x 384, 391–93 (6th Cir. 2016).

[168] U.S. District Judge James Donato said that he was "skeptical that . . . *Spokeo* . . . was a 'big change of law.'" Dorothy Atkins, *Facebook's Spokeo Bid to End Privacy Suit Faces Skepticisim*, LAW360 (Oct. 27, 2016), https://www.law360.com/articles/856826/facebook-s-spokeo-bid-to-end-privacy-suit-faces-skepticism. He further stated, "'[i]t's old law simply restated . . . [and] [t]here's nothing particularly novel about it.'" *Id.*

[169] *In re* Zappos.com, Inc., 2016 WL 4521681, at *1.

V. WHY SO SILENT: THE DIFFICULTY OF ASSIGNING LIABILITY IN DATA PRIVACY

It may well be that Congress is yet to legislate and that the Court may have erred on the side of being vague (in both *Spokeo* and *Clapper*) because of the impending policy implications attached to any decisive move related to data privacy. It is important to understand what is at stake and why assigning rights and liabilities is so difficult in the privacy space: if consumers can earn standing easily, a floodgate may open, and if it is too hard for them to earn standing, one of their last few avenues for redress may be closed.

A. *The Problem of the Disappearing Culprit*

What makes privacy cases so complicated and difficult to address is that hackers—the truly liable criminals—are virtually never caught.[170] Many times "cybergangs" can complete remote work through "zombie computers," which makes it increasingly difficult to locate the hackers.[171] As cybercrime costs quadrupled from 2013 to 2015 (and continue to increase),[172] cyber attackers continue uncaught.

B. *Who Should Take the Hit: Consumers or Companies?*

Unable to sue the culprits, both companies and consumers must turn elsewhere for redress. If companies implement its security system through a certified vendor, they may be able to sue such vendor.[173] Also, companies sometimes buy cyber insurance to lower the costs of a breach.[174] On the other hand, consumers may try to sue

---

[170] James Andrew Lewis, the Senior Vice President and Director at Center for Strategic International Studies, and an ex-Foreign Service officer, stated that "most cybercriminals . . . and the most successful ones are not caught . . . [and] so far there is impunity for cybercriminals." *See* Tom Risen, *supra* note 42.

[171] Elinor Mills, *Finjan Finds Botnet of 1.9 million Infected Computers*, CNET (Apr. 21, 2009), https://www.cnet.com/news/finjan-finds-botnet-of-1-9-million-infected-computers/.

[172] *See* Morgan, *supra* note 4.

[173] Kristin Casler, *Data Breach Defenses When Consumer Plaintiffs Come Knocking*, LEXISNEXIS (Aug. 15, 2015), https://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2016/08/15/data-breach-defenses-when-consumer-plaintiffs-come-knocking.aspx.

[174] *Id.*

the company—the custodian of their PII—but may encounter constitutional standing obstacles.[175] This is because constitutional standing is the "first avenue of defense" for defendant companies.[176]

Regardless of the varying potential scenarios, from a legislative and judicial standpoint, any future laws or court decisions will essentially decide how to spread liability between consumers and companies. Keeping in mind the respective availability for redress, this Note now examines the policy implications of privacy legislation and jurisprudence. As an introduction, consider the following:

> When it comes to protection of online privacy, you will probably hear the claim that some measures, if implemented, would prevent innovation or destroy the Internet altogether. You will also hear the claim that without protective measures we will . . . end up with a society that sees people as nothing more than consumers.[177]

1. CONSUMER RISKS AND FRIGHT IN A DATA DRIVEN SOCIETY

One could argue that laws should shift liability away from consumers and instead protect them because of the urgent threat of identity theft and other consumer harms caused by data theft and made more likely by data misuse. By providing PII to companies, consumers risk their financial stability, their identity, and potentially even their mental or physical safety.[178] For the fifteenth consecutive year,

---

[175] Maria Vathis & David Zetoony, *The Cybersecurity Question: To Insure Or Not To Insure*, LAW360 (Oct. 31, 2013), https://www.law360.com/articles/481543/the-cybersecurity-question-to-insure-or-not-to-insure.

[176] Gerald D. Silver, *Tips For Defending Data Breach Class Actions*, LAW360 (Mar. 8, 2013), https://www.law360.com/articles/421934/tips-for-defending-against-data-breach-class-actions. A dismissal means consumers may no longer argue on the merits nor seek redress for harms. *Id.*

[177] Irina Raicu, *Are Attitudes about Privacy Changing?*, MARKKULA CTR. FOR APPLIED ETHICS (June 1, 2012), https://www.scu.edu/ethics/privacy/are-attitudes-about-privacy-changing/ [hereinafter *Attitudes*].

[178] *See* M. GRANGER MORGAN, ET AL., THE MANY MEANINGS OF "SMART GRID" 5 (2009), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1026&context=epp. For instance, a hacker could monitor Smart Grid power usage to determine when a consumer is at work, facilitating burglary, unauthorized entry, or worse. *Id. See also* Brief for Electronic Privacy Information Center (EPIC) and Thirty-Two Technical Experts and Legal Scholars as Amici Curiae Supporting

identity theft is the top complaint among consumers.[179] In 2012 alone, more than sixteen-million Americans fell victim to identity thefts, costing over twenty-four-billion dollars—fourteen-billion dollars more than losses attributed to burglary, theft, automobile theft, and all other property crimes.[180] Without adequate company safeguards, hackers can "collect[] consumer profiles that would give them a clear picture of consumers' habits over time, thereby enabling them to predict passwords, challenge questions, or other authentication credentials."[181]

While companies may lose money (and in some scenarios, corporate livelihood) from misused or stolen information, individual victims risk a value unique to them because they face "special threats to [their] ability to structure their lives in unconventional ways."[182] Privacy incursions can cause uniquely detrimental and irreparable effects on individuals.[183] Research in cognitive psychology shows that a "lack of privacy stunts social development and growth, neither of which is fungible or replaceable in human beings."[184]

Furthermore, consumers' right to privacy includes the right to manage and control their personal data, which helps "individuals

---

Respondent at 5, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339) [hereinafter Brief for EPIC] ("Many consumers are unable to obtain jobs or credit because of inaccurate or incomplete information made available by data brokers.").

179 Press Release, Fed. Trade Comm'n, Identity Theft Tops FTC's Consumer Complaint Categories Again in 2014 (Feb. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014.

180 *See* Press Release, Bureau of Justice Stat., 16.6 Million People Experienced Identity Theft in 2012 (Dec. 12, 2013), https://www.bjs.gov/content/pub/press/vit12pr.cfm.

181 FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

182 Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2121 (2001).

183 *See* Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PA. L. REV. 52, 54 (2007).

184 Brief for EPIC, *supra* note 178 (citing Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 n.195 (2000)).

avoid the embarrassment that accompanies the disclosure of certain personal details"; "to preserve human dignity, respect, and autonomy"; and "[to] construct intimacy with others."[185] This line of thinking is tied to a control theory, which conceptualizes privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[186] It follows that companies are in a better position to protect that control because they are the custodians of private information.[187] Therefore, the company in possession should bear the consequences of data misuse or theft.[188]

The FTC has stated that there is a power imbalance between customers and the companies with which they conduct business, especially for companies offering important services such as utilities, which leaves consumers relatively disempowered and without meaningful choice.[189] Others take a step further, arguing that the collection of PII facilitates a company's power to influence or direct consumer behavior.[190] "The ability of a company—a company that you have no relationship with—to know where you live, your de-

---

[185] *Id.* (citing Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1212–16, 1260 (1998)).

[186] Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 766 (2007) (explaining "the control we have over information about ourselves" and the importance of maintaining that control to avoid resulting in "a suffocating powerlessness and vulnerability" from its loss).

[187] *See* Bruce Schneier, *When It Comes to Security, We're Back to Feudalism*, WIRED (Nov. 26, 2012) https://www.wired.com/2012/11/feudal-security/ ("We give companies our data and trust them with our security, but we receive very few assurances of protection in return, and those companies have very few restrictions on what they can do.").

[188] *Id.*

[189] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 51 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. Typically, the business-consumer relationship is already relatively one-sided. For example, for important services, contracts are typically dictated and may be changed at will by companies. *Id.*

[190] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1953 (2013).

mographics, your interests, and how to contact you is unprecedented."[191] To summarize the arguments against precluding consumers from redress:

> None of this is acceptable because it allocates the risk of loss to consumers even though they are in no position to prevent the breach and allows the merchant to escape liability in proximately-caused harms even though it has the power and resources to minimize the risk of these breaches.[192]

2. CORPORATE LENIENCY FOR INNOVATION AND FAIRNESS

There are also strong arguments for corporate leniency, including the protection of innovation, the level of sophistication of modern hackers, the difficulty of making changes so quickly, and the already costly repercussions for victim companies. First, as the role of Congress and the Supreme Court "remains central to defining and reshaping the contours of privacy rights and remedies,"[193] many tech executives like Scott McNealy, who famously proclaimed that "[people] have zero privacy" and that people should "get over it,"[194] may urge for corporate leniency for the sake of innovation.[195] In other words, holding companies to a high security compliance standard would be costly and hinder innovation efforts. Therefore, lawmaking bodies should consider the harmful repercussions that could

---

191 Jeff Jonas, *The Surveillance Society and Transparent You*, *in* PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS 93, 98 (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015).

192 Adam Lamparello, *Online Data Breaches, Standing, and the Third-Party Doctrine*, 2015 CARDOZO L. REV. DE NOVO 119, 127.

193 LAW BUS. RESEARCH LTD, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 288 (Alan Charles Raul ed., 2014), https://www.sidley.com/-/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-states/fileattachment/united-states.pdf [hereinafter PRIVACY].

194 Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED, (Jan. 26, 1999), http://archive.wired.com/politics/law/news/1999/01/17538.

195 *See Attitudes*, *supra* note 177 ("[Y]ou will probably hear the claim that some measures, if implemented, would prevent innovation[.]").

follow from broadening privacy rights, which are integrated with the United States' economy and technological initiatives.[196]

Next, it may be unfair to fault companies that are unable to protect themselves against highly sophisticated hackers. Today's cyberattacks "are more stealthy and malicious than ever before . . . . [and] are programmed to remain unnoticed for as long as possible . . . ."[197] Hackers are no longer "attention-seeking geeks" but instead "part of a highly specialized and distributed criminal ecology."[198] This new level of sophistication can reach any organization from large technology companies (like Yahoo) to the Federal Reserve.[199] The threat applies to small businesses as well (who often make the mistake of thinking they will not be hacked).[200] If the best and most protected organizations are having trouble keeping up with current "inevitable"[201] breaches, then it is likely that small businesses and innovative startup companies may be even further behind.[202] Assuming courts lower the standing threshold, these smaller

---

[196] PRIVACY, *supra* note 193, at v ("[T]he frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations.").

[197] *Data Breach Threat Analysis*, SWORD & SHIELD, https://www.sword-shield.com/security-assessments/data-breach-threat-analysis/ (last visited Feb. 13, 2018).

[198] Lance Cottrell, *Today's Hackers Are Way More Sophisticated Than You Think*, READWRITE (Feb. 4, 2015) http://readwrite.com/2015/02/04/sophisticated-hackers-defense-in-depth/.

[199] *Cf.* Robert E. Sumner, IV & Mindy L. Vervais, *The Typical Data Breach Lawsuit and How to Protect Your Company*, INSIDE COUNSEL (Oct. 1, 2014), http://www.insidecounsel.com/2014/10/01/the-typical-data-breach-lawsuit-and-how-to-protect ("It has been said that there are two types of companies: those that have experienced a data breach and those that *know* they have experienced a data breach.").

[200] Dennis Milewski, *Survey Shows Small Businesses Have Big Data Breach Exposure*, MUNICH RE (Mar. 6, 2013). The Ponemon Institue found in a 2013 study that 55% of small businesses surveyed experienced a data breach. *Id.*

[201] *See* Casler, *supra* note 173.

[202] *See* Penny Crosman, *New York Rewriting Cybersecurity Rules After Banker Pushback*, AM. BANKER (Dec. 22, 2016), https://www.americanbanker.com/news/new-york-rewriting-cybersecurity-rules-after-banker-pushback. While larger companies may be able to adapt to new regulations, and in turn new liabilities, smaller companies may have a harder time adjusting to the requirements. As an example, consider a New York proposal to increase regulation thresholds on encryption for banks, to which many bank groups voiced concerns that, "[s]mall banks have much more limited resources than their larger bank

entities "[would be] at a greater risk of going out of business because of the litigation" costs,[203] potentially hindering innovation.

Third, and related to the prior point, companies may *need* more time to adapt their security methods to the heightening cybersecurity threats. For example, at least as it pertains to healthcare companies (42.5% of which were breached last year), technology is outdated and there is a short supply of qualified professionals (e.g., security engineers), making it difficult for companies to make quick changes and to hire the adequate people.[204] Similarly, "[t]raditional anti-virus/anti-malware vendors continue to lag behind online criminals"[205] and "IT teams need more robust intelligence, protection, and remediation to protect their data from breach or loss."[206] Law-making institutions have to understand what is actually possible. These changes are not going to happen overnight, and Congress and the judicial branch must be weary of making it too costly (through increased compliance standards or easy consumer protection suits) for companies to transition to adequate protection measures.[207]

Finally, one could argue that the status quo may be sufficient to effectuate change because business and legal enforcement costs already push companies to improve security and compliance measures. Even without successful consumer suits or new security compliance regulations, data breaches already cost companies enough money to incentivize them to take measures to avoid future breaches.[208] Each data breach costs companies an average of $5.85

---

brethren, therefore should not be made to meet all the same requirements . . . ." *Id.*

[203] *See* Casler, *supra* note 173.

[204] *See* Tim Cannon, *The Root of the Problem: How to Prevent Security Breaches*, WIRED, https://www.wired.com/insights/2015/02/the-root-of-the-security-problem/ (last visited Feb. 13, 2018). This article also offers investing in education (to account for qualified professional shortage) as a solution to data breach problems, thereby implying that no short-term solution is available. *Id.*

[205] *Data Breach Threat Analysis*, *supra* note 199.

[206] *Netskope*, *supra* note 40.

[207] *See* John Nadolenco & Evan M. Wooten, *Lack of Standing in Data Privacy Cases: Not Just A Federal Court Defense*, MAYER BROWN (July 31, 2014), https://www.mayerbrown.com/de/Lack-of-Standing-in-Data-Privacy-Cases? (claiming that privacy cases have "particularly . . . high costs of discovery and potential exposure").

[208] *See* John Stringer, *Protecting Personally Identifiable Information: What Data Is at Risk and What You Can do About It*, SOPHOS 3 (Oct. 2011),

million, according to the Ponemon Institute.[209] Among this figure, the average cost of defense of a data breach lawsuit comes out to $574,984 and the average settlement to $258,099.[210] International scholars have admired the United States' current privacy enforcement structure:

> Taken together, this enforcement ecosystem has proven to be nimble, flexible, and effective in adapting to rapidly changing technological developments and practices, responding to evolving consumer and citizen expectations, and serving as a meaningful agent of deterrence and accountability. Indeed, the US enforcement and litigation-based approach appears to be particularly well suited to deal with 'recent inventions and business methods'– namely, new technologies and modes of commerce – that pose ever changing opportunities and unpredictable privacy challenges.[211]

Further, these same scholars have also stated that the United States had "success of enforcement in pushing corporate privacy managers . . . to develop state-of-the-art privacy practices . . . ."[212] They attribute the proactive development of privacy policies and standards to the "constant threat and unpredictability of future enforcement by the FTC and parallel state consumer protection officials, combined with the deterrent effect of enforcement actions against peer companies . . . ."[213] As a result of this dynamic, accepting this line of thinking would put a lesser burden on the judicial branch to resolve its privacy standing circuit splits and on Congress to legislate.

---

https://www.sophos.com/en-us/medialibrary/pdfs/other/sophosprotectingpii.pdf (noting "the consequences [of data breaches] include [fines], reputation damage, loss of customer trust, employee dissatisfaction and attrition, and clean-up costs following the breach").

209 *See* Sumner & Vervais, *supra* note 199.

210 *Id.* Other costs include $3,324,959 in lost business. *Id.*

211 PRIVACY, *supra* note 193, at 270.

212 *Id.* at 281.

213 *Id.* at 281–82.

VI. PRIVACY LAWS, RIGHTS, AND LIABILITIES: WHERE DO WE GO FROM HERE?

"Concern about over-regulating in the private sector" has been acknowledged as a reason why Congress has been slow to act, and the judicial branch may be doing the same.[214] Despite these concerns, something must be done. We have been in this situation before. In 1890, when Samuel D. Warren and Louis D. Brandeis defined privacy for the first time as the "right to be let alone," they recognized the "new right[]" because it *needed* to "grow[] to meet the demands of society."[215] Just as the "[r]ecent inventions and business methods" called for changes then,[216] the demands of society today—the digitization of the persona and constant exchange, use, and loss of PII—call for changes now.

Congress (mainly) and the Supreme Court have the power and responsibility to define the limits of these new rights and of the redress available for these unique and unprecedented harms. They must give clarity to consumers, companies, and everyone else affected by privacy issues—specifically in cases of data theft and data misuse. In doing so, they must try to balance the interests of consumers (availability of redress in a situation where companies have the most bargaining power and control of data) and companies (needing adequate time to improve security and latitude to continue driving innovation).[217]

A. *Final Thoughts on Data Theft Situations and the Supreme Court's Role*

Regarding data theft cases, Congress has not provided any breach compliance and notification legislation, and, in the courts, there is inconsistency over whether the risk of harm is enough for Article III standing.[218] However, because cybersecurity breaches are

---

214 *Id.* at 268–70.

215 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–95 (1890) ("For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons . . . .") (footnote omitted).

216 *Id.*

217 *See supra* Part V.

218 *See supra* Part III. As discussed earlier, because of the Supreme Court's unclear guidance to date, federal courts differ on whether the certainly impending

technical, sophisticated, and difficult to understand without the proper background,[219] Congress may be more prepared to provide guidance. It is likely that, because of the complexity of data privacy rights, the Supreme Court is waiting on Congress to act, as it should have by now. However, if given the opportunity, the Supreme Court should, at the very least, clarify its analysis for determining data theft harms as sufficient for standing.

To start, the Court should determine whether the certainly impending or substantial risk standard applies to data theft suits. The substantial risk standard is a lower threshold of imminence than the certainly impending standard.[220] *Remijas* applied a substantial risk standard and conferred standing. [221] The Seventh Circuit explained that hackers steal information with a fraudulent intent of using it for a crime, and this in itself is a sufficient substantial risk.[222] Though *Remijas*' logic and holding may be deemed too tough on companies—especially because of the inevitable nature of data breaches—by either supporting or denying this as the standard (as opposed to the certainly impending standard), the Supreme Court will steer the lower courts to apply and develop *one* standard. Having one standard will at least narrow the discussion and hopefully, help establish a factual pattern that serves as precedent. That is, until Congress decides to legislate.

The Court could also provide guiding factors that take into account the policy implications of conferring standing (or not) in data theft cases. Courts should at least consider what sort of information was stolen and whether there is any presence of actual misuse of the stolen data. In other words, it should matter factually what type of information hackers steal. This Note does not explore the different types of PII and the comparable risks of it being stolen, but it seems logical that there should be a difference between one's email address

---

standard or the substantial risk standard applies; whether the inherent fraudulent intent of hackers is enough, or if something more is needed, to get a claim from merely speculative to imminent; and consequently, whether to acknowledge post-breach mitigation costs as reasonable or as manufactured harm. In other words, constitutional standing in privacy cases is a mess.

219 *See supra* Part II.

220 *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013).

221 *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015); *Clapper*, 568 U.S. at 407.

222 *See Remijas*, 794 F. 3d at 693.

being stolen versus one's credit card information being stolen. In general, it seems courts fear acknowledging harms (such as credit monitoring services, credit card changes, etc.) as sufficient for standing because of the risk that doing so would set precedent for letting plaintiffs manufacture standing. Focusing on the type of information stolen would help filter and keep plaintiffs from manufacturing standing.

The more dangerous the type of information stolen, the more reasonable for a consumer to respond, and therefore, the more reasonable for him or her to have access to the court system to seek redress. For example, buying credit reporting services has been acknowledged as an adequate response to stolen credit card numbers.[223] If the threats arising from a stolen credit card are more imminent than with a stolen email address, then this should be a consideration that goes to the imminence of the harm. Additionally, this would probably incentivize companies to categorize and minimize the type and amount of data that they collect and keep, thereby reducing the risk for both consumers and companies.[224]

Also, the Court should take into account whether any other plaintiff class members' stolen PII has been misused.[225] If the credit cards or social security numbers of *other* class members have been used without their authority, then that may serve as proof of imminent harm.[226] This may have made a difference in *Remijas*, where out of 350,000 exposed credit card numbers, 9,200 were known to have been used fraudulently at the time of suit.[227] Other possible policy considerations, such as the timing of the breach and of subsequent notification to consumers could be considered as well. In

---

[223] *See id.* at 694. (the victims [received] free credit monitoring and identity theft protection, and "[t]hese credit-monitoring services come at a price that is more than *de minimis*").

[224] *See* Bernard Marr, *Why Data Minimization Is An Important Concept In The Age of Big Data*, FORBES (Mar. 16, 2016), http://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#116cee76327f ("Data minimization also reduces cost. All data storage costs money, and no business has an infinite budget — so no business can go on collecting and storing data indefinitely.").

[225] *See* Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1283 (M.D. Fla. 2016) ("For these courts, one influential factor is the number of plaintiffs in the class action who experienced fraudulent charges.").

[226] *Id.*

[227] *Remijas*, 794 F.3d at 690.

theory, this would be favorable to companies that notify users quickly.

Considerations such as these will help develop a more consistent jurisprudence that will hopefully lead to a better understanding of when a consumer acts reasonably by incurring mitigation costs following a breach. With a more structured imminence analysis, courts can more comfortably recognize the mitigation harms (and other harms reasonably flowing from the breach) as merited.[228] In sum, the Supreme Court should—as a temporary solution to Congress' silence—address the circuit split resulting from *Clapper* and be clearer about standards and factors that lower courts should use in determining data theft standing.

B. *Final Thoughts on Data Misuse Situations and the Supreme Court's Role*

Regarding data misuse, while courts typically try to apply *Spokeo*'s concreteness analysis (looking at the history and congressional judgment related to the alleged harm), they perform it in an inconsistent manner that results in unpredictable outcomes.[229] While the Supreme Court acknowledged that Congress could confer statutory rights, it also made contradicting statements that put lower courts in a frenzy. Is a statutory violation procedural or substantive? If procedural, is the violation sufficient for standing? It remains unclear.[230]

To make matters worse, the Court introduced a two-step test, the historical and congressional judgment analysis, but it did not apply it nor provide guidance to lower courts on its application. With regards to history, as mentioned above, some lower courts emphasize the right to privacy as a traditional harm, while other courts do not even mention the right to privacy at all.[231] This all seems too abstract

---

[228] *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 965 (7th Cir. 2016) (finding a concrete injury amounting to the time and expense incurred to prevent and monitor fraudulent charges after plaintiffs' data was breached); *Remijas*, 794 F.3d at 688 (finding that "immediate preventative measures" were "necessary" and conferring standing). *But see* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (finding that these harms were unwarranted).

[229] *See infra* Part IV.

[230] *Id.*

[231] *Id.*

and unnecessary. Instead, the analysis should focus on whether Congress has spoken, and if so, whether the Court should confer standing based on a statutory violation.

As a starting point, Justice Kennedy's concurrence in *Lujan v. Defenders of Wildlife* provides a clearer analysis for standing based on statutory violations.[232] As will be explained below, it is a lower standard because, put simply, the Court "must be sensitive to the articulation of new rights of action that do not have clear analogs in [the] common-law tradition."[233] While Congress and the Supreme Court have acknowledged the right to privacy as a constitutional right,[234] it is unclear where the protection of personal data, such as PII, fits within that constitutional sphere. And this is Congress' job. As Justice Kennedy wrote, "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before . . . ."[235] The Court should defer to Congress and acknowledge that privacy rights may be broadening through the digitization of the persona, which should give people certain rights over the protection and dissemination of their PII. This would differentiate cases where Congress has spoken (data misuse cases) from cases based purely on imminence of harm (data theft cases), in which courts say that plaintiffs rely on a "highly attenuated chain of possibilities."[236]

These cases also differ from data theft cases in that, typically, the only actor at fault is the company (instead of an unidentifiable hacker). By failing to comply, companies that have the sole control of PII put consumers in a vulnerable place. Such behavior, at least where Congress has spoken, should be deterred. So, for data misuse cases, the standard for conferring standing should not be very high. These suits involve new and "complicated" types of harm and more

---

232 Lujan v. Defenders of Wildlife, 504 U.S. 555, 580–81 (1992) (Kennedy, J., concurring).

233 *Id.* at 580.

234 *See generally* 5 § U.S.C. 552(a) (2012) (delineating how agencies should use personal records publicly and acknowledging the possible invasion of one's personal privacy)

235 *Lujan*, 504 U.S. at 580.

236 Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013).

deference should be given to Congress' consumer protection statutes.[237]

Specifically for data misuse cases, standing should be conferred so long as Congress identifies the injury it seeks to vindicate and relates the injury to the class of persons entitled to bring suit.[238] This should be the "outer limit to [Congress' power] to confer rights of action" in data and consumer protection space.[239] However, if Congress clearly confers a harm (pursuant to Justice Kennedy's concurrence in *Lujan*), such legislation should be taken seriously to protect the people's right to privacy.[240]

As an example, in the case of ensuring accurate reports, the FCRA seems to both identify the injury it seeks to vindicate and to relate the injury to the class of persons entitled to bring suit. [241] The FCRA states that "a reporting agency . . . shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates."[242] So, it is indicating the injury as the inaccuracy of the report. It also states that any "person who willfully fails to comply with any requirement . . . is liable to that consumer . . . [for] any actual damages sustained . . . or damages [between $100 and $1000]."[243] It is specifically trying to protect the persons harmed by the inaccurate report. Therefore, by this standard, Congress has recognized the harm

---

[237] *Cf.* Brief for EPIC, *supra* note 178, at 16–17 ("The need for statutory remedies is due, in part, to the complicated nature of harms resulting from privacy violations."); *see also* Bartnicki v. Vopper, 532 U.S. 514, 549 (2001) (Rehnquist, C.J., dissenting) (explaining that the harms resulting from privacy invasions are especially difficult to quantify and trace).

[238] *Lujan*, 504 U.S. at 580–81 (Kennedy, J., concurring).

[239] *Id.*

[240] Though not exactly the same because hackers are not companies, intentional trespass jurisprudence may serve as a potentially helpful analogy for defining the right to privacy. Some courts award at least nominal damages in intentional trespass cases (and sometimes even punitive damages) on grounds that people have a "constitutional right to the exclusive enjoyment" of their property. Jacque v. Steenberg Homes, Inc., 563 N.W.2d 154, 160 (Wis. 1997). Should we view the right to control and protect consumer data, essentially a sort of digital persona, as some courts view the right to exclusivity? Should we at least provide minimal nominal or statutory damages when our digital persona is trespassed?

[241] *See* 15 U.S.C. § 1681e(b) (2012).

[242] *Id.*

[243] *Id.* § 1681n.

and the class of persons, thereby demonstrating a "chain[] of causation" sufficient for standing.[244]

Similarly, the FDCPA seeks to "protect consumers against debt collection abuses"[245] by identifying consumers facing debt collectors as the injury class and by forbidding specific practices that are "false, deceptive, or misleading representation[s] with the collection of any debt."[246] Therefore, "any debt collector who fails to comply . . . is liable to such person"[247] because the debt collector has at least statutorily injured a consumer.

As a final example, the TCPA makes it "unlawful for any person within the United States" to initiate "any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without . . . prior express consent . . . ."[248] It creates a private right of action by those parties who are victims of the unlawful calls and establishes damages provisions to redress for the intrusion itself or other monetary loss.[249]

The *Lujan* concurrence analysis fits well with the deference that should be due to Congress and is beneficial to courts—it leaves the procedural versus substantive right analysis to Congress because Congress can clearly express when it creates a cause of action. As for the public, it ensures that companies are at least abiding by the minimum standard set forth by federal consumer protection statutes. Also, assuming Congress decides to finally legislate on data theft cases or to create other consumer protection statutes regarding the integrity of PII, such statutes, coupled with this straightforward analysis, will help parties better understand their rights.

CONCLUSION

With more people online, more information being exchanged, and more companies getting hacked, the government needs to act to protect PII.[250] The *ideal* scenario would incentivize companies to improve security measures and practices while not placing such a

---

244 *Lujan*, 504 U.S. at 580 (Kennedy, J., concurring).
245 15 U.S.C. § 1692(e).
246 *Id.* § 1692(e).
247 *Id.* § 1692(k).
248 47 U.S.C. § 227(b)(1)(B).
249 *Id.* § 227(b)(3).
250 *See supra* Part I.

burden that breach and litigation costs could bring businesses to fail and stall innovation. While the issue would be best tackled by Congress, the Supreme Court may find itself in the driver's seat once again after its *Clapper* and *Spokeo* decisions resulted in circuit splits and lower court confusion.[251]

The imminence and concreteness requirements for standing remain fuddled as "early dismissals [in privacy suits] have prevented courts from defining what is reasonable."[252] If given the chance, the Court should clarify the applicable imminence standard and provide a set of considerations that could help lead to more predictable results and a more understandable threshold for data theft cases.[253]

Further, where Congress has spoken through consumer protection statutes, the Court should apply the *Lujan* concurrence analysis, which rightfully defers to Congress the creation of privacy standing because of the complicated nature of privacy harms. "While merely complying [with statutes] may not be the best strategy for protecting data from increasing attacks, it does ensure that, there is a minimum standard to be met, at least decreasing the likelihood of a successful breach."[254]

---

[251] *See supra* Parts III, IV.

[252] Casler, *supra* note 173. Likely referring to reasonableness of consumers taking mitigating precautions and becoming emotionally disturbed by the threat of future harm. *See supra* Part V.

[253] *See supra* Part V.

[254] Lambert, *supra* note 15.