Indiana Law Journal

Volume 96 | Issue 3 Article 7

Spring 2021

What's the Harm? Federalism, the Separation of Powers, and Standing in Data Breach Litigation

Grayson Wells
Indiana University Maurer School of Law, grwells@iu.edu

What's the Harm? Federalism, the Separation of Powers, and Standing in Data Breach Litigation

GRAYSON WELLS*

INTRODUCTION

Craig and Sarah are customers of Cascadia Corporation, a large online retailer. Cascadia tracks the buying habits and personal information of its customers to provide advertising that its customers are more likely to appreciate and to predict the types of products and services its customers will want to purchase in the future. To this end, Cascadia stores vast amounts of information about its customers in its corporate data center. The company employs a large team of technology and cybersecurity engineers, but its Board of Directors does not always see the value in fully funding the security recommendations of the engineering teams. Vulnerabilities abound.

One day, Craig and Sarah are notified that their personal information—including names, credit card numbers, birthdays, physical addresses, telephone numbers, and a list of every product Craig and Sarah have ever purchased—have been stolen by hackers. Neither have seen any malicious activity on their accounts yet, but they know their data has been compromised and could be sold online. They worry they could have their identities stolen but also that their buying habits, including the more personal ones, could be made available for the public to see.

As news leaks of Cascadia's relaxed cybersecurity measures, Craig and Sarah become angry that a company they trusted would put them in this position. They consider joining together, along with other similarly situated consumers, in a class action lawsuit to sue the company. At their first meeting with an attorney, she asks Craig and Sarah: What's the harm? Have you suffered any financial loss because of this? Has anyone actually stolen your identity? Neither know how to respond. They feel as though they have been harmed. The company's failure to secure their private

* J.D., Indiana University Maurer School of Law, 2020; M.S. in Cybersecurity Risk Management, Indiana University, 2020; B.S. in Computer Science, Park University, 2010.

data means they must now worry about how that data will be used. But is that enough? The attorney worries that Craig and Sarah may not even have standing to bring suit in federal court.

Unfortunately, this story is common. The breach of corporate data networks by malicious actors is the new normal.[1] As a result, private consumer data is often viewed or stolen, or even placed for sale online.[2] The hackers who are directly responsible for these data breaches are often never caught.[3] Instead of suing these largely unidentified hackers, the consumers affected by the breaches then sue the businesses on a variety of causes of action for any role the business's lack of adequate cybersecurity measures played in the disclosure of personal information.[4] Thus, companies are often the target of large-scale data breach litigation.[5]

Often, this data is used in identity theft crimes.[6] But regardless, the exposure of consumer data creates a risk of malicious use, anxiety on the part of the consumer,

---

1. Benjamin Dynkin & Barry Dynkin, *Derivative Liability in the Wake of a Cyber Attack*, 28 ALB. L.J. SCI. & TECH. 23, 33 (2018) ("[T]here are so many data breaches that consumers are beginning to report 'data breach fatigue.'").

2. While some stolen data may end up for sale on the dark web, other stolen data may be disclosed online for all to see. *See* Alex Hern, *Largest Collection Ever of Breached Data Found*, THE GUARDIAN (Jan. 17, 2019, 12:31 PM), https://www.theguardian.com/technology/2019/jan/17/breached-data-largest-collection-ever-seen-email-password-hacking [https://perma.cc/D233-E9FU]; Marianne Kolbasuk McGee, *4 Stolen Health Databases Reportedly for Sale on Dark Web*, DATA BREACH TODAY (June 27, 2016), https://www.databreachtoday.com/3-stolen-health-databases-reportedly-for-sale-on-dark-web-a-9227 [https://perma.cc/9QSA-4Z3D]; Kate O'Flaherty, *Another 127 Million Records Have Gone on Sale on the Dark Web – Here's What You Should Do*, FORBES (Feb. 15, 2019, 7:50 AM), https://www.forbes.com/sites/kateoflahertyuk/2019/02/15/another-127-million-records-have-gone-on-sale-on-the-dark-web-heres-what-you-should-do/#4348d2293044 [https://perma.cc/MRX5-BM38].

3. Roger A. Grimes, *Why It's So Hard to Prosecute Cyber Criminals*, CSO (Dec. 6, 2016, 3:00 AM), https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html [https://perma.cc/NFY2-2VY8] ("Cyber criminals steal hundreds of millions of dollars each year with near impunity. For every 1 that gets caught, 10,000 go free – maybe more."). Still, hackers are sometimes caught, especially if they boast about their exploits. *See* Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, THE N.Y. TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html [https://perma.cc/2HRG-DU9L] ("The suspect, Paige Thompson, 33, left a trail online for investigators to follow as she boasted about the hacking, according to court documents in Seattle, where she was arrested and charged with one count of computer fraud and abuse.").

4. *See infra* Part II.

5. David Balser, Phyllis Sumner, Stewart Haskins & John Toro, *INSIGHT: Data Breach Litigation Trends to Watch*, BLOOMBERG LAW (Mar. 4, 2019, 4:01 AM), https://news.bloomberglaw.com/us-law-week/insight-data-breach-litigation-trends-to-watch [https://perma.cc/CP57-SL58] (discussing the scale at which data breaches occur and that they often lead to litigation and regulatory enforcement actions).

6. *See* Matt Tatham, *Experian Forecasts the Top 5 Data Breach Predictions for 2019*, DATA BREACH (Dec. 10, 2018), https://www.experian.com/blogs/ask-experian/experian-forecasts-the-top-5-data-breach-predictions-for-2019 [https://perma.cc/89XZ-DHNR] (discussing the increased risk in identity theft because the increase in personal data exposure "has made it easy for cybercriminals to monetize stolen data, which has, in turn, led to an

and represents an invasion of the consumer's privacy.[7] In fact, Statistica noted in 2014 that Americans now worry about the harm from hacking more than most other harms.[8] Statistica notes that sixty-nine percent of respondents to a recent Gallop poll reported being "frequently or occasionally worr[ied] about having credit card information stolen by hackers," while only thirty-one percent feared getting mugged and only eighteen percent feared being murdered.[9] This is probably because "over a quarter of all Americans have experienced" credit card data theft, while few Americans experience more violent crimes like robbery.[10] Jordan Elias noted that "the dominant harm from data breaches lies not in low-level fraud but in the loss of private facts themselves and consequent damage of an intangible nature: anxiety, depression, and distress."[11]

Once a breach has occurred, consumers often form class action lawsuits against the breached business.[12] These lawsuits are based on a variety of causes of action, including negligence, breach of an express or implied contract, violations of state consumer privacy laws, and violations of state breach notification laws.[13] Still, a major hurdle for plaintiffs in these actions has been to convince the federal judiciary that they have standing to sue, such that the court has subject-matter jurisdiction.[14]

---

increased risk of identity theft").

7. *See* Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 ILL. L. REV. 295, 347 (discussing the invasion of privacy torts and noting that the malicious actor, and not the company, invaded the consumer's privacy); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 745 (2018) ("Knowing that thieves may be using one's personal data for criminal ends can produce significant anxiety.").

8. Niall McCarthy, *Hacking Has Become Every American's Worst Nightmare*, STATISTICA (Oct. 28, 2014), https://www.statista.com/chart/2881/hacking-has-become-every-americans-worst-nightmare [https://perma.cc/8RZA-S4JS].

9. *Id.*

10. *Id.*; *Robbery Rate Per 100,000 Inhabitants in the United States in 2019, by State*, STATISTICA (Oct. 1, 2020), https://www.statista.com/statistics/232564/robbery-rate-in-the-us-by-state [https://perma.cc/3AMC-YRXQ] (showing that the robbery rate in the United States was 81.6 per 100,000).

11. Jordan Elias, *Course Correction—Data Breach as Invasion of Privacy*, 69 BAYLOR L. REV. 574, 576 (2017).

12. *See* Solove et al., *supra* note 7, at 749; *see also* Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 62 (2017) ("Due to the large number of consumers affected, the high frequency, and the sensitive nature of the information lost in data breaches, class actions are a crucial mechanism for ensuring damaged consumers have access to justice and may seek relief.").

13. *See infra* Part II.

14. *See* United States v. Sanchez-Gomez, 138 S. Ct. 1532, 1537 (2018) ("To invoke federal jurisdiction, a plaintiff must show a 'personal stake' in the outcome of the action. . . . A case that becomes moot at any point during the proceeding is 'no longer a "Case" or "Controversy" for purposes of Article III,' and is outside the jurisdiction of the federal courts."); *see also* Bugni, *supra* note 12, at 63 ("Data breach class actions present a quandary because, although the plaintiffs' information is stolen, there is often no indication of financial damages when plaintiffs bring suit. Due to this lack of concrete financial loss, many courts dismiss for lack of injury."). The difficulty of the standing hurdle likely exists because the law does not seem to be settled here. *See* Solove et al., *supra* note 7, at 739 ("The concept of harm

Specifically, the courts typically analyze whether plaintiffs have standing based on an identity theft analysis.[15] They ask whether the exposure of the consumers' data has resulted in malicious activity (e.g., fraudulent financial transactions).[16] But that analysis is too narrow. The question becomes, when a state private right—created either by common or statutory law—is violated, how does applying federal Article III standing law comply with core principles of the separation of powers and federalism? In other words, is requiring an identity theft analysis in data breach standing consistent with core principles when the claim arises under state law?

This Comment will argue that the Supreme Court should analyze standing in data breach litigation under a standard that is deferential to state statutory and common law. Specifically, federal standing analysis should look to state law when determining whether an injury is concrete such that the injury-in-fact requirement is met. Some argue that allowing more data breach cases to proceed to the merits could lead to an explosion of successful litigation and settlements, burdening the federal courts[17] and causing economic losses for the breached businesses.[18] These concerns may be valid. But if state law provides a remedy to the harm suffered, the federal courts should not remove their redress. Federalism instructs otherwise.[19]

Part I explains the current data breach climate. Part II then discusses the more common causes of action that plaintiffs claim in data breach litigation. Part III then begins the standing discussion and lays out the existing state of affairs for standing

---

stemming from a data breach has confounded the lower courts. There has been no consistent or coherent judicial approach to data-breach harms.").

15. Solove et al., *supra* note 7, at 741–42 (discussing identity-based harm reasoning used by courts in data breach litigation); Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1325 (2017) (noting that typical plaintiffs allege "that the defendant's failure to protect [their] personal data [have caused them] damages by increasing [their] risk of suffering actual identity theft").

16. *In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) (concluding that "the complaint has not sufficiently alleged a substantial risk of identity theft, and plaintiffs' allegations of future injury do not support standing").

17. *See* Note, *Competitors' Standing To Challenge Administrative Action Under the APA*, 104 U. PENN. L. REV. 843, 845 (1956) (noting that, in the administrative law context, "[a] liberal application of statutory standing might result in a flood of suits and appeals"); *see also* Stephen Lanza, *The Liberalization of Article III Standing: The Supreme Court's Ill-Considered Endorsement of Citizen Suits in Friends of the Earth v. Laidlaw Environmental Services, Inc.*, 52 ADMIN. L. REV. 1447, 1454 (2000) (discussing congressional recognition that the possibility that public action in the citizen suit context could overburden the courts).

18. Settlements in data breach litigation can be quite high, which results in severe economic loss either for the business or their insurance provider—assuming they even have cyber insurance. Marty Puranik, *What Is the Cost of a Data Breach*, FORBES (Dec. 2, 2019, 8:40 AM), https://www.forbes.com/sites/forbestechcouncil/2019/12/02/what-is-the-cost-of-a-data-breach [https://perma.cc/6728-V3CH] ("The average total cost per breach has increased from $3.54 million in 2006 to $8.19 million in 2019."). On the extreme high end, Equifax recently settled with private plaintiffs and the Federal Trade Commission. The settlement will pay between $575 and $700 million. *Equifax To Pay up to $700 Million in US Data Breach Settlement*, CNBC (July 22, 2019, 7:03 AM), https://www.cnbc.com/2019/07/22/equifax-to-pay-up-to-650-million-in-data-breach-settlement.html [https://perma.cc/8LED-5CNE].

19. *See infra* Section IV.C.

in data breach litigation. Next, Part IV discusses dignitary harms and the need to respect the sovereignty of the individual states and their ability to define their own laws. That Part argues the Supreme Court should defer to state determinations of what constitutes harm under the law the state wrote. Then, Part V addresses the inconsistent results that the tightening of standing law has created and discusses the possibility of a federal omnibus privacy law. Finally, this Comment concludes by reiterating the point that plaintiffs must allege that a legally protected right has been violated. To effectively analyze this claim, the Supreme Court should defer to the entity that created that legally protected interest and determine what it sought to protect.

I. DATA BREACH CLIMATE

Data breaches have become routine.[20] As a result, all fifty states have passed legislation that requires breached companies to notify relevant consumers that their data has been compromised.[21] The FTC, under authority of section five of the FTC Act, has started prosecuting companies that "deceptively" fail to live up to their own privacy policies.[22] Furthermore, under the same authority, the FTC has started to prosecute corporate entities for "unfair" cybersecurity practices. These unfair practices are those that are likely to cause substantial injury to consumers—injuries that are both reasonably unavoidable by the consumer and are not outweighed by countervailing benefits to those consumers or to competition.[23] Still, no general federal law or regulation exists to mandate minimum standards for how all companies protect consumer data or to provide a private right of action for consumers to hold companies accountable.[24] U.S. policy has instead been to pass piecemeal,

---

20. Dynkin et al., *supra* note 1; *see also* Jon L. Mills & Kelsey Harclerode, *Privacy, Mass Intrusion, and the Modern Data Breach*, 69 FLA. L. REV. 771, 771 (2017) (noting the daily occurrence of data breaches).

21. Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961, 1970 (stating that "all fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted [data breach notification] laws"). Still, data breach notification laws do not sufficiently protect privacy. *See* Solove et al., *supra* note 7, at 781 ("Data-breach-notification laws require provision of notice to people about data breaches, but they do little to redress any injuries caused.").

22. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241 (3rd Cir. 2015) (discussing that the complaint charged a "deception claim" that alleged Wyndham's privacy policy overstated the company's cybersecurity posture).

23. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1148–49 (2019); *Wyndham Worldwide Corp.*, 799 F.3d at 240 (noting the FTC allegation that Wyndham engaged in "unfair" practices because their cybersecurity posture "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft").

24. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014) (noting that "there is no federal law that directly protects the privacy of data collected and used by merchants such as Macy's and Amazon.com . . . [or] the forms of data collection in use by companies such as Facebook and Google"); Scott J. Shackelford, Andrew A. Proia, Brenton Martell & Amanda N. Craig, *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50

sector-specific privacy laws.[25] Thus, aggrieved consumers often rely on state statutory and common law, or one of the federal statutes that apply in limited circumstances.[26]

This ability to seek legal redress under state law is increasingly important because of how common data breaches have become. According to one source, there were forty-five percent more data breaches in 2017 than in 2016.[27] USA Today has reported that between April and June of 2018, more than 765 million people were affected by data breaches.[28] In September 2018, Facebook was breached, exposing the personal data of nearly fifty million users.[29] And Fortune has noted that, even though the total number of breaches declined from the previous year, "the number of exposed records more than doubled" in 2018.[30]

The risk of consumer data being breached is only exacerbated by the nature and scope of the data being collected by corporate entities. Data has become a commodity and is used to create behavioral profiles of consumers.[31] This information is

---

TEX. INT'L L.J. 305, 309–10 (2015) (noting that "[c]urrently, no baseline, comprehensive cybersecurity obligations are imposed across all of the U.S. critical infrastructure, but regulations do exist for certain sectors . . . .").

25. Federal privacy law is, currently, a patchwork of laws that each apply to different "sectors." If an entity operates in that sector, then those laws apply. Digit. & Cyberspace Pol'y Program, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/JLJ9-RK6M] ("Most Western countries have already adopted comprehensive legal protections for personal data, but the United States—home to some of the most advanced, and largest, technology and data companies in the world—continues to lumber forward with a patchwork of sector-specific laws and regulations that fail to adequately protect data.").

26. *See infra* Part II.

27. Steve Turner, *2018 Data Breaches—The Worst of Last Year*, IDENTITY FORCE (Dec. 27, 2017), https://www.identityforce.com/blog/2018-data-breaches [https://perma.cc/8FAX-T6GP].

28. Mike Snider, *Your Data Was Probably Stolen in Cyberattack in 2018—and You Should Care*, USA TODAY (Dec. 28, 2018, 6:00 AM), https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002 [https://perma.cc/A6V3-KUET].

29. Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, THE NY TIMES (Sep. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html?rref=collection%2Ftimestopic%2FPrivacy [https://perma.cc/DAM3-DTR5].

30. Danielle Abril, *Data Breaches Declined Last Year. But Here's Why You Should Be More Worried Than Ever*, FORTUNE (Jan. 29, 2019, 5:53 PM), http://fortune.com/2019/01/29/data-breaches-decline-2018-consumer-data-risk-rises [https://perma.cc/SC8W-5WHP].

31. Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 32 (2011) ("Indeed, behavioral advertising is already being used to aggregate a commodity-consumer information-that, to the individual consumer, has little exchange value into a valuable product that allows the consumer to access relevant and free Internet content."); *see also* Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 99 (2013) (explaining that behavioral advertising is "based on information about the individual user" and "requires that the entity serving up the ad have access to a trove of information about particular Internet

extremely valuable to companies interested in targeted advertising, which has created a vast market for information.[32] Furthermore, companies collect this data for a reason; it is highly instructive about the consumer's personality and potential buying habits.[33] Thus, the unconsented-to exposure of this data to malicious actors, and to the public, could be highly offensive to the privacy and dignity of the consumer, regardless of the pecuniary harm involved.[34] This is especially true if the company involved engages in behavioral advertising, which incentivizes the accumulation of more and more data[35] and requires the "large-scale and long-term collection, storage, analysis, and . . . sharing" of that data.[36]

Given the dearth of federal law requiring companies to reasonably protect consumer data and given the resulting lack of statutory damages for failing to meet such a requirement, the ability to seek legal redress on state law theories is critically important. Furthermore, data breach litigation could increase the cost to businesses for failing to follow reasonable cybersecurity measures.[37] These settlements can be quite expensive for the breached business, which likely encourages businesses to invest in cybersecurity insurance.[38] This only increases the likelihood that consumers will be better protected. Cybersecurity insurance providers often end up acting like pseudo regulatory bodies, because of those providers' requirements for covering companies with insurance.[39]

---

users").

32. Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospect of an Information Civilization*, 30 J. INFO. TECH. 75, 85 (2015) ("New monetization opportunities are thus associated with a new global architecture of data capture and analysis that produces rewards and punishments aimed at modifying and commoditizing behavior for profit."). Still, as Katherine Strandburg notes, "it is difficult to measure the effectiveness of online advertising." Strandburg, *supra* note 31, at 102. And some people may even argue that even behavioral advertising, the more intrusive option, is not that effective. Avi Goldfarb and Catherine Tucker looked at the effectiveness of behavioral advertising and concluded that its effectiveness "declined by about 65 percent after the adoption" of the European Union's 2002 Data Protection Directive. Strandburg, *supra* note 31, at 103 (citing Avi Goldfarb & Catherine Tucker, Privacy Regulation and Online Advertising 18 (Aug. 5, 2010) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259 [https://perma.cc/7CDL-TCPP]. Still, as Katherine Strandburg explains, "[t]he overall impact of the ads was small both before and after enactment [of the Data Protection Directive], corresponding to about a 2.5 percent increase in expressed willingness to purchase." Strandburg, *supra* note 31, at 103 (citing Goldfarb et al., *supra* note 32, at 19).

33. *See* Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87, 95–96 (2018).

34. Solove et al., *supra* note 7, at 764, 768 (noting how plaintiffs "clearly suffer emotional distress" and interfere with a person's ability to develop their "inviolate personality").

35. Strandburg, *supra* note 31, at 125.

36. *Id.* at 100.

37. *See supra* note 18 and accompanying text.

38. *See id.*; James A. Johnson, *Insuring Against Cybercrime – Know the Risks*, N.Y. ST. B. ASS'N J., May 2019, at 14, 16 (explaining that quality cyber insurance policies should cover the cost of "[s]ettlements, judgments, [and] civil awards after a data breach").

39. Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 L. & SOC. INQUIRY 417, 429

II. CAUSES OF ACTION

Data breach cases are argued under a myriad of theories, often under state law causes of action.[40] While some sectoral federal law does offer privacy protection,[41] and some private rights of action, in very specific circumstances,[42] data breach plaintiffs often resort to state common law claims of negligence, unjust enrichment, bailment,[43] and breach of contract—both implied and express.[44] Depending on the state, plaintiffs may also seek redress under state statutory laws governing breach notification, unfair competition, and consumer privacy.[45] Under federal law, plaintiffs can sue if the events giving rise to the litigation fall under one of the various sectoral privacy laws. These include violations of the Fair Credit Reporting Act (FCRA), the Stored Communications Act (SCA), the Gramm-Leach-Bliley Act, and the Privacy Act.[46] But as discussed, these laws apply in only specific—often in-

---

(2017) (explaining that cyber insurance providers will assess the cyber risk of the company and could require certain cyber improvements before covering the company and further explaining how being more cyber secure may lower the premiums the company must pay for the insurance).

40. Timothy H. Madden, *Data Breach Class Action Litigation – A Tough Road for Plaintiffs*, 55 BOSTON B.J. 27, 29 (2011) ("Plaintiffs have brought these claims under myriad legal theories, including negligence, breach of contract, breach of fiduciary duty, negligent misrepresentation, violation of state consumer protection laws such as Mass. General Laws ch. 93A, and others. Sometimes, class action plaintiffs also seek to invoke the protections of the various state data breach notification laws.").

41. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, PUB. L. NO. 104-191, 110 STAT. 1936; Children's Online Privacy Protection Act of 1998, PUB. L. NO. 105-277, 112 STAT. 2681-728; Video Privacy Protection Act of 1988, PUB. L. NO. 100-618, 102 STAT. 3195.

42. *See* Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618, 621–22 (7th Cir. 2014) (discussing VPPA's private right of action). *But see* O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176, 1179, 1182 (D. Wyo. 2001) (finding no private right of action, either implied or express, exists in HIPAA).

43. While some people may argue that bailment as a cause of action in data breach litigation is a stretch, Justice Gorsuch conceptualized data held by third parties in the Fourth Amendment context as a bailment. Carpenter v. United States, 138 S. Ct. 2206, 2268–70 (2018) (Gorsuch, J., dissenting). While this is merely a dissenting opinion, it could serve as the first sign of how future courts could view data held by third parties.

44. Madden*, supra* note 40.

45. *See, e.g.*, Third Amended Class Action Complaint at 20–22, 28–31, Antman v. Uber Technologies, Inc., No. 15-cv-0115-LB, 2015 WL 2151231 (N.D. Cal. May 10, 2018) (No. 15-1175), ECF No. 179 (claiming negligence, breach of contract, California statutory law); Consumer Plaintiffs' First Amended Consolidated Class Action Complaint at ¶¶ 240–42, In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014) (MDL No. 14-2522), ECF No. 258 (alleging numerous state data breach and consumer law statutes, negligence, breach of implied contract, bailment, and unjust enrichment); *see also* Madden, *supra* note 40.

46. *See, e.g.*, Amended Complaint ¶ 9, In re U.S. Office Pers. Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1 (D.D.C. 2017) (No. 15-1394), ECF No. 63 (claiming a violation of the Privacy Act, among other things); Class Action Complaint at 12, 18, 22, Green v. eBay Inc., No. 2:14-cv-01688, 2015 WL 2066531 (E.D. La. 2015) (No. 14-1688), ECF No. 1

applicable—circumstances.[47]

Regardless of the cause of action, data breach plaintiffs have encountered problems.[48] The obvious problem—and one of the reasons traditional, *intentional* invasion of privacy torts[49] are not a clean fit—is that the individual directly responsible for the harm is the malicious actor that breached the company and accessed the personal data of the plaintiffs. The company can hardly be responsible for intentionally invading the privacy of the consumers.[50] Presumably, the company did not hack itself or directly expose the consumers' personal data to the public. Rather, it merely failed to live up to reasonable standards for protecting the consumers' data. But we have a tort for that—negligence.[51] The company may not have intended to disclose the consumers' data to the public or a malicious third party, but, as the theory goes, the company does have a duty to safeguard the consumer data it collects and failing to implement reasonable security measures is a breach of that duty.[52]

Still, the merits of these negligence claims, or any other cause of action, cannot be litigated until the court determines that the plaintiffs have standing to sue, such that the court has subject-matter jurisdiction over the case.[53] As the next Part explains, data breach plaintiffs have struggled with this requirement in no small part because of the "concrete" injury analysis.

III. STANDING

The U.S. Constitution calls for a tripartite system of government in which the

---

(claiming violations of the Stored Communications Act, the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act, and more).

47. Essentially, if limited to federal law, plaintiffs would have to hope the breached records implicate one of the more protected sectors (e.g., medical or financial records). *See supra* note 41.

48. *See* Madden, *supra* note 40 ("All of these types of claims, however, have [fared] poorly, in Massachusetts and elsewhere.").

49. "The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, . . . these four torts may be described as follows: 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness." William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

50. This is because the privacy torts are intentional torts. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1908 (2010) (describing Prosser's privacy torts as intentional torts).

51. Travis N. Jenson, Note, *Cooling the Hot Pursuit: Toward A Categorical Approach*, 73 IND. L.J. 1277, 1287 & n.70 (1998) (citing W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 30, at 164 (5th ed. 1984)) (describing negligence and its elements).

52. *See, e.g.*, Consumer Plaintiffs' First Amended Consolidated Class Action Complaint ¶¶ 108–13, In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014) (MDL No. 14-2522), ECF No. 258 (detailing plaintiff's claim of negligence).

53. *See supra* note 14 and accompanying text (discussing that issues of justiciability are jurisdictional in nature).

legislative, judicial, and executive functions are separated into distinct branches of government.[54] To ensure the judiciary does not invade the sphere of the other two branches,[55] federal courts are deprived of subject-matter jurisdiction when cases are deemed nonjusticiable.[56] In other words, cases must be the type that federal judges are equipped to resolve.[57] Along with the requirement that cases be ripe[58] and not moot,[59] standing is a key element of justiciability.[60]

Most of Article III standing law has been created since 1944.[61] But early Article III standing analysis simply limited federal courts' jurisdiction to cases and controversies where "Congress or any other source of law had granted the plaintiff the right to sue."[62] Still, little evidence exists to prove what precisely the Founders meant by cases and controversies.[63] And while modern standing law goes beyond

---

54. U.S. CONST. art. I, § 1; U.S. CONST. art. II, § 1, cl. 1; U.S. CONST. art. III, §§ 1, 3.

55. Raines v. Byrd, 521 U.S. 811, 820 (1997) (noting that "the law of Art. III standing is built on a single basic idea—the idea of separation of powers" (quoting Allen v. Wright, 468 U.S. 737, 752 (1984))).

56. United States v. Sanchez-Gomez, 138 S. Ct. 1532, 1537 (2018) ("To invoke federal jurisdiction, a plaintiff must show a 'personal stake' in the outcome of the action. . . . A case that becomes moot at any point during the proceedings is 'no longer a "Case" or "Controversy" for purposes of Article III,' and is outside the jurisdiction of the federal courts."); Warth v. Seldin, 422 U.S. 490, 498 (1975) (describing questions of justiciability as being required to warrant the "invocation of federal-court jurisdiction").

57. Kristin E. Hickman, *How Did We Get Here Anyway?: Considering the Standing Question in* DaimlerCrystler v. Cuno, 4 GEO. J.L. PUB. POL'Y 47, 48–49 (2006) ("Standing doctrine plays an important role in a system of government that divides power among three co-equal branches and dual sovereigns. Both Article III and prudential standing requirements serve the federal judiciary by limiting its jurisdiction to actual disputes between parties that judges are particularly equipped to resolve.").

58. Renne v. Geary, 501 U.S. 312, 321 (1991) ("We also discern no ripe controversy in the allegations that respondents desire to endorse candidates in future elections . . . ."); *see also* 13B CHARLES ALAN WRIGHT, ARTHUR R. MILLER & EDWARD H. COOPER, FEDERAL PRACTICE AND PROCEDURE § 3532.1 (3d ed. 2008) (noting that ripeness is concerned with "whether a dispute has yet matured to a point that warrants decision").

59. *Renne*, 501 U.S. at 320 (noting that "[j]usticiability concerns not only the standing of litigants to assert particular claims, but also the appropriate timing of judicial intervention" and that the respondents failed to demonstrate a "live controversy," meaning the disputes had been rendered "moot by the time respondents filed suit"); *see also* WRIGHT ET AL., *supra* note 58, § 3533.1 (noting that mootness is concerned with whether "any effective purpose can still be served by a specific remedy").

60. WRIGHT ET AL., *supra* note 58, § 3529 ("The central concepts often are elaborated into more specific categories—advisory opinions, feigned and collusive cases, standing, ripeness, mootness, political questions, and administrative questions.").

61. Cass R. Sunstein, *What's Standing After Lujan? Of Citizen Suits, "Injuries," and Article III*, 91 MICH. L. REV. 163, 169 (1992). *But see* Massachusetts v. Mellon, 262 U.S. 447, 487 (1923) (describing the harm as "remote, fluctuating and uncertain," which speaks to much of the same concerns as today's interpretation of the Article III standing requirement). Still, Sunstein's analysis that much of modern standing law was developed in recent history remains valid even if previous case law sounded in similar concerns.

62. Sunstein, *supra* note 61, at 170.

63. *Id.* at 173.

intent of the legislature,[64] Cass Sunstein has noted that "[t]here is no reason to think that the Framers sought to limit Congress' power to create 'cases' or 'controversies' by conferring causes of action."[65] The Framers' intent was simply to limit federal courts' jurisdiction to "cases where individual plaintiffs brought their own grievances for resolution and relief."[66] But still, the cases and controversies requirement has morphed into an increasingly complex body of law.[67]

The policy behind the case and controversy limitations was built on the separation of powers, to ensure one branch of government did not inappropriately invade the sphere of another.[68] This is why the Supreme Court has applied an especially rigorous analysis in cases where plaintiffs ask the judiciary to second-guess a decision of the executive or legislative branch.[69] But, as Erwin Chemerensky has explained, refusing to confer standing on plaintiffs can also impinge on the separation of powers.[70] Thus, the standing analysis "focuses attention directly on the question of what is the proper place of the judiciary in the American system of government."[71]

Modern interpretation of Article III standing has created a test to ensure the objective of the separation of powers principle is respected.[72] Now, under the *Lujan* test, the Court must be able to find an injury in fact, trace that injury to the conduct complained of, and the resolution of the case at bar must produce a likelihood that

---

64. *See id.* at 164–66 (discussing Scalia's argument that Article III should impose limits on "the power of Congress to convert generalized benefits into legal rights" and then later discussing how Scalia's opinion in *Lujan* forbids Congress from creating citizen standing).

65. *Id.* at 173.

66. "In sum, a fair reading of the proceedings of the Constitutional Convention and the contemporary legal environment makes it more likely than not that the Framers envisioned that the federal courts would be limited, as a constitutional matter, to cases where individual plaintiffs brought their own grievances for resolution and relief."
James Leonard & Joanne C. Brant, *The Half-Open Door: Article III, the Injury-in-Fact Rule, and the Framers' Plan for Federal Courts of Limited Jurisdiction*, 54 RUTGERS L. REV. 1, 40, 47 (2001); *see also* Town of Chester v. Laroe Estates, Inc., 137 S. Ct. 1645, 1650 (2017) ("Our standing doctrine accomplishes this by requiring plaintiffs to 'alleg[e] such a personal stake in the outcome of the controversy as to . . . justify [the] exercise of the court's remedial powers on [their] behalf.'" (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 38 (1976))).

67. Lanza, *supra* note 17, at 1452–53 (explaining that courts "rarely follow bright-line rules" and that "the introduction of citizen suit provisions in environmental statutes . . . brought the Supreme Court face to face with the glaring inadequacies of an increasingly complex body of law").

68. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013) ("The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches."). *But see* Leonard & Brant, *supra* note 66, at 48 ("Yet a quick glance at the [Constitution] as a whole reveals that the concept of divided government was never intended to compartmentalize strictly governmental powers by type, nor to prohibit certain interactions between the branches of government.").

69. *See infra* notes 109–12 and accompanying text.

70. ERWIN CHEMERINSKY, FEDERAL JURISDICTION §2.3.1, at 56 (7th ed. 2016).

71. *Id.*

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

the injury will be redressed.[73] Given that standing is a jurisdictional question,[74] the burden of proving each element lies with the party asserting federal jurisdiction.[75] I turn to these elements in reverse order to dispense quickly with the second two, as they are not the focus of this Comment.

For any federal court to hear a case, the resolution of the action must provide redress for the injury complained of. This is logically a forward-looking test. Will finding for the plaintiff and awarding the requested relief redress the injury? Instead of requiring an absolute certainty, the Court requires a *likelihood* that the injury will be redressed, something beyond mere speculation.[76] For example, in *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, the Court recognized that civil penalties not paid to the plaintiffs could provide a deterrent effect to the defendant's ongoing unlawful activity.[77] Thus, the plaintiffs met the redressability element of the standing requirement.[78] As stated, however, the likelihood of redress must not be merely speculative.[79]

Whether the injury in data breach litigation can be redressed depends on what the injury is. Is it the anxiety that occurred because of the data breach itself, or is it the pecuniary harm from identity theft or fraud—or from trying to prevent identity theft or fraud? To analyze this prong of the *Lujan* test, federal courts need to determine what the harm is and then determine whether the relief requested will likely remedy that harm. Stated differently, courts cannot redress the harm until the injury-in-fact analysis is complete. Then, they must delve into the complex analysis of whether the requested remedy redresses that harm and how much remediation is required to satisfy constitutional standing requirements. Still, whether resolution of a data breach case can be properly redressed without merely speculating is outside the narrow scope of this Comment.

---

73. *Id.*; *see also* Kimberly N. Brown, *What's Left Standing? FECA Citizen Suits and the Battle For Judicial Review*, 55 U. KAN. L. REV. 677, 677 (2007) (referring to the *Lujan* test as "the reigning test").

74. *See supra* note 14 and accompanying text (discussing that issues of justiciability are jurisdictional in nature).

75. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 411–12 (2013) ("'The party invoking federal jurisdiction bears the burden of establishing' standing—and, at the summary judgment stage, such a party 'can no longer rest on . . . "mere allegations," but must "set forth" by affidavit or other evidence "specific facts."'" (quoting *Lujan*, 504 U.S. at 561)); *see also Lujan*, 504 U.S. at 561 (noting further that the requirements of proof depend on the litigation stage, factual allegation at the pleading stage or setting forth specific facts through evidence or affidavits at the summary judgment stage).

76. *Lujan*, 504 U.S. at 561.

77. 528 U.S. 167, 185–86 (2000).

78. *Id. But see* Massachusetts v. EPA, 529 U.S. 497, 518 (2007) ("When a litigant is vested with a procedural right, that litigant has standing if there is *some possibility* that the requested relief will prompt the injury-causing party to reconsider the decision that allegedly harmed the litigant." (emphasis added)).

79. *See* Ariz. Christian Sch. Tuition Org. v. Winn, 563 U.S. 125, 136 (2011); *see also* City of Los Angeles v. Lyons, 461 U.S. 95, 129 & n.20 (1983) (Marshall, J., dissenting) (noting that the redressability requirement "reflects the view that the adjudication of rights which a court is powerless to enforce is tantamount to an advisory opinion").

Next, the injury must be fairly traceable to the conduct complained of. This means there must be a causal nexus between the conduct complained of and the injury such that the line of causation between the two is not attenuated.[80] But this causal nexus requirement is a lower burden than traditional proximate cause.[81] Again, this should be discussed in more detail once harm has been found. This is because whether the harm is traceable largely depends on where the Court finds harm—whether the harm is in the anxiety resulting from the breach itself or merely in the subsequent malicious use of the data. Some may argue that traceability is difficult given the problems in knowing whether a particular malicious actor obtained the consumer's data from the complained of breach or from another source—especially given how many entities collect consumer data.[82] Still, if the plaintiff's anxiety is a result of their knowledge of the defendant's breach and not of subsequent misuse, then that harm, if recognized, may be more easily traceable to the defendant's failure to maintain a reasonable standard of care.[83] Again though, whether the injury complained of can be fairly traced to the conduct of the defendant is a topic to be explored later, in subsequent scholarship, and in further detail.

Finally, modern Article III standing law requires the existence of an injury-in-fact, even though this term did not appear in Supreme Court case law until 1970 in *Barlow v. Collins*.[84] Now, a plaintiff must show a violation of a legally protected interest that is concrete, particularized, and actual or imminent, as opposed to merely conjectural or hypothetical.[85] To be sure, all of these elements are required. While the concrete and particularized elements may have been conflated in the past, the Supreme Court held in *Spokeo, Inc. v. Robins* that while the "particularized" element is necessary, it is not sufficient.[86] For a harm to satisfy the injury-in-fact requirement, it must also be concrete.[87] In other words, it must be real—not abstract.[88] Though, as

---

80. Wash. Envtl. Council v. Bellon, 732 F.3d 1131, 1141 (9th Cir. 2013) (explaining that the alleged misconduct must not be a result of the actions of third parties not before the court, and that the causal connection must not be attenuated, even though there can be links in the chain).

81. Rothstein v. UBS AG, 708 F.3d 82, 91–92 (2nd Cir. 2013).

82. In other words, one could argue that even if a plaintiff proves that their data is for sale on the dark web, as one example, that fact alone does not necessarily mean the data came from the defendant's network at all. This is because that same data could be held by a plethora of other businesses that may or may not have been hacked as well. To support this theory, one need only look to the fact that data has become a commodity. Countless companies collect information on their customers. Adam B. Thimmesch, *Transacting in Data: Tax, Privacy, and the New Economy*, 94 DENVER L. REV. 145, 149 (2016) (discussing the ubiquitous nature of data collection practices). And those companies may not even know if they have been hacked. *See, e.g.*, Lance Bonner, Note, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 WASH. U. J.L. & POL'Y 257, 263 (2012) ("At least one of these data breaches went undiscovered for almost two years, and some most likely have never been discovered.").

83. Solove et al., *supra* note 7.

84. 397 U.S. 159 (1970); Sunstein, *supra* note 61.

85. 136 S. Ct. 1540, 1548 (2016); Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

86. 136 S. Ct. at 1548.

87. *Id.*

88. *Id.*

will be discussed later, *Spokeo* expressly states that intangible injuries can be concrete.[89]

Whether a harm is concrete is especially important in privacy cases, where injuries may be dignitary, as opposed to the pecuniary harms common in property-based grievances.[90] Still, data breach litigation typically resorts to claims of identity theft or fraud, or an increased risk thereof. As the next sections explain, circuits have not been entirely consistent on how to conduct injury in fact analysis.[91] But assuming the plaintiff has alleged facts necessary to show that the injury is particularized to them,[92] the inquiry must continue to the concreteness analysis.[93]

Before transitioning to Part V and the discussion of dignitary harms and the need to respect state sovereignty, this Part lays out the current state of affairs in data breach litigation. Section III.A delves deeper into the injury-in-fact analysis and the need to avoid speculative claims of harm. Then, Section III.B discusses the so-called circuit split over the question of whether an increased risk of harm is sufficient for Article III standing.

A. Injury in Fact After Clapper

In data breach litigation, the injury-in-fact inquiry has proved a difficult obstacle for plaintiffs.[94] Some see the injury to plaintiffs as trivial.[95] Others see the litigation as favoring plaintiffs' attorneys rather than remedying any real harm.[96] This is often

---

89. *Id.* at 1549.

90. Solove et al.*, supra* note 7, at 745 ("Knowing that thieves may be using one's personal data for criminal ends can produce significant anxiety.").

91. *See infra* Sections III.A–D.

92. Injuries are particularized when they have a "personal stake in the outcome of the controversy." Baker v. Carr, 369 U.S. 186, 204 (1962) (further implying that particularization helps ensure that the plaintiff's personal stake in the outcome of the controversy is necessary to sharpen the presentation of issues—that is, to properly advance the best arguments for the legal questions).

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

94. Bugni*, supra* note 12, at 72 ("In sum, plaintiffs face many obstacles in data breach class actions that relate to the injury element of standing.").

95. Of course, whether an injury is *de minimus* changes depending on what information is stolen. For example, in *Alonso v. Blue Sky Resorts, LLC*, 179 F. Supp. 3d 857, 862 (S.D. Ind. 2016), the plaintiff alleged that the breach resulted in the theft of their names, credit card numbers, and expiration dates. The court noted that credit cards were replaced, credit monitoring services provided, and the plaintiffs did not allege actual lost wages or reduced credit limits. *Id.* at 864. Thus, the court determined that the injury was not concrete, particularized, or certainly impending. *Id.*

96. *See* Abraham B. Dyk, *A Better Way to Cy Pres: A Proposal to Reform Class Action Cy Pres Distribution*, 21 NYU J. LEGIS. & PUB. POL'Y 635, 650 (2018) (noting the generous awards going to attorneys' fees "with little money going to actual class members"). Thinking logically, individual plaintiffs receive relatively low percentages in these class actions. On the other hand, the attorneys collectively receive very generous payouts. Thus, plaintiffs' attorneys seem to have the high incentive to bring data breach class action lawsuits against breached companies.

because the recovery by each individual plaintiff in the class can be quite low.[97] Nonetheless, settlements are often very high because of the number of plaintiffs involved.[98] Thus, resolving the standing issue in these cases remains critically important. Ultimately, this Comment argues that the Supreme Court should defer to state substantive law when determining whether an alleged injury is concrete. But first, an understanding of the current approach is warranted.

Typically, plaintiffs argue that the disclosure of the breached information either led to, or increased the risk of, identity theft or fraud.[99] Of course, if someone's identity has been stolen, that is a very real injury. But what if all the information needed to steal a plaintiff's identity is now in the hands of a malicious actor because of a data breach? Does the capability to steal a plaintiff's identity—or evidence that others have seen malicious use of their data—make a future possible injury imminent or does it remain hypothetical?

In *Clapper v. Amnesty International USA*, the plaintiffs were engaged in work that required them to communicate with individuals that the plaintiffs believed were under surveillance by the U.S. intelligence community.[100] Thus, the *Clapper* plaintiffs argued that they suffered an injury in fact because an objectively reasonable likelihood existed that their communications with those individuals would be captured by the intelligence community.[101] In a narrow 5-4 majority, the Court disagreed.[102] The Court held that the *Clapper* plaintiffs' "theory of *future* injury

---

97. *See, e.g.*, Kate O'Flaherty, *Equifax Can't Afford Promised Customer Payout, FTC Confirms*, FORBES (Aug. 1, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/08/01/ftc-confirms-equifax-cant-afford-promised-customer-payout [https://perma.cc/E4UT-98CG] (noting that the minimum $125 payout may not even be available to all customers); Jessica Karmasek, *Federal Judge Grants Final Approval in Consumer Class Action over Target Data Breach*, LEGAL NEWSLINE (Dec. 3, 2015), https://legalnewsline.com/stories/510651158-federal-judge-grants-final-approval-in-consumer-class-action-over-target-data-breach [https://perma.cc/FE9K-CYN3] (noting an average payout of $300).

98. *See, e.g.*, Brigette Honaker, *Equifax Data Breach Class Action Settlement*, TOP CLASS ACTIONS (July 26, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/909741-equifax-data-breach-class-action-settlement [https://perma.cc/GE6L-D7BZ] (estimating 147 million people affected for a $380.5 restitution fund with another $125 in potential funding); Kelly Tyko, *Yahoo Data Breach Settlement 2019: How to Get Up to $358 or Free Credit Monitoring*, USA TODAY (Oct. 14, 2019, 3:00 PM), https://www.usatoday.com/story/money/2019/10/14/yahoo-data-breach-117-5-million-settlement-get-cash-monitoring/3976582002 [https://perma.cc/KB8E-XWB3] (noting the $117.5 million class action settlement, which was only $358 per person but also noting that the amount could be $100 or less and that it depended the number of claimants relative to the size of the fund pool).

99. Brandon Ferrick, *No Harm, No Foul: The Fourth Circuit Struggles with the "Injury-in-Fact" Requirement to Article III Standing in Data Breach Class Actions*, 59 B.C. L. REV. ELEC. SUPPLEMENT 462, 463 (2018) (noting that "an increased risk of future identity theft is the most commonly alleged injury in lawsuits following data breaches" and also noting that two other arguments center around actual identity theft and actual financial harm).

100. 568 U.S. 398, 406 (2013) ("Respondents are attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals . . . .").

101. *Id.* at 407.

102. *Clapper v. Amnesty International USA*, OYEZ.COM, https://www.oyez.org/cases/2012

[was] too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'"[103] The Court further noted that deciding otherwise would amount to "abandon[ing] our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors."[104] In so holding, the *Clapper* Court expressly rejected the Second Circuit's "objectively reasonable likelihood" standard for determining when an injury is certainly impending.[105]

But the *Clapper* plaintiffs were asking the Court to confer standing where reaching the merits of the dispute would have forced the federal courts to determine the constitutionality of an action taken by another branch of government[106]—an action that would offend the original underlying purpose of standing, the separation of powers.[107] Even though reviewing the constitutionality of government action is a critical role of the Court,[108] Justice Alito—writing for the majority in *Clapper*—applied a heightened standard for these cases.[109] He noted, "[o]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."[110] Furthermore, Justice Alito noted that the federal courts have "often found a lack of standing" where they have been asked to "review actions of the political branches in the fields of intelligence gathering and foreign affairs."[111] Given that the *Clapper* Court stressed the importance of applying a heightened burden in cases that question the other branches of government—especially in cases that implicate the intelligence and foreign affairs communities—one may expect post-*Clapper* courts to apply a lesser standard to data breach claims that do not implicate these concerns. But that has not been the case.[112]

Furthermore, the *Clapper* plaintiffs were not completely off track. The *Clapper* decision was announced just four months before the revelations surrounding Edward

---

/11-1025 [https://perma.cc/2FS6-DMS3].

103. *Clapper*, 568 U.S. at 401. The Court further noted that the *Clapper* plaintiffs' argument rested on the "highly speculative fear" that the government was, or would be, targeting the people with whom the plaintiffs communicate, that they would be doing so under the authority of the law the plaintiffs sought declared unconstitutional, that the FISA judges would determine that the government satisfied the strictures of that law, that the government's surveillance attempts would be successful, and that the plaintiffs' communications would then actually be among those intercepted. *Id.* at 410.

104. *Id.* at 414.

105. *Id.* at 410. The Second Circuit's analysis would have established standing where plaintiffs could establish that they suffered burdens not based on "fanciful, paranoid, or otherwise unreasonable" grounds. *Id.* at 416 (quoting Amnesty Int'l USA v. Clapper, 667 F.3d 163, 180 (2d Cir. 2011) (Reena Raggi, J., dissenting)).

106. *Clapper*, 568 U.S. at 408.

107. *See supra* note 68 and accompanying text.

108. Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803) (establishing judicial review and noting that "the theory of every such government must be, that an act of the legislature, repugnant to the constitution, is void").

109. *See Clapper*, 568 U.S. at 408.

110. *Id.* (quoting Raines v. Byrd, 521 U.S. 811, 819–20 (1997)).

111. *Id.* at 409.

112. *See infra* Section III.B.

Snowden and the NSA's widespread surveillance program.[113] The *Clapper* plaintiffs lost because they were supposedly speculating about whether their communications had been collected.[114] But "[t]hey had no actual knowledge of these government surveillance programs because the programs were kept secret by the plaintiffs' adversary—the government."[115] Before Snowden, the lay citizen may have reasonably deemed fears of government spying as the fanciful fears of conspiracy theorists and anti-government activists. After Snowden, widespread government surveillance may be considered the norm—and hardly speculative. Still, reasonable minds can differ on how much speculation and inference is appropriate. In fact, reasonable minds did differ.[116] Regardless, courts should not lose sight of the fact that the context in which the Supreme Court decided *Clapper* was considerably different than private, consumer litigation.

Clapper has proven very influential in data breach litigation, even though data breach litigation does not present the same separation of powers concerns as were present in *Clapper*.[117] In applying *Clapper*, courts have seemingly come to opposite

---

113. Margo E. Kaminski, *Standing After Snowden*, 66 DEPAUL L. REV. 413, 421 (2017) ("Then in June 2013, a mere four months after *Amnesty*, the Snowden stories began."). In 2013, Snowden revealed that the government was conducting widespread surveillance that seems to make the *Clapper* plaintiffs' claims seem much less like speculation. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/8A6Y-N7SK] (reporting the mass surveillance at the heart of the Edward Snowden controversy); Glenn Greenwood, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 11, 2013, 09:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [https://perma.cc/6X7U-ESQX] (identifying Edward Snowden as the whistleblower). For a helpful background on Edward Snowden, see generally Hanna Kim, Note, *The Resilient Foundation of Democracy: The Legal Deconstruction of the Washington Post's Condemnation of Edward Snowden*, 93 IND. L.J. 533, 535–37 (2018).

114. Obama v. Klayman, 800 F.3d 559, 567 (D.C. Cir. 2015) (Williams, J., concurring) (explaining that the *Clapper* Court determined that plaintiffs were merely speculating but noting the strength of the plaintiff's claims, including the fact that the government had "already intercepted 10,000 phone calls and 20,000 emails involving one individual who [was] in regular communication with one of the plaintiffs").

115. Kaminski, *supra* note 113, at 421–22.

116. *Compare Klayman*, 800 F.3d at 564 (Brown, J., concurring) (distinguishing *Clapper* post-Snowden and noting that while "the *Clapper* plaintiffs relied on speculation and conjecture to press their claim, here, plaintiffs offer an inference derived from known facts"), *with id.* at 567 (Williams, J., concurring) ("But, assuming [plaintiffs'] evidence to be in some sense more specific, the relevant inquiry is whether that evidence indicates that the program targets plaintiffs. As to that, the plaintiffs here do no better than those in *Clapper*."), *and id.* at 569 (Sentelle, J., dissenting) (noting that "plaintiffs never in any fashion demonstrate that the government is or has been collecting such records from their telecommunications provider, nor that it will do so").

117. *See, e.g.*, Paul G. Karlsgodt & Dustin M. Dow, *The Practical Approach: How the Roberts Court Has Enhanced Class Action Procedure by Strategically Carving at the Edges*, 48 AKRON L. REV. 883, 891 (2015) ("The *Clapper* decision has been applied by many lower courts, particularly in the data breach context, in rejecting class actions due to the lack of any

conclusions.[118] When malicious actors steal data and expose it to the public, the victim's privacy has been intruded.[119] But if plaintiffs argue standing based on an increased risk of identity theft, then they arguably are speculating that *independent actors* not before the court will act in a certain way. That is precisely the sort of speculation *Clapper* sought to avoid—just in a different context. In the end—and as the next Section explains—circuit courts have seemingly applied two different approaches. One approach is stricter, and one more liberally recognizes the increased risk of harm as sufficient to confer standing.

B. Increased Risk of Identity Theft

For several years, scholars and judges have argued that circuits are split as to whether plaintiffs can establish standing based on an increased risk of identity theft.[120] However, the split arguably does not exist at all. Instead, the cases can be synthesized by analyzing the factual differences.[121] In other words, the circuits are not necessarily applying different legal analyses, they are simply dealing with differing sets of facts. Judge Scriven in the Middle District of Florida has gleaned three factors from an analysis of the various circuits' standing decisions.[122] These are

---

injury-in-fact sufficient to support Article III standing.").

118. *See* Kimberly Fasking, Comment, Beck v. McDonald*: The Waiting Game—Is an Increased Risk of Future Identity Theft an Injury-in-Fact for Article III Standing?*, 41 AM. J. TRIAL ADVOC. 387, 389 (2017) ("Currently, a circuit split exists on the issue of whether the victim of a data breach has Article III standing to sue the entity with whom she entrusted her personally identifying information when that information has not yet been used to commit fraud.").

119. Benjamin C. West, *No Harm, Still Foul: When an Injury-in-Fact Materializes in a Consumer Data Breach*, 69 HASTINGS L.J. 701, 716 (2018) ("Even without the loss of time and money, there is a more basic harm—the invasion of privacy itself. On its own, a breach constitutes a sufficient harm for standing purposes because of the presumed psychological harms associated with it.").

120. Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017) ("Our sister circuits are divided on whether a plaintiff may establish an Article III injury in fact based on an increased risk of future identity theft."); Allison Holt, Joby Ryan & Joseph W. Ryan, Jr., *Standing in the Midst of a Data Breach Class Action*, 84 DEF. COUNS. J. 1, 9 (2017) (explaining that "[w]hat practitioners are left with is a true Circuit Split"); Hanley Chew & Tyler G. Newby, *Eight Circuit Holds Data Breach Plaintiffs Must Allege Actual Injury to Establish Standing*, 22 NO. 9 CYBERSPACE LAW. NL 6 (2017) ("The Circuit Split is likely to continue until—and unless—the Supreme Court weighs in and offers more definitive guidance."); Michael Hopkins, Comment, *Your Personal Information Was Stolen? That's an Injury: Article III Standing in the Context of Data Breaches*, 50 U. PAC. L. REV. 427, 440 (2019) (noting that "the growing incidence of data breach litigation has since led to a sizeable circuit split").

121. *In re* 21st Century Oncology Customer Data Sec. Breach Litig., 380 F. Supp. 3d 1243, 1251 (M.D. Fla. 2019) ("Notably, however, although the circuits have diverged in result, the bases behind the differing decisions have several commonalities. That is to say, the differing sets of facts involved in each circuit's decision are what appear to have driven the ultimate decision on standing, not necessarily a fundamental disagreement on the law.").

122. *Id.* at 1251–54; *see also In re* Brinker Data Incident Litig., No. 3:18-cv-686-J-32MCR, 2019 WL 3502993, at *6 (M.D. Fla. Aug. 1, 2019) (endorsing Judge Scriven's analysis).

(1) the motives of the potentially malicious actor,[123] (2) the type of information involved in the data breach,[124] and (3) whether evidence exists showing that a third party has in fact accessed or fraudulently used the information at issue.[125]

All of this shows how plaintiffs, under the right circumstances, can argue that they have standing in federal court based on an increased risk of identity theft. Given this well-documented path to standing, plaintiffs' lawyers may be most compelled to argue standing on a theory of identity theft. But that should not be the only path. The Supreme Court in *Spokeo* clearly stated that intangible harms can be sufficient to confer Article III standing.[126] Thus, plaintiffs' lawyers should at least argue in the alternative that their clients have standing based on the dignitary harms they suffered as a result of the data breach. If they do, Judge Scriven's three-prong imminence test[127] can still be instructive because meeting those factors would logically deepen a plaintiff's negative emotional state. Still, plaintiffs' attorneys may decide that arguing standing under a theory of dignitary harm may imperil their chances at class certification under Federal Rule of Civil Procedure 23(a)(2),[128] but that discussion will be saved for a subsequent article. Instead of delving into the question of class certification, this Comment assumes for now that class certification will not prohibit dignitary harms from being redressed in federal court.

IV. DIGNITARY HARM AND RESPECT FOR STATE SOVEREIGNTY

As discussed above, the current standing arguments in data breach litigation center around the idea that the harm is the identity theft or fraud that results from the privacies of life being made available online. But while identity theft or fraud is certainly a harm, it can take a significant amount of time to develop.[129] The more immediate harm from data breaches is often the dignitary harm that results not from the subsequent misuse of the data but from the mere fact that the data has been disclosed to the public.[130] And while arguments may center around pecuniary harm,

123. *21st Century Oncology*, 380 F. Supp. 3d at 1252 ("Thus, the Court finds that one factor considered by the diverging circuits in determining whether Plaintiffs have alleged an injury based on an increased risk of identity theft is the alleged motive of the unauthorized third-party that obtained access to Plaintiffs' personal information.").

124. *Id.* at 1253–54 ("What can be gleaned from the circuits' decisions in this respect is that the type of information compromised can play a role in the Court's injury in fact analysis, and, where that information includes personally identifiable information, this factor will weigh in favor of a finding of injury in fact.").

125. *Id.* at 1254 ("Third, the circuits have found that an increased risk of identity theft is more likely to constitute an injury in fact where there is evidence that a third-party has accessed the sensitive information and/or already used the compromised data fraudulently.").

126. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

127. *21st Century Oncology*, 380 F. Supp. 3d at 1252–54.

128. *See* Fed. R. Civ. P. 23(a)(2). Rule 23(a)(2) requires that class members have "questions of law or fact" in common. Some may argue that this could preclude certification for dignitary harms that *may* require more investigation into individual class members than identity-based harms. While I disagree, this will be the focus of follow-up scholarship.

129. West, *supra* note 119, at 712–13 (discussing the delay that can occur between the breach and the resulting harm and noting that this creates problems with statutes of limitation).

130. *Id.* at 716 ("Even without the loss of time and money, there is a more basic harm—

intangible harms—like anxiety and emotional distress—do not per se fail the injury-in-fact analysis. The Supreme Court has expressly determined that intangible injuries can be concrete.[131]

In recognizing that an intangible injury can be concrete, Justice Alito—writing for the majority in *Spokeo*—noted that courts should consider historical practice and the judgment of Congress.[132] With causes of action arising under common law, the historical factor then becomes more important.[133] For the historical factor, *Spokeo* instructs courts to determine whether the intangible harm bears a "close relationship to harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[134]

The dignitary harm inflicted by failing to protect consumer data privacy seems to bear a close relationship to the commonly recognized right to privacy. Samuel Warren and Louis Brandeis wrote their famous article, *The Right to Privacy*, in 1890.[135] In it, they proclaimed that "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[136] They wrote their article in response to a growing concern of the media intruding on the privacies of life.[137] The result was simple: Warren and Brandeis subscribed to Judge Cooley's belief[138] that each person has a "general right to be let alone."[139] Even in 1890, Warren and Brandeis saw mental suffering as a recognized "basis for compensation."[140]

---

the invasion of privacy itself. On its own, a breach constitutes a sufficient harm for standing purposes because of the presumed psychological harms associated with it.").

131. *Spokeo*, 136 S. Ct. at 1549 (referring to two free speech cases as examples of intangible harm, even though those cases did not implicate standing doctrine).

132. Long v. Se. Penn. Trans. Auth., 903 F.3d 312, 321 (3rd Cir. 2018) ("In determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles." (quoting *Spokeo*, 136 S. Ct. at 1549)).

133. Of course, this is because if a law is judge made, the legislature played no role. Then again, one may argue that legislative inaction is itself a judgment call.

134. *Spokeo*, 136 S. Ct. at 1549.

135. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

136. *Id.* at 198.

137. *Id.* at 195 ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" (quoting THOMAS M. COOLEY, COOLEY ON TORTS 29 (2d ed. 1888))).

138. *Id.*

139. *Id.* at 205 ("These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone.").

140. *Id.* at 213 ("If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation.").

Following Warren and Brandeis's article, some courts recognized the right to privacy, and others were slower to accept it.[141] But regardless, the recognition of dignitary harms—those against the dignity and reputation of the victim—have long been recognized at common law.[142] In 1960, William Prosser published his influential article, *Privacy*, in which he built on Warren and Brandeis's work by articulating four invasion-of-privacy torts.[143] These torts were the intrusion upon seclusion, public disclosure of private facts, false light, and appropriation.[144] Like the anxiety and general emotional distress in data breach litigation, the harms these torts recognize represent harms to the dignity and inviolate personality of the victim.[145] But these harms have not only been recognized by academics; the courts have long accepted them as well.[146]

Arguably, the harm resulting from a data breach bears an even closer relationship to the breach of confidentiality tort.[147] In *Burger v. Blair Medical Associates, Inc.*, the Supreme Court of Pennsylvania noted that the "confidential nature" of the relationship between patient and physician, and the "personal nature of the information" collected, gave rise to a breach of confidential tort claim if that sensitive information was improperly disclosed.[148] Similarly, when companies collect and

---

141. Prosser, *supra* note 49, at 385 (discussing cases in New York and Massachusetts that allowed recovery on an independent right to privacy theory and then discussing *Atkinson v. John E. Doherty & Co.*, 80 N.W. 285 (Mich. 1899), in Michigan, which "flatly rejected the whole idea").

142. Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 380–81 (2013) ("This view of privacy harms focuses on dignitary harms, like harm to reputation, based on the concept that privacy violations are a type of invasion to the victim's dignity.").

143. Prosser, *supra* note 49.

144. *Id.*

145. Solove et al., *supra* note 7 (discussing emotional distress as a "crucial aspect" of the harm suffered by the consumer victims of data breaches); Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 23 (2008) ("If dignity recognizes the right of each individual to his or her own, unique 'inviolate personality,' privacy allows that personhood to develop.").

146. Even in 1960, Prosser noted that "the right to privacy, in one form or another, is declared to exist by the overwhelming majority of the American courts." Prosser, *supra* note 49, at 386. Apart from privacy torts, the American Law Institute also created a project, in which Daniel Solove and Paul Schwartz were the reporters, to "provide a set of best practices for entities that collect and control data concerning individuals." Daniel Solove, *ALI Principles of Law, Data Privacy*, TEACHPRIVACY (May 23, 2019), https://teachprivacy.com/ali-principles-of-law-data-privacy [https://perma.cc/KA4L-QBTQ]; Daniel J. Solove & Paul M. Schwartz, ALI Data Privacy: Overview and Black Letter Text (Jan. 24, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3457563 [https://perma.cc/3XWC-EXVP].

147. While the tort most commonly applies to physicians, it can be found to apply more broadly by looking at the nature of the relationship between the parties, by considering fiduciary duties, or by finding a breach of an implied contract of confidentiality. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 157–58 (2007).

148. *See* 964 A.2d 374, 376, 381 (Pa. 2009) (noting the existence of a physician-patient

retain data on consumers because of the established business-consumer relationship, a privilege should be created whereby those businesses must exercise due diligence to protect that data—the confidences—the consumers trusted them with. Then, when malicious actors break into those companies' networks—and exfiltrate sensitive consumer data because of the companies' failure to adequately safeguard the data—those companies have breached the consumers' confidence.[149]

Thus, dignitary harms have long been recognized, and they seem to satisfy the *Spokeo* requirements for intangible but concrete injuries. Given the language in *Spokeo* and given the history of recognizing dignitary harms, the idea that federal courts would recognize dignitary harms in data breach litigation should not be radical. But there is another reason to recognize dignitary harms—that the same underlying rationale in *Erie* Doctrine applies here and, therefore, the Supreme Court should instruct lower federal courts to defer to state interpretations of what constitutes harm under the laws that the state created. Some may ask why plaintiffs cannot simply bring their claims in state court to begin with, but that argument misses the point. Plaintiffs have a statutory right to bring cases in federal court that do not necessarily have a federal interest, so long as those cases satisfy the requirements for diversity jurisdiction.[150] Just as federal courts defer to state substantive law in these diversity cases, the rationale of *Erie* can be furthered by looking to the underlying state law to determine whether the "concrete" requirement of the injury-in-fact analysis has been satisfied. The rest of this Part delves into that argument by discussing *Erie* Doctrine and its underlying rationale; how the concrete analysis of standing doctrine implicates the substantive law at issue; and why those rationales and the substantive nature of the concreteness analysis militate toward deference to state interpretations of their own law.

A. Erie *Doctrine*

In 1938, the Supreme Court decided *Erie Railroad Co. v. Tompkins*.[151] There, the plaintiff was walking next to train tracks and was injured by an object protruding from a passing train.[152] The company—Erie Railroad Company—argued that Pennsylvania law should apply.[153] However, Tompkins argued for the application of *Swift v. Tyson*, such that the absence of state statutory law would have allowed the

---

breach of confidentiality tort when the physician discloses the privileged confidences of the patient).

149. The analogy here is even stronger because unlike some other torts, the breach of confidentiality does not require a showing that the conduct of the defendant was "highly offensive." Solove et al., *supra* note 7, at 746 ("The tort of breach of confidentiality recognizes emotional distress as a cognizable injury without the need to show highly offensive conduct.").

150. F. Andrew Hessick, *Cases, Controversies, and Diversity*, 109 NW. U. L. REV. 57, 100 (2014).

151. 304 U.S. 64 (1938).

152. *Id.* at 69 (noting the allegation that the plaintiff "was struck by something which looked like a door projecting from one of the moving cars").

153. *Id.* at 70.

federal courts to apply their own general common law.[154] The Court rejected the notion that there is such a thing as a general federal common law.[155]

Instead, the Court determined that for issues of substantive law, federal courts must defer to the state law applicable in each case, whether statutory or common.[156] Of course, the Court did not mean that there is no federal common law at all. On the same day the Court announced *Erie*, it also explained, in *Hinderlider v. La Plata River & Cherry Creek Ditch Co.*, that some non-general federal common law still exists.[157] Still, that case directly involved two states.[158] And as Jay Tidmarsh has argued, in cases where a state's self interest in the outcome is "less acute, and participation by interested parties is possible[,] . . . no resort to a separate body of federal common law is necessary."[159] While both Tidmarsh's article and the *Erie* decision discussed the rules of decision governing a case, their rationales remain valid in the standing context.

Multiple rationales underpinned the *Erie* decision, and they should be considered here. While the *Erie* decision has been debated,[160] the widely recognized underlying rationales were to prevent forum shopping, to promote uniformity of the administration of the laws of the individual states,[161] and to respect federalism.[162] If the federal courts continue to maintain that these rationales are sacred, then the application of these rationales to concreteness analysis could be compelling.

---

154. *Id.* at 70–71. In *Swift v. Tyson*, Justice Story endorsed the idea of a federal common law for "questions of a more general nature." Gregory Gelfand & Howard B. Abrams, *Putting Erie On the Right Track*, 49 U. PITT. L. REV. 937, 943 (1998) (quoting Swift v. Tyson, 41 U.S. 1, 18–19 (1842)).

155. *Erie*, 304 U.S. at 78 ("There is no federal general common law.").

156. *See id.* at 78–79.

157. 304 U.S. 92, 110 (1938) ("For whether the water of an interstate stream must be apportioned between the two States is a question of 'federal common law' upon which neither the statutes nor the decisions of either State can be conclusive.").

158. *Id.*

159. Jay Tidmarsh, *A Theory of Federal Common Law*, 100 NW. U. L. REV. 585, 588 (2006).

160. *E.g.*, Boggs v. Blue Diamond Coal Co., 497 F. Supp. 1105, 1111 (E.D. Ky. 1980) (explaining the debate as to whether *Erie* "is a statutory or constitutional decision").

161. Jeffrey W. Stempel, *Shady Grove and the Potential Democracy-Enhancing Benefits of Erie Formalism*, 44 AKRON L. REV. 907, 923 (noting "*Erie*'s policy goals of avoiding, where possible, disparate outcomes in state and federal court as well as the discouragement of undue federal-state forum shopping").

162. Boyle v. United Techs. Corp., 487 U.S. 500, 517 (1988) (Brennan, J., dissenting) ("Thus, *Erie* was deeply rooted in notions of federalism, and is most seriously implicated when, as here, federal judges displace the state law that would ordinarily govern with their own rules of federal common law."); Hanna v. Plumer, 380 U.S. 460, 474 (1965) (Harlan, J., concurring) ("Erie was something more than an opinion which worried about 'forum-shopping and avoidance of inequitable administration of the laws,' although to be sure these were important elements of the decision. I have always regarded that decision as one of the modern cornerstones of our federalism, expressing policies that profoundly touch the allocation of judicial power between the state and federal systems." (citation omitted)); *In re* County of Orange, 784 F.3d 520, 524 (9th Cir. 2015) (referring to "*Erie's* federalism principle").

First, *Erie* sought to avoid forum shopping—the practice of seeking out the court mostly likely to provide a favorable outcome.[163] In the standing context, recognizing harms inconsistent with state interpretations could lead to outcome-determinative forum shopping by plaintiffs' lawyers. Second, Justice Brandeis—writing for the Court in *Erie*—was particularly concerned that *Swift* had "prevented uniformity in the administration of the law of the state."[164] In other words, the doctrine in *Swift v. Tyson* meant that diversity jurisdiction cases in federal court applied different substantive law—and potentially resulted in different outcomes—than if those same cases were litigated in state court.[165] In the standing context, a failure to implement state interpretations of harm will lead to federal courts vindicating rights less often under the same underlying law because they may have different opinions about which harms create a case or controversy. And third, Justice Brandeis noted in the concluding paragraphs of the *Erie* majority opinion that "[s]upervision over either the legislative or the judicial action of the states is in no case permissible except as to matters by the constitution specifically authorized or delegated to the United States."[166] In other words, federal courts should respect our constitutional system of federalism—do not intrude on a state's power to make its own laws. Again, in the standing context, applying state substantive law—as *Erie* mandates—but without deferring to state interpretations of what constitutes harm under those same laws seems to violate federalism and the spirit of *Erie*.

These same rationales should be considered in data breach litigation when determining whether plaintiffs have standing. Specifically, and as stated above, the Supreme Court should defer to state substantive law when determining whether the complained-of injury is concrete for the purposes of the injury-in-fact analysis. This is because, as the next section discusses, the "concrete" nature of the injury is necessarily wrapped up in the merits of the plaintiffs' claims. Of course, federal courts will always apply the irreducible minimum three-prong test, but that should not remove their ability to look to state authority when ensuring the existence of a concrete injury.

B. Standing as Procedural, Concreteness as Substantive

Even though some cases have seemed to differentiate subject-matter jurisdiction and questions of standing,[167] more recent Supreme Court case law has made it clear that issues of justiciability represent a limitation on federal subject-matter

---

163. Gelfand et al., *supra* note 154, at 972 (discussing the forum-shopping incentive test and noting the possibility that a "reasonable lawyer who is about to file the lawsuit would be substantially motivated by the difference between the state and federal rules to select either the federal or state court over the other").

164. *Erie*, 304 U.S. at 75.

165. *See id.*

166. *Id.* at 79 (further noting that "[a]ny interference with either . . . is an invasion of the authority of the state, and, to that extent, a denial of its independence").

167. *See, e.g.*, Powell v. McCormack, 395 U.S. 486, 512 (1969) ("[T]here is a significant difference between determining whether a federal court has 'jurisdiction of the subject matter' and determining whether a cause over which a court has subject matter jurisdiction is 'justiciable.'" (quoting Baker v. Carr, 369 U.S. 186, 198 (1962))).

jurisdiction.[168] If a plaintiff presents a nonjusticiable case, federal courts have no jurisdiction.[169] Of course, one element of justiciability is that plaintiffs must have standing to bring suit.[170] These types of questions may not always be thought of as substantive, and therefore, *Erie* has not been applied.[171] Instead of deferring to the desires of state judges and lawmakers, federal courts have simply noted their requirement to apply the irreducible minimum three-prong test. Critically, and as previously stated, this Comment recognizes that federal courts must comply with the strictures of Article III precedent.

But while the injury-in-fact prong must be satisfied, the Supreme Court should recognize that analyzing the injury necessarily should involve an analysis of the law that created the legally protected interest that has been allegedly violated. In other words, for the concreteness analysis of the injury-in-fact prong, the Justices should defer to state interpretations of what counts as a concrete injury under the laws that the state created. Courts ask whether the plaintiff complains of a violation of a legally protected interest. When answering this question, the appropriate analysis would be to ask what legal interest the creator of the law sought to protect. If the interest the state sought to protect has been violated, the Supreme Court should hold that plaintiffs have suffered a concrete injury. The Supreme Court should not care that a state, and not the federal government, created the legal interest. If a state cause of action seeks to protect dignitary harms in the data breach context—or any other context—then those harms should be sufficient to confer standing such that plaintiffs' rights can be vindicated in federal court. Anything less defeats the purpose of diversity jurisdiction and disrespects the state's objective and its sovereign right to define its own legal protections.

C. Federalism, Dual Sovereignty, and Extending Erie

Central to our constitutional republic, and part of the underlying rationale in *Erie*, is the idea that the federal government and the various state governments are separate political sovereigns. One should not intrude upon the other's sphere of power.[172]

---

168. *See* United States v. Sanchez-Gomez, 138 S. Ct. 1532, 1537 (2018) ("A case that becomes moot at any point during the proceedings is 'no longer a "Case" or "Controversy" for purposes of Article III,' and is outside the jurisdiction of the federal courts." (quoting Already, LLC v. Nike, Inc., 568 U.S. 85, 91 (2013))). Of course, this was in the context of mootness. *Id.*

169. CAMP Legal Def. Fund, Inc. v. City of Atlanta, 451 F.3d 1257, 1269 (11th Cir. 2006) ("The Constitution of the United States limits the *subject matter jurisdiction* of federal courts to 'Cases' and 'Controversies.'" (emphasis added)); *see also* Norvell v. Sangre de Cristo Dev. Co., 519 F.2d 370, 378 (10th Cir. 1975) ("District courts are without jurisdiction when confronted with non-justiciable political questions.").

170. Flast v. Cohen, 392 U.S. 83, 98 (1968) (noting that "[s]tanding is an aspect of justiciability"); *see also* La. Env't Action Network v. Browner, 87 F.3d 1379, 1385 (D.C. Cir. 1996) (referring to standing as an element of justiciability).

171. *See* Gasperini v. Ctr. for Humans., Inc., 518 U.S. 415, 427 (1996) ("Under the *Erie* doctrine, federal courts sitting in diversity apply state substantive law and federal procedural law.").

172. McCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 410 (1819) ("In America, the powers of sovereignty are divided between the government of the Union, and those of the States. They

Federalism was developed by the Framers as a "response to the real and perceived shortcomings of the Articles of Confederation."[173] Still, the debate over the bounds of federalism existed even at the Founding. For example, Alexander Hamilton proposed that state governors should be appointed by the President.[174] Today's debate over the value of federalism would probably not go that far. Even the modern legal scholars that do not prioritize federalism would likely be uncomfortable with Hamilton's proposed level of federal involvement in state politics.[175]

To be sure, the centrality and importance of federalism is still a debated topic. But even though the Court has permitted the expansion of the federal government,[176] federalism remains a core constitutional principle and a powerful "protection against federal tyranny."[177] The core of the federalism argument is simple: "Impermissible interference with state sovereignty is not within the enumerated powers of the National Government, and action that exceeds the National Government's enumerated powers undermines the sovereign interests of States."[178]

The Supreme Court should consider federalism when analyzing whether plaintiffs have suffered a concrete injury after a data breach. As discussed above, many of the causes of action arise under state law.[179] As Professor Hessick notes, "Whether a plaintiff has standing depends on whether the [substantive] law gives [them] standing."[180] This means that determining whether the complained-of injury is concrete "cannot be divorced from the merits" of the case.[181] This view of standing, as intertwined with the merits, means that in diversity cases the Supreme Court should apply the state's interpretation of state law claims—just as state courts do.[182]

---

are each sovereign, with respect to the objects committed to it, and neither sovereign with respect to the objects committed to the other.").

173. Richard E. Levy & Stephen R. McAllister, *Defining the Roles of the National and State Governments in the American Federal System: A Symposium*, 45 U. KAN. L. REV. 971, 974 (1997).

174. *Id.* at 974–75.

175. For interesting background information on some of the different conceptualizations of federalism and some criticism of the traditional idea of dual federalism, see Robert A. Schapiro, *Toward a Theory of Interactive Federalism*, 91 IOWA L. REV. 243 (2005).

176. Namely, in the expansion of the Commerce Clause in cases like *Wickard v. Filburn*, 317 U.S. 111 (1942).

177. Levy, *supra* note 173, at 975, 979 (referring to Alexander Hamilton's Federalist No. 32 and later discussing that federalism can be interpreted to promote political accountability and protect individual liberties).

178. Bond v. United States, 564 U.S. 211, 225 (2011) (citing New York v. United States, 505 U.S. 144, 155–59 (1992)) (citation omitted).

179. *See supra* Part II.

180. F. Andrew Hessick, *Standing in Diversity*, 65 ALA. L. REV. 417, 418 (2013).

181. *Id.*

182. *Id.* Applying state standing law in diversity cases also comports with the purpose underlying diversity jurisdiction. *Id.* at 424. The point is that federal court can act as an alternative forum for litigants that live in different states. *Id.* This will almost always be the case in data breach litigation because of the nature of our economy. Companies large enough to be sued via class action lawsuit for a data breach are likely doing business across state lines. Applying federal standing law to data breach litigation is merely a signal to data breach plaintiffs that diversity jurisdiction is simply not available to them in the same way, that their

Of course, requiring the federal judiciary to limit itself to cases and controversies is important. But that does not negate the point that, in determining whether a legally protected interest has or has not been violated, the Supreme Court should defer to state interpretations of what constitutes harm under their own laws. In the data breach context, this means that instead of relegating the standing analysis to identity-based harm analysis in all cases, courts should recognize the harm that the state causes of action seek to protect.

We have seen that standing analysis can be more rigorous when national security and the intelligence community are at issue, like in *Clapper*.[183] And we saw in that same case that there is a heightened interest in deferring to another branch of government.[184] But just as the separation of powers may lead to a heightened reason to find a lack of standing, federalism—respect for the state's right to determine when harm exists under its own common and statutory law—should create a less searching standard whereby the Supreme Court instructs federal courts to defer to the state's understanding of harm. Let the state determine whether the state believes the alleged injury is sufficiently pronounced.[185]

Courts have sometimes seemed to confer standing on the grounds of emotional, dignitary harms.[186] And the *Spokeo* test for intangible injuries seems to expressly allow for that.[187] But the *Spokeo* test should not be the only way in which a court could recognize emotional and dignitary harms in data breach litigation. The

---

harm must be greater in federal court versus state court.

183. *See supra* notes 109–13 and accompanying text.

184. *See supra* Section III.A.

185. Unfortunately, the Supreme Court to date has not followed this reasoning. *See* Hollingsworth v. Perry, 570 U.S. 693, 715 (2013) ("And no matter its reasons, the fact that a State thinks a private party should have standing to seek relief for a generalized grievance cannot override our settled law to the contrary."). But even in *Hollingsworth*, the Court was analyzing particularization. *Id.* (noting the requirement that plaintiffs seek relief for a "personal, particularized injury"). Maybe the Court will be inclined to view federalism differently under the "concrete" injury analysis, especially given Justice Thomas's view that parties seeking relief under a private right of action should have an easier route to standing. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550, 1552 (2016) (Thomas, J., concurring).

186. *E.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010) (finding an injury in fact when "the only present injury" was that the plaintiff had "generalized anxiety and stress"—though whether the anxiety was enough is arguably unclear given that the *Krottner* court also found that the theft of the laptop created an increased risk of harm); *see also* Doe v. Chao, 540 U.S. 614, 641 (2004) (Ginsburg, J., dissenting) ("Doe has standing to sue, the Court agrees, based on 'allegations that he was "torn . . . all to pieces" and "greatly concerned and worried" because of the disclosure of his Social Security number and its potentially "devastating" consequences.'"). Of course, *Doe* was in the Privacy Act context where Congress had expressly created a legally protected interest. *Id.* Furthermore, these examples pre-date *Spokeo*. They represent instances where emotional, dignitary harms have been sufficient, but they do not apply the reasoning in *Spokeo* for recognizing intangible injuries. Also, the cited language in *Chao* was merely dicta. Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017).

187. *Spokeo*, 136 S. Ct. at 1549 ("Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.").

Supreme Court should consider the underlying rationale of *Erie* doctrine and extend that rationale to the concrete injury analysis.[188] While standing is a jurisdiction question,[189] determining whether a harm is concrete necessarily becomes intertwined with substantive law.[190] Thus, based on the same underlying rationale in *Erie*,[191] the Supreme Court should defer to state sovereignty—it should look to state substantive law in determining whether the state common or statutory law recognizes the harm complained of. If state common or statutory law recognizes dignitary harms in data breach litigation, then plaintiffs alleging those harms have alleged a concrete injury to a protected legal right—the federal inquiry should go no further. Likewise, if a state determines that recognizing anxiety harms in data breach litigation is not the law of that state, then the federal judiciary should not second guess that state's decision and standing should not exist. This could lead to inconsistent results among the states, but of course it is each state's right to have a law inconsistent from the rest. If the United States Congress determines that this inconsistency is undesirable, then preemption of that inconsistency is within their power.

V. INCONSISTENT RESULTS, THE SEPARATION OF POWERS, AND CONGRESSIONAL ACTION

Failing to defer to state law could lead to different results in federal and state courts.[192] Data breach plaintiffs reside in jurisdictions across the country, and these lawsuits are often class actions that rely on diversity jurisdiction under the Class Action Fairness Act.[193] Thus, they have a right to litigate in federal court. But without

---

188. *See supra* Section IV.A.

189. *See supra* note 14 and accompanying text (discussing that issues of justiciability are jurisdictional in nature); *supra* Section IV.B.

190. Hessick, *supra* note 180, at 421 ("Although framed as a threshold jurisdictional question, standing cannot be so easily separated from the merits of the case.").

191. Pizarro-de-Ramirez v. Grecomar Shipping Agency, 82 F.R.D. 327, 330 (D.P.R. 1976) ("In *Hanna*, the policies underlying the *Erie* decision were defined as discouragement of forum shopping and avoidance of inequitable administration of the laws."). *But see* Hanna v. Plumer, 380 U.S. 460, 474 (1965) (Harlan, J., concurring) ("Erie was something more than an opinion which worried about 'forum-shopping and avoidance of inequitable administration of the laws,' although to be sure these were important elements of the decision. I have always regarded that decision as one of the modern cornerstones of our federalism, expressing policies that profoundly touch the allocation of judicial power between the state and federal systems." (internal citation omitted)).

192. Heather Elliott, *Federalism Standing*, 65 ALA. L. REV. 435, 436 (2013) (discussing Judge Fletcher's scholarship and arguing that standing analysis can have the troubling result "that state courts can announce unreviewable decisions on federal law" and further discussing Andrew Hessick's point that state law claims should be analyzed under state standing law so that litigants are "truly free to choose between state and federal court" without risking dismissal of the case). Notably, while this paper only argues that federal courts should defer to state law when analyzing whether a harm is concrete, Professor Hessick has argued more broadly that "[f]ederal justiciability doctrines should not apply to state law suits brought in federal court under diversity jurisdiction." Hessick, *supra* note 150, at 106.

193. 28 U.S.C. § 1332(d)(2) (2018); *see also* Sean-Patrick Wilson & Roland M. Jaurez, *Class Action Fairness Act: Determining the "Amount in Controversy" in California*, HUNTON

exercising deference to the states, federal judges are removing this right to sue in federal court and relegating data breach plaintiffs to the state judicial process. This point merely serves the purpose of noting that symmetry between federal and state courts would lead to more consistent results. Just as in *Erie*,[194] federal courts should be concerned that these inconsistent results could lead to forum shopping.[195]

As discussed above, the "concrete harm" analysis always seems to come back to identity theft, or at least a heightened risk of being a victim of identity theft or fraud.[196] But why? The courts have long recognized dignitary harms in other contexts. Prosser's invasion of privacy torts are just that.[197] While some causes of action—like a violation of the right to publicity—seek to recover from economic or property harm,[198] other causes of action—like appropriation—seek to redress dignitary harms.[199] For example, one particularly analogous tort, the breach of confidentiality, recognizes "harms of broken trust, betrayal, and disrupted expectations of secrecy."[200] But just because one harm is dignitary and the other is pecuniary should not mean that the federal courts will refuse to even hear the case.

Given that the courts have not refused to recognize all dignitary harm,[201] relegating data breach claims to a risk of identity theft analysis seems inconsistent. Why would the courts recognize dignitary harm in one context, but not recognize the

---

EMP. & LAB. PERSPS. (July 2, 2018), https://www.huntonlaborblog.com/2018/07/articles/california-developments/class-action-fairness-act-determining-amount-controversy-california [https://perma.cc/USV8-M6W8] (discussing further that defendants can remove these class actions to federal court if originally filed in state court); Perry Cooper, *T-Mobile Keeps Data Breach Class Action Federal*, BLOOMBERG LAW (April 3, 2019, 4:19 PM), https://news.bloomberglaw.com/class-action/t-mobile-keeps-data-breach-class-action-federal [https://perma.cc/62DJ-WQZ2].

194. Hanna v. Plumer, 380 U.S. 460, 467 (1965) ("The decision was also in part a reaction to the practice of 'forum-shopping' which had grown up in response to the rule of *Swift v. Tyson*.").

195. Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co., 559 U.S. 393, 456 (2010) (Ginsburg, J., dissenting) ("[F]orum shopping will undoubtedly result if a plaintiff need only file in federal instead of state court to seek a massive monetary award explicitly barred by state law.").

196. *See supra* note 15 and accompanying text.

197. Prosser, *supra* note 49.

198. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 (AM. L. INST. 1995) (explaining that damages for violations of the right to publicity address the commercial interest in one's name or likeness).

199. Kenneth S. Abraham & G. Edward White, *The Puzzle of the Dignitary Torts*, 104 CORNELL L. REV. 317, 340 (2019) (explaining that while appropriation has often evolved into a commercial appropriation claim—the right to publicity—appropriation began as a tort focused on the protection of dignitary harms that occur based on a "presumed or anticipated diminution of respect for the plaintiff that results from being perceived to have voluntarily associated with the defendant's commercial activity").

200. Solove, *supra* note 7, at 770–71 (quoting Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 147–48 (1992)).

201. *Id.* ("In case after case involving the privacy torts and breach-of-confidentiality tort, courts have recognized harm based on pure emotional distress or psychological impairment. Fear, anxiety, embarrassment, and loss of trust are all recognized as harms. Humiliation, nervousness, worry, and loss of sleep are understood as compensable harms.").

dignitary harm that results from the breach of a consumer's data, regardless of whether the data is ever misused? Requiring a misuse of the data misses the point. The simple breach of a duty to safeguard personal and confidential data—to properly secure the data a company has collected on consumers—can itself result in a dignitary harm analogous to the breach of confidentiality tort.[202] Whether the data will ever be misused is not dispositive; the point is that the consumer must now worry that their data is no longer safe—the trust they had in the security of their personal information is broken, and their data is potentially available to the public or even to malicious actors.

One possible explanation for this inconsistency of harm recognition is simply the potential for a significant influx in data breach litigation if the injury-in-fact requirement was lessened. This is certainly a colorable argument, but the counterargument is that data breach litigation vindicates the rights of consumers. Additionally, by vindicating the rights of consumers, plaintiff class action lawsuits against offending companies acts as a deterrent against other companies giving short shrift to their data security budgets. Furthermore, it provides additional incentive for companies to invest in cyber insurance[203]—and those insurance plans would likely require companies to implement minimum security standards.[204]

Still, limiting these class action lawsuits may be the policy goal of lawmakers, but it is just that—a policy goal.[205] As Justice Thomas noted in his *Spokeo* concurrence, "These [standing] limitations preserve separation of powers by preventing the judiciary's entanglement in disputes that are *primarily political* in nature."[206] In other words, part of the point of standing is to make sure judges decide cases, and elected representatives decide policy.[207] But when courts use standing analysis as a way of deciding policy questions, they are violating the fundamental purpose of standing itself—the separation of powers. Furthermore, data breach litigation does not inherently impinge on any separation of powers concern. Unlike the *Clapper* plaintiffs,[208] data breach plaintiffs are not asking federal courts to review any action of another branch of government. Thus, the only separation of powers concern in data breach litigation is the need to avoid undue policymaking.

---

202. *See supra* notes 145–47 and accompanying text.

203. *See supra* note 38 and accompanying text.

204. *See supra* note 39 and accompanying text.

205. Still, courts have a history of letting these sort of policy goals influence their decisions. *See* Prosser, *supra* note 49, at 385 (discussing *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538 (1902), in which the court declined to find a right to privacy in part because of the potential for an explosion of litigation).

206. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1551 (2016) (emphasis added).

207. Gill v. Whitford, 138 S. Ct. 1916, 1923 (2018) ("That threshold requirement 'ensures that we act *as judges*, and do not engage in policymaking properly left to elected representatives.'" (quoting Hollingsworth v. Perry, 570 U.S. 693, 700 (2013)) (emphasis in original)); Hickman, *supra* note 57, at 49 ("Standing doctrine also prevents the judiciary from intruding too deeply into matters of policy better left to the states or the political branches of the federal government.").

208. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).

Congress has considered an omnibus privacy law and could consider a national data breach law.[209] These laws could, if Congress deems it necessary, preempt state law in the data breach context.[210] Furthermore, that law could remove plaintiffs' private right of action, which would be even more true if the federal law expressly preempts state common law causes of action. But preempting state law is the proper domain of Congress. Such policymaking has no proper home in the judiciary.

Some may question whether deference to state law in these instances is even constitutionally permissible. But justiciability requirements are largely judicially created common-law rules made in an effort to promote the values at the core of our Constitution. The text of Article III does not itself require the rigidity that has developed in modern standing law.[211] Just as the Supreme Court has developed these laws to promote our core constitutional values, the Court is soundly within its power to modify the concreteness analysis to further promote these same values.

CONCLUSION

Regardless of whether the state determines that intangible harms should be recognized, the Supreme Court should follow the rationale in *Erie* and defer to state determinations of what constitutes harm under their own common and statutory law. While the federal courts must continue to apply the *Lujan* three-prong test, they should also recognize that the determination of whether a harm is concrete is naturally wrapped up in the substantive law. Thus, the underlying rationale of *Erie*, and the core principle of federalism, should apply. The individual states have a sovereign right to define the legal protections they afford their citizens. If a state sets out to protect dignitary harms in data breach litigation—or any other context—federal standing law should be no bar to suit when the court hears a case on diversity jurisdiction.

---

209. STEPHEN P. MULLIGAN, WILSON C. FREEMAN, & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 39, n.373 (2019) ("These developments have all combined to put the issue of consumer data privacy squarely *on* Congress' doorstep. The question is no longer whether we need a federal law to protect consumers' privacy. The question is what shape that law should take." (quoting *Examining Safeguards for Consumer Data Privacy Before the S. Comm. on Commerce, Science, & Transp.*, 115th Cong. (2018) (statement of Sen. John Thune)) (emphasis added)).

210. *Id.* at 62 ("Further, given that the states are likely to continue to experiment with legislation, the CCPA being a prime example, it is likely that preemption will be a highly significant issue in the debate over future federal privacy legislation.").

211. Hessick, *supra* note 150, at 104.