Journal of Business & Technology Law

Volume 17 | Issue 2 Article 7

Article III Standing: Getting Over "Mount Everest" in Modern Data Breach Litigation

Ahmed Eissa

Article III Standing: Getting Over "Mount Everest" in Modern Data Breach Litigation

AHMED EISSA*©**

The enormity of the data breach problem needs no qualification. Although data breaches affect millions of Americans, they are largely left without legal recourse because the law has failed to recognize a legally cognizable harm for data breach victims whose compromised information has not yet been put to misuse. Courts have erroneously relied on the Supreme Court's landmark decision regarding Article III standing in *Clapper v. Amnesty International USA* to dismiss civil data breach lawsuits brought by consumer-victims for lack of standing. In doing so, courts broadcast their fundamental misunderstanding of the nature of data breaches and their associated predictable harms. Ultimately, this Comment will show that the resulting harm from data breaches is not prohibitively speculative and that a correct reading of *Clapper* should not prevent standing in data breach litigation. Moreover, this Comment relies on an original data set of state data breach notification statutes and notices sent in compliance with those laws to show that states, breached organizations, and affected victims all objectively recognize the injury that courts struggle to acknowledge.

While writing this Article, I received letters for multiple data breaches notifying me that I was impacted by a data breach.[1] Because the companies – each an ostensible digital custodian of my personal information – "take data security very seriously," they wrote to "inform [me] of an incident involving [my] information."[2] As a Maryland resident, receiving this notice was significant; Maryland's data

* J.D. Candidate 2022, University of Maryland Francis King Carey School of Law. The author would like to thank the Journal of Business & Technology Law and its student editors for providing a forum for publishing student research. The author would also like to thank Professors Mark Graber and April Doss for their expert guidance on constitutional law and data privacy law. Finally, the author would like to thank his fiancée Rachel Cohen for her unyielding support and encouragement throughout the last four years of full-time work and evening law classes.

** This Comment reflects current events, the state of the law, and pending litigation as of December 2020.

1. One such data breach notice I received was from Wegmans, a privately held supermarket chain. E-mail from Wegmans Food Markets, Inc., to Ahmed Eissa (June 22, 2021, 12:35 PM) (on file with author).

2. *Id.*

breach statute, like dozens of other state data breach statutes, only compels notification when the breached entity conducts an investigation[3] and finds actual misuse of the exposed data, or a heightened likelihood that the leaked personal information will be misused.[4] Despite the hefty legalese and abundant reassurances littered throughout the five-page data breach notification letter, there was one major takeaway: I am at risk.

This is the new reality for myself and millions of other Americans.[5] But collectively, we have minimal legal recourse available because of *standing*[6] – a judicial doctrine developed in service of Article III of the United States Constitution[7] with an ostensible purpose of limiting the reach of federal courts and respecting the bedrock principle of separation of powers.[8] Today, this hallowed Constitutional principle stands as a momentous barrier to data breach victims pursuing redress in court, with most cases being dismissed before trial.[9] Indeed, the typical result in a data breach lawsuit is rather bleak: an organization (usually private and for-profit) is hacked and suffers nominal consequences;[10] external, malicious attackers are able to harvest and exploit sensitive personal information; and the individual victims are left with nothing but free credit monitoring and the perpetual threat of identity theft.[11] Since the pace of data breach litigation filings show no signs of abating,[12] it is important to develop a more uniform jurisprudence on Article III

3. Breached entities must conduct "a reasonable and prompt investigation to determine the likelihood that personal information . . . has been or will be misused as a result of the breach." MD. CODE ANN., COM. LAW § 14-3504(b)(1).

4. Notification to affected individuals is required if and when the breached entity "determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused . . . ." MD. CODE ANN., COM. LAW § 14-3504(b)(1)(2). See *infra* Part V.C. for a discussion on other similar state statutes.

5. *See infra* Part IV.C.

6. *Infra* Part III.A.

7. U.S. CONST. art. III.

8. *See* Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 881 (1983) (stating that the judicial doctrine of standing is a crucial and inseparable element of the principle of separation of powers).

9. "Most of these cases have failed at the pleading stage." David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 937 (2016).

10. For example, the health insurance provider Anthem, Inc. was fined $39.5 million by the Illinois Attorney General in a settlement stemming from Anthem's massive data breach in 2014 which impacted the personal information of more than 78 million Americans. *Attorney General Raoul Announces $39.5 Million Settlement with Anthem Over 2014 Data Breach*, ILL. ATT'Y GEN., https://illinoisattorneygeneral.gov/pressroom/2020_09/20200930.html (last visited Aug. 16, 2021). The fine constitutes approximately 0.04% of Anthem's 2019 total revenue. *Id.*

11. *See, e.g.*, *Submitted Breach Notification Sample*, CAL. ATT'Y GEN., https://oag.ca.gov/ecrime/databreach/reports/sb24-101693 (last visited Sept. 19, 2021) (select "Equifax notice only.pdf" which illustrates how organizations offer credit monitoring as a remedy to data breach victims).

12. David W. Opderbeck, *Current Developments in Data Breach Litigation: Article III*

standing in data breach litigation so that courts can deal with more substantive issues, like class certification[13] and eventually, the actual merits of claims. After all, pleading an injury sufficient to achieve standing should not be "Mount Everest."[14] The first step towards justice for victim-consumers in the data breach context should be a recognition of the objective circumstances that satisfy all of the Supreme Court's tests for Article III standing.[15]

Part I of this Comment discusses data breaches generally, highlighting the evolution of data breaches, their role in society, and prevailing cultural norms.[16] Part II of this Comment provides an overview of the modern standing doctrine developed by the Supreme Court, with a particular emphasis on the various espoused rationales and justifications that have impacted, or may impact, data breach litigation.[17] Part III focuses on application of the modern standing doctrine in the context of data breach litigation and highlights prominent federal appellate interpretations of the Supreme Court's standing precedent in this domain.[18] Part IV reviews the scholarship and leading theories on measuring data breach harms, distinguishes data breach litigation from the seminal standing cases, and ultimately proposes a new framework for obtaining standing in data breach litigation.[19] Part V addresses anticipated criticisms of the proposed way forward and argues that this Comment's proposal is consistent with evolving jurisprudence on data-centric issues and is checked by other procedural safeguards.[20] Part VI concludes.[21]

I. BACKGROUND: DATA BREACHES

A data breach occurs when sensitive, protected, or confidential information is copied, transmitted, viewed, stolen, or used by an individual who is unauthorized

Standing After Clapper, 67 S.C. L. REV. 599, 606 (2016) (showing that a docket search limited to December 2015 through February 2016 revealed putative consumer class actions filed in federal courts around the U.S. arising from data breaches involving the financial credit reporting company Experian, the online stock broker Scottrade, the adult dating site Ashley Madison, Hyatt Hotels, the makeup retailer Lime Crime, the restaurant chain Wendy's, and the web-hosting company Web.com.).

13. *See* Davis S. Almeida & Mark S. Eisen, *Barbarians at the Gate: Seventh Circuit Finds Article II Standing for Data Breach Class Actions*, NAT'L L. REV. (July 24, 2015), https://www.natlawreview.com/article/barbarians-gate-seventh-circuit-finds-article-iii-standing-data-breach-class-actions.

14. When Justice Alito was a judge on the Court of Appeals for the Third Circuit, he endorsed the view that to survive a motion to dismiss, it was sufficient for a plaintiff to "allege . . . some specific, 'identifiable' trifle of injury." Danvers Motor Co., Inc. v. Ford Motor Co., 432 F.3d 286, 294 (3d Cir. 2005).

15. *See infra* Part IV.

16. *See infra* Part I.

17. *See infra* Part II.

18. *See infra* Part III.

19. *See infra* Part IV.

20. *See infra* Part V.

21. *See infra* Part VI.

to do so.[22] Exposed data may include personally identifiable information ("PII"),[23] credit card numbers, personal health information, customer data and company trade secrets, and more.[24] The enormity of the data breach problem needs no qualification.[25] Yet despite the prevalence of data breaches, several communities – including cybersecurity practitioners, scholars, lawyers, and others – are still endeavoring to understand the phenomenon.[26] Who is most affected? What are the direct and indirect costs? How can society better address this intricate issue? Discussion on this topic necessarily rests on first understanding the scope of the modern data breach problem.[27]

Currently, there is no single, authoritative source or method for tracking, verifying, and studying data breaches, though several approaches have emerged.[28] There are several industry-standard reports, including Verizon's *Data Breach Investigations Report*[29] and the Ponemon Institute's *Cost of a Data Breach Report*,[30] which conduct a broad survey of data breaches and associated costs, and ultimately provide comprehensive analyses of the collected incidents. There are also academic and non-profit repositories of data breach information, such as the collections hosted by *Data Breach Archives*[31] and *Privacy Rights Clearinghouse*,[32] who engage in tracking, compiling, and normalizing data breach information provided by state governments. Finally, there is a wide array of collection and analysis performed by

22. *Cybersecurity Basics – Glossary*, NAT'L INSTS. OF STANDARDS AND TECH., https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary (last visited Aug. 16, 2021).

23. There are several definitions of PII across state and federal governments. *See infra* Part IV.C.

24. *Cybersecurity Basics – Glossary*, *supra* note 22.

25. Regardless, this section reviews recent quantitative research that summarizes the frequency, scope, and severity of data breaches. *See, e.g.*, *infra* notes 29-35 and accompanying text.

26. *See infra* notes 28-33.

27. *See infra* Part V.

28. *See* Ed Felten, *Enhancing the Security of Data Breach Notifications and Settlement Notices*, FREEDOM TO TINKER (Nov. 8, 2019), https://freedom-to-tinker.com/2019/11/08/enhancing-the-security-of-data-breach-notifications-and-settlement-notices/ ("At a high level, we recommend the creation of a centralized database of settlements and breaches, so that users have a way to verify the notices distributed.").

29. Verizon's *Data Breach Investigations Report* is in its 13th year. *2020 Data Breach Investigations Report*, VERIZON, https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf (last visited Aug. 16, 2021).

30. The Ponemon Institute's *Cost of a Data Breach Report*, which is sponsored and published by IBM, is in its 15th year. Ponemon Institute, *Cost of a Data Breach Report (2020)*, IBM, https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542 (select "Download the report" after completing the form) (last visited Aug. 16, 2021).

31. DATA BREACH ARCHIVES, https://databreacharchives.com/ (last visited Aug. 16, 2021). The Data Breach Archives project and its dataset was created by the author of this Comment prior to drafting of this Comment and is heavily relied on in the subsequent analysis. *See infra* Part V.C.

32. *Data Breaches*, PRIV. RTS. CLEARINGHOUSE, https://privacyrights.org/data-breaches (last visited Aug. 16, 2021).

independent security researchers,[33] security and threat intelligence companies,[34] and even malicious threat actors who aggregate data breaches solely to resell the information.[35]

The 2020 release of the *Data Breach Investigations Report* ("DBIR") paints a bleak picture of recent trends.[36] After analyzing over 157,000 security incidents which occurred since the last iteration of the report, over 32,000 met Verizon's quality standards, resulting in 3,950 officially categorized as data breaches.[37] Over 70% of the identified data breaches were perpetrated by external actors, and 45% of the incidents involved malicious hacking (rather than misuse by authorized users or physical actions, for example).[38] Moreover, these breaches affect large and small businesses alike, with larger businesses comprising 72% of the breaches and small businesses comprising the remainder.[39] Across all breached entities, the DBIR found that 58% of victims had personal information compromised in the leaked data.[40] In addition, almost all data breaches were financially motivated.[41]

Looking beyond the initial event, the aftermath of a data breach can generally be broken down into effects on: (1) organizations and businesses (i.e., entities that store data); and (2) individuals and consumers (i.e., the people who provided the data or who the data is about).[42] There is abundant research about the former, but not the latter.[43] The Ponemon Institute's *Cost of a Data Breach Report* ("CDBR") is one such body of work that provides transparency into the breached entities.[44] The 2020 release of the CDBR reviewed over 500 breached organizations in over a dozen

33. *Pwned Websites*, HAVE I BEEN PWNED, https://haveibeenpwned.com/PwnedWebsites (last visited Aug. 16, 2021).

34. Brett Heidenreich, Cory Kujawski & Marcelle Lee, *Compromised Credentials Are Still Your Organization's Worst Nightmare*, LOOKINGGLASS (Apr. 16, 2018), https://www.lookingglasscyber.com/blog/rsa-preview-compromised-credentials-are-still-your-organizations-worst-nightmare/.

35. Catalin Cimpanu, *FBI Seizes WeLeakInfo, a Website that Sold Access to Breached Data*, ZDNET (Jan. 17, 2020, 9:13 AM), https://www.zdnet.com/article/fbi-seizes-weleakinfo-a-website-that-sold-access-breached-data/.

36. *2020 Data Breach Investigations Report*, *supra* note 29, at 6.

37. *Id.* at 7.

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.*

42. For example, when a computer or other electronic device is stolen or lost and contains personally identifiable information – one of the most common fact patterns in data breach litigation – the organization is affected by the loss of the resource, and individuals are affected by the exposure of sensitive information. Paul G. Karlsgodt, *Key Issues in Consumer Data Breach Litigation*, PRAC. L. J. 50 (October 2014), https://www.bakerlaw.com/files/uploads/News/Articles/LITIGATION/2014/Karlsgodt-Lit_OctNov14_DataBreachFeature.pdf ("A stolen or lost computer . . . containing PII is one of the most common fact patterns underlying data breach litigation.").

43. *See generally supra* notes 29-35 and accompanying text.

44. *See supra* note 30.

industries and found the average cost of a data breach to be $3.86 million.[45] Eighty percent of the affected organizations said the customers' personal information was compromised during the breach, which is valued at approximately $150 per record.[46] Furthermore, companies that experience so-called "mega breaches"[47] incur astronomically higher costs; breaches that expose between one and ten million cost an average of $50 million and breaches that expose more than fifty million records cost $392 million on average.[48]

Although prevailing research on data breaches does not provide extensive coverage of the long-lasting effects to individuals and consumers, some general trends are still discernable. Data breaches can result in significant financial harm to individuals.[49] One of the most common forms of financial harm is fraudulent tax filings, which has resulted in the Internal Revenue Service ("IRS") paying out billions in fraudulent tax returns.[50] There are indirect costs, too; the IRS has stated that the proliferation of PII made widely available from data breaches makes it fundamentally more difficult to authenticate an individual.[51] In addition, fraudsters regularly use stolen and leaked information from data breaches to apply for credit cards and bank loans, or to make Social Security, medical, and unemployment claims.[52] There are several other less-obvious forms of financial harm as well. For example, threat actors who harvest information from large data breaches can engage in *credential stuffing*[53] against a wide variety of websites with online

45. *See* Ponemon Institute, *supra* note 30, at 10. When classified by size, the average cost is $5.52 million for organizations with more than 25,000 employees and $2.64 million for organizations with under 500 employees. *Id.* at 14.

46. *Id.* at 8.

47. A breach that exposes more than one million records. *Id.* at 66.

48. *Id.* at 10.

49. *See infra* notes 50-54.

50. U.S. GOV'T ACCOUNTABILITY OFF., GAO-18-702T, IDENTITY THEFT: STRENGTHENING TAXPAYER AUTHENTICATION EFFORTS COULD HELP PROTECT IRS AGAINST FRAUDSTERS 1 (2018), https://www.gao.gov/assets/700/694737.pdf (showing that in 2016 alone, the IRS received over $12 billion in fraudulent tax return filings and paid out at least $1.6 billion of those claims).

51. Jory Heckman, *IRS: Frequent Data Breaches Make It "Fundamentally More Difficult" to Verify Taxpayers*, FED. NEWS NETWORK (Sept. 27, 2018, 7:43 AM), https://federalnewsnetwork.com/cybersecurity/2018/09/irs-frequent-data-breaches-make-it-fundamentally-more-difficult-to-verify-taxpayers/ (quoting congressional testimony given by Edward Killen, the IRS' chief privacy officer, to the House Ways and Means Committee).

52. *How Do Criminals Use Stolen Data?*, FORBES (Sept. 11, 2019, 3:31 PM), https://www.forbes.com/sites/quora/2019/09/11/how-do-criminals-use-stolen-data/#4c55f6997551.

53. Credential stuffing is the automated attempt to use a pair of compromised account credentials in order to gain fraudulent access to another's account. Neal Mueller, *Credential Stuffing*, OWASP, https://owasp.org/www-community/attacks/Credential_stuffing (last visited Aug. 16, 2021).

shopping carts in order to hijack payment details or make anonymous purchases through the compromised account.[54]

Data breaches have the potential to expose more than just a victim's email address and password – they can end relationships and careers.[55] For example, when Ashley Madison, an online dating website for extramarital affairs and discreet married dating, suffered a massive data breach in 2015,[56] the affected individuals frantically searched for answers from individuals who obtained the data. Some of the post-data breach messages included "I am hoping to find out how much of my data is exposed and to prepare for the worst" and "I just found out my husband's [Ashley Madison] account is part of the hack. I want to know what information he put on the site."[57]

The devasting uses for sensitive information obtained from data breaches are endless, including blackmail and spamming,[58] and espionage,[59] for example. But despite the obvious magnitude of this problem, individual victims are largely left without legal recourse unless and until a court finds standing, which has traditionally proved to be overly burdensome.[60] The following section of this Comment explores the constitutional foundation of the standing doctrine and the array of Supreme Court cases which have developed the doctrine to its current form.[61]

54. *Why Do Hackers Want Your Personal Information?*, F-SECURE, https://www.f-secure.com/us-en/home/articles/why-do-hackers-want-your-personal-information (last visited Aug. 16, 2021) (explaining how login details are needed for account takeover).

55. Jose Pagliery, *The Ashley Madison Hack Ruined My Life*, CNN BUS. (Aug. 21, 2015, 5:41 PM), https://money.cnn.com/2015/08/21/technology/ashley-madison-ruined-lives/index.html; Mary Emily O'Hara, *Ex-State Employee Named in Ashley Madison Hack Says He Was Unfairly Fired*, DAILY DOT (Feb. 29, 2020, 12:51 AM), https://www.dailydot.com/irl/new-mexico-ashley-madison-fired-employee/.

56. The Ashley Madison data breach exposed dates of birth, email addresses, ethnicities, genders, names, passwords, payment histories, phone numbers, physical addresses, security questions and answers sexual orientations, usernames, and website activity for over thirty million accounts. *Ashley Madison*, HAVE I BEEN PWNED, https://haveibeenpwned.com/PwnedWebsites#AshleyMadison (last visited Aug. 16, 2021).

57. Troy Hunt, *Here's What Ashley Madison Members Have Told Me*, TROY HUNT (Aug. 24, 2015), https://www.troyhunt.com/heres-what-ashley-madison-members-have/.

58. *What Do Cybercriminals Do With the Data They Steal?*, SYSNET, https://sysnetgs.com/2018/06/what-do-cybercriminals-do-with-the-data-they-steal/ (last visited Aug. 16, 2021).

59. *2020 Data Breach Investigations Report*, *supra* note 29.

60. *See supra* note 9 and accompanying text.

61. *See infra* Part II.

II. THE MODERN STANDING DOCTRINE

A. Constitutional Background

The United States Constitution limits the power of the federal judiciary to "cases" and "controversies."[62] The doctrine of "standing" gives meaning to the limits set forth in Article III of the Constitution by identifying disputes which are most appropriately resolved through the judicial process.[63] The Supreme Court has recognized this bedrock principle to be "an essential and unchanging part of the case-or-controversy requirement of Article III."[64]

Various rationales for the standing doctrine have been espoused by courts and legal scholars.[65] One of the chief rationales is the principle of separation-of-powers.[66] This theory holds that limiting the court's power to "cases" and "controversies" is, in fact, a defining feature of the federal judiciary because it delineates what is appropriately within the judiciary's province.[67] The separation-of-powers explanation also holds that the standing doctrine effectively prevents the judicial process from being used to usurp the powers of the legislative and executive branches,[68] which would be an impermissible expansion of judicial power.[69]

Another prominent explanation for the standing requirement is to ensure and preserve the adversarial process which characterizes the American legal system.[70] The adversarial process assures that the litigating parties "have an actual, as opposed to professed, stake in the outcome" and that a resolution will occur "in a concrete factual context conducive to a realistic appreciation of the consequences of judicial action."[71]

B. Seminal Cases

Despite the widespread agreement on the various rationales for the standing doctrine, application of the standing doctrine has not enjoyed similar accord.[72] As this Comment will show, and as the Supreme Court and other courts have

62. *See* U.S. CONST. art. III, § 2, cl. 1.

63. Susan B. Anthony List v. Driehaus, 573 U.S. 149, 157 (2014).

64. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

65. *See* Martin H. Redish & Sopan Joshi, *Litigating Article III Standing: A Proposed Solution to the Serious (But Unrecognized) Separation of Powers Problem*, 162 UNIV. PA. L. REV. 1373, 1375 (2014) (providing a broad overview of the reasons for the standing doctrine).

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

67. *Lujan*, 504 U.S. at 559-60.

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

69. *See id.* at 409.

70. *Lujan*, 504 U.S. at 581 (Kennedy, J., concurring).

71. *Id.*

72. See *supra* Part II.A.

recognized, the disparate treatment and application of standing stems from the imprecise boundaries of the "case or controversy" requirement, which are "not discernible by any precise test."[73]

Standing is one of the first major substantive hurdles in federal litigation; if a plaintiff cannot establish standing, then a plaintiff's lawsuit cannot proceed in federal court.[74] The Supreme Court has refined modern standing doctrine in recent years through several cases.[75] The three elements of standing were most clearly aggregated and pronounced by the Court in *Lujan v. Defenders of Wildlife* after the Court reviewed its precedent cases to discern the "irreducible constitutional minimum" that a workable standing doctrine needs to comply with Article III.[76] The Court held that first, a plaintiff must have suffered an "injury in fact . . . which is (a) concrete and particularized . . . and (b) actual or imminent, not conjectural or hypothetical."[77] Second, standing requires a causal connection between the injury and the conduct complained of.[78] Third, the standing doctrine compels that the injury or harm at issue is likely to be redressed by a favorable court decision.[79] Finally, the party invoking federal jurisdiction bears the burden of establishing the three elements of the standing requirement.[80]

After its pronouncement of the irreducible constitutional minimum of standing, much of the Court's analysis in *Lujan* focused on the first necessary element – the injury-in-fact requirement.[81] Explaining that standing is not "an ingenious academic exercise in the conceivable,"[82] the first element requires a "factual showing of perceptible harm."[83] In addition, an injury is not actual or imminent when it only

73. *Clapper*, 568 U.S. at 423 (Breyer, J., dissenting) (citing Babbitt v. Farm Workers, 442 U.S. 289, 297 (1979)).

74. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (explaining that when a case is at the pleading stage, the plaintiff must clearly allege facts demonstrating each element of standing).

75. *See infra* Part II.B.

76. 504 U.S. at 560. In *Lujan*, respondent-plaintiffs sought a declaratory judgment that a new rule promulgated by the Department of the Interior, which was made in interpretation of the Endangered Species Act of 1973, 16 U.S.C. § 1536, was in error, and further sought an injunction requiring the Secretary of the Interior to promulgate a new regulation restoring the department's initial interpretation. *Id.* at 558-59.

77. *Id.* at 560 (internal quotations omitted).

78. *Id.* (explaining that the injury has to be fairly traceable to the challenged action of the defendant, rather than a third party, independent actor).

79. *Id.* at 561.

80. *Id.*

81. The dispute in *Lujan* centered on alleged future environmental damages as a result of an Interior Department rule. *Id.* at 558-59. Respondent-plaintiffs advanced three theories of harm – so-called "ecosystem nexus," "animal nexus," and "vocational nexus" – which were all dismissed by the Court under the injury-in-fact requirement for being too speculative and insufficiently concrete. *Id.* at 565-67.

82. *Id*. at 566 (citing United States v. Students Challenging Regul. Agency Procs., 412 U.S. 669, 688 (1973)).

83. *Id.* The Court noted that such a showing was required at the summary judgment stage, which was central to the litigation in *Lujan*. *See id.* at 559. In practice, standing is commonly challenged pursuant to Rule

consists of alleged "'some day' intentions" that lack a description of concrete plans.[84]

The next significant development in the standing doctrine came in *Clapper v. Amnesty Int'l USA*, in which the Supreme Court heard a challenge to § 1881a of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 by a collection of attorneys and human rights, labor, legal, and media organizations.[85] Like *Lujan* and other standing cases, the principal focus in *Clapper* was whether the respondent-plaintiffs could satisfy the injury-in-fact element of standing under the actual or imminent requirement.[86] Although the Court conceded that imminence is a "somewhat elastic concept," it stressed that the alleged injury must be "*certainly* impending"[87] and in turn rejected the Second Circuit's "objectively reasonable likelihood" standard.[88] Therefore, "[a]llegations of *possible* future injury" are not sufficient to establish Article III standing.[89] The Court did not define the exact contours of its "certainly impending" requirement, but instead labeled respondent-plaintiffs' proffered theory of harm as a "highly attenuated chain of possibilities" which illustrated an injury that did *not* meet the certainly impending standard.[90] That chain of possibilities was specific to the facts in *Clapper* but nonetheless warrants a thorough review because it was the Court's chosen manner of elucidating the Second Circuit's error:

> *Furthermore, respondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the [Foreign Intelligence Surveillance Court] will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of*

12(b)(6) and Rule 56 of the Federal Rules of Civil Procedure; however, courts often fail to determine conclusively whether the plaintiff has Article III standing until the trial stage. Redish & Joshi, *supra* note 65, at 1377.

84. *Lujan*, 504 U.S. at 564.

85. 568 U.S. 398, 406 (2012).

86. *Id.* at 401.

87. *Id.* at 409.

88. *Id.* at 410 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)). In *Amnesty Int'l USA v. Clapper*, the Second Circuit rejected the government's argument that plaintiffs could only obtain standing by showing they had been monitored under the disputed surveillance program or that it was "effectively certain" that they would be monitored. 638 F.3d 118, 135 (2d Cir. 2011). The court instead found that the totality of the circumstances created an objectively reasonably likelihood that the plaintiff's communications will be surveilled, and their fears are not mere conjecture of speculation. *Id*. at 139.

89. *Clapper*, 568 U.S. at 409 (quoting *Whitmore*, 95 U.S. at 158).

90. *Id* at 410.

> *respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.*[91]

What *Clapper* did not clarify, however, is what would have conferred standing in those circumstances, or rather, the minimum number of contingencies that respondent-plaintiffs needed to resolve or prove in order to establishing an imminent injury-in-fact.[92]

Finally, at the conclusion of the Court's analysis on future harm, it left a footnote which has been called – and subsequently interpreted as – "an alternative holding."[93] The Court reflected that its precedent does "not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about" and that in some instances, the Court has "found standing based on a 'substantial risk' that the harm will occur . . . ."[94] The footnote introduced confusion as to which standard the Court was declaring to be controlling law for Article III standing.[95] This seeming discrepancy was highlighted by the dissent, which provided a detailed list of cases[96] in which the Court found standing "where the occurrence of the relevant injury was far *less* certain than here."[97] In the dissent's view, the "certainly impending" standard does not and should not require absolute certainty, and both the Constitution and the Court's case law instead require something more comparable to "reasonable probability" or "high probability."[98]

In the term immediately following the Court's decision in *Clapper*, it adjudicated the issue of Article III standing once again in *Susan B. Anthony List v. Driehaus*, which also centered on the injury-in-fact requirement.[99] Justice Thomas, writing for the

91. *Id.*

92. *See id.* at 414 (concluding that "respondents' speculative chain of possibilities does not establish that injury based on potential future [harm] is certainly impending . . ." without opining or suggesting the circumstances that would achieve that threshold).

93. *See* Marty Lederman, *Commentary:* Susan B. Anthony List, Clapper *Footnote 5, and the State of Article III Standing Doctrine*, SCOTUSBLOG (June 17, 2014, 4:34 PM), https://www.scotusblog.com/2014/06/commentary-susan-b-anthony-list-clapper-footnote-5-and-the-state-of-article-iii-standing-doctrine/.

94. *Clapper*, 568 U.S. at 414 n.5 (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153 (2010)). The Court further argued that "to the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement," that respondents did not meet the former standard. *Id.* (internal citation omitted).

95. *See* Lederman, *supra* note 93 (explaining that those who closely followed Article III legal developments were unsure if the traditional "substantial risk" standard remained the law, or if the more onerous "certainly impending" standard supplanted the old rule).

96. *Clapper*, 568 U.S. at 433-37 (Breyer, J., dissenting).

97. *Id.* at 433.

98. *Id.* at 439-41.

99. 573 U.S. 149, 158 (2014) (stating that "[t]his case concerns the injury-in-fact requirement, which helps to ensure that the plaintiff has a 'personal stake in the outcome of the controversy.'").

majority, expressed the relevant standard for evaluating a claim of future injury: "[a]n allegation of future injury *may* suffice if the threatened injury is 'certainly impending,' *or* there is a 'substantial risk' that the harm will occur."[100] The Court's use of "may" and "or" is notable, as the expounded rule would allow for the "substantial risk" standard that was ostensibly rejected in *Clapper*.[101] In addition, the expressed standard was permissive, which allows either test to suffice for Article III standing, but does not necessitate that result.[102] Despite any uncertainties that the Court's language might have introduced, its subsequent analysis in *Susan B. Anthony* employed the substantial risk test, and not the certainly impending test from *Clapper*.[103] The Court concluded by limiting its holding to the specific facts of the case, which generated additional unpredictability regarding the applicability of the substantial risk and certainly impending tests.[104]

The most recent development in the Court's Article III standing jurisprudence came in *Spokeo v. Robins*, which was principally concerned with the "concrete and particularized" requirement of the injury-in-fact element.[105] The Court reaffirmed that the alleged injury needs to be both concrete *and* particularized – one of those characteristics alone will not suffice.[106] Concreteness requires that the injury "actually exist" – it cannot be abstract[107] while particularity necessitates that the injury "affect the plaintiff in a personal and individual way."[108] The Court's clarification of the requirements of the injury-in-fact element is noteworthy because its precedent cases had commonly coupled the terms "concrete and particularized" without explicitly differentiating them.[109]

100. *Id.* (emphasis added and internal quotation marks omitted).

101. *Clapper*, 568 U.S. at 410. The Court rejected "the Second Circuit's 'objectively reasonable likelihood' standard" and subsequently referred to that standard throughout *Clapper* as standing based on "substantial risk." *Id.*

102. *See* Lederman, *supra* note 93 (arguing that there is some ambiguity as to whether the Court is "actually holding that a showing of 'substantial harm' is sufficient" for Article III standing).

103. *See id.* (noting that after the Court stated the standard for evaluating a future harm, it "does not mention the 'certainly impending' test at all" for the remainder of the opinion).

104. *Susan B. Anthony List*, 573 U.S. at 166 (concluding that there was an "Article III injury under the circumstances of this case").

105. 136 S. Ct. 1540, 1547-48 (2016). In *Spokeo*, respondent-plaintiff brought an action against Spokeo alleging that it published inaccurate information about him in violation of the Fair Credit Reporting Act. *Id.* at 1544-45. It was disputed whether respondent-plaintiff sufficiently alleged an injury-in-fact sufficient for Article III standing. *Id.*

106. *Id.* at 1545 (explaining that the Ninth Circuit's analysis erroneously focused on particularity while overlooking concreteness).

107. *Id.* The concrete requirement, however, does not prevent plaintiffs from alleging, and courts from recognizing, intangible injuries. *Id.* at 1549.

108. *Id.* at 1548.

109. *Id.* at 1555 (Ginsburg, J., dissenting) (stating that in the cases cited by the majority, "and many others, opinions do not discuss the separate offices of the terms 'concrete' and 'particularized'").

Overall, the Court's development of the standing doctrine in these cases has bred confusion and disagreement.[110] Its fact-specific inquiries in these cases have also failed to deliver a practical and cogent doctrine that can create equitable outcomes in various legal contexts.[111]

III. Litigating Data Breaches Against "Mount Everest"

A. Data Breach Litigation Before Clapper

Satisfying Article III standing has remained the central legal hurdle for plaintiffs in data breach litigation, and distinct patterns of case treatment have emerged.[112] To begin, many plaintiffs face courts which dismiss based on standing, finding that an increased risk of harm from a data breach is too speculative and uncertain to establish Article III standing.[113] However, employing a substantial risk standard, some courts have found the increased risk of identity theft and harm as sufficient injury for Article III standing.[114] Other courts have required a slightly greater showing of increased or substantial risk, holding that when at least one plaintiff was defrauded, then other victims of the same data breach have sufficient reason to fear imminent harm.[115] In another variant, courts have also found standing for data

110. *See, e.g.,* Daniel J. Solove & Danielle Citron*, Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 744 (2018) (arguing that *Spokeo* failed to clarify (1) the relationship between the concreteness of harm and the need for at least a substantial risk of harm as discussed in *Clapper*; (2) when an increased risk of injury constitutes a substantial risk of harm; and (3) why some intangible injuries are sufficient for standing while others are not).

111. *See id.* (arguing that *Clapper* and *Spokeo* have led to confusion about how harms involving personal data should be conceptualized); *see also infra* Part III.A (arguing that the data breach context is distinguished from the circumstances in the modern standing cases).

112. This section analyzes trends in data breach litigation generally, which include decisions in federal district courts and appellate courts issued both before and after the Supreme Court's decision in *Clapper.* See *infra* Part III.B for a focused discussion on appellate decisions trends after *Clapper*.

113. Loren F. Selznick & Carolyn LaMacchia have compiled and organized the various ways that courts have dealt with standing and increased risk of harm. One such group of cases includes courts that reject the theory of increased risk of harm as too speculative for Article III standing. Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?,* 13 J. BUS. & TECH. L. 217, 231 (2018) (citing Reilly v. Ceridian Corp., 664 F.3d 38, 44-46 (3d Cir. 2011); Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 753 (W.D.N.Y. 2017); Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 U.S. Dist. LEXIS 89992, at *10-22 (E.D. Mo. July 12, 2016); Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1283-84 (M.D. Fla. 2016); Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 531 (D. Md. 2016); Alonso v. Blue Sky Resorts, LLC, 179 F. Supp. 3d 857, 863-65 (S.D. Ind. 2016); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25-26 (D.D.C. 2014)).

114. *Id.* at 231 (citing Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142-43 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007)).

115. *Id.* at 231 (citing Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *17 (N.D. Ill. July 14, 2014)).

breach victims when fraudulent activity occurs in close proximity to a cyberattack or data leak, making the likelihood of harm appear imminent or impending.[116] Collectively, the varied jurisprudence in this domain shows that the central disagreement is whether plaintiffs, whose information was hacked, have standing when the data has not yet been put to dishonest use.[117]

B. Appellate Court Split After Clapper

The application of the standing doctrine in data breach litigation after *Clapper*, *Susan B. Anthony*, and *Spokeo* has been anything but uniform.[118] Although this Comment detailed those three cases as the core of the Supreme Court's modern standing doctrine, scholarship in this domain has largely focused on evaluating standing before and after *Clapper*. [119] Prior to *Clapper,* there was a circuit split on whether plaintiffs bringing data breach lawsuits could satisfy the Article III standing requirement.[120] The circuit split became more pronounced after *Clapper*, particularly regarding the first element of the standing doctrine – injury-in-fact – and its various requirements.[121] The Third, Sixth, Seventh, and D.C. Circuits have all found standing in data breach lawsuits when there was no actual injury.[122] The

116. Loren F. Selznick & Carolyn LaMacchia provide several examples of these cases in their research. First, in *Hapka v. CareCentrix*, "where the IRS notified the plaintiff that a fraudulent tax return was filed in her name[.]" *Id.* at 230 (citing Hapka v. CareCentrix, Inc., No. 16-2372, 2016 WL 7336407, at *1 (D. Kan. Dec. 19, 2016)). Second, in In re *Cmty Health Sys., Inc.*, "where some of the named plaintiffs alleged accompanying misuse of their data resulting from the data breach[.]" *Id.* (citing *In re* Cmty. Health Sys., Inc., No. 15-CV222-KOB, 2016 WL 4732630, at *9 (N.D. Ala. Sept. 12, 2016)). Third, in *Smith v. Triad of Ala., LLC*, "where at least 124 federal tax returns were fraudulent filed by the individual who illegally stole patient health records[.]" *Id.* (citing Smith v. Triad of Ala., LLC, No. 1:14-CV-324-WKW, 2017 WL 1044692, at *2 (M.D. Ala. Sept. 29, 2015)). And finally, in In re *Target Corp., Customer Data Sec. Breach Litig.*, "where 114 named plaintiffs alleged that they actually incurred unauthorized charges, lost access to their accounts, and/or were forced to pay sums such as late fees and card-replacement fees[.]" *Id.* (citing *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1158 (D. Minn. 2014)).

117. *Id.* (citing Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878 (N.D. Ill. 2014)).

118. Commentators noted that the standing doctrine still lacked clarity after *Spokeo*. Joseph J. Lazzarotti & Maya Atrakchi, *Standing in Data Breach Litigation: Will the U.S. Supreme Court Weigh In?*, JACKSONLEWIS (Feb. 12, 2019), https://www.workplaceprivacyreport.com/2019/02/articles/consumer-privacy/standing-in-data-breach-litigation-will-the-u-s-supreme-court-weigh-in/.

119. *See* Opderbeck, *supra* note 12, at 601 (stating that "[t]he standing analysis in recent data breach cases has focused on the requirements for Article III standing discussed in the Supreme Court's *Clapper v. Amnesty International* opinion.").

120. Opderbeck, *supra* note 9, at 942-43 (citing Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (finding that Article III standing was not satisfied); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding that Article III standing was satisfied); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (finding that Article III standing was satisfied)).

121. *See supra* Part III.B for a discussion on "actual or imminent" and "concrete and particular."

122. Daniel J. Solove and Paul M. Schwartz have compiled and organized the various ways that the Circuit Courts have dealt with standing in data breach cases. Daniel J. Solove & Paul M. Schwartz, Privacy Law

Ninth Circuit, which previously found increased risk of harm sufficient for standing,[123] upheld that decision in a recent case, which places the Ninth Circuit with the first group of appellate courts.[124] By contrast, the Second, Fifth, and Eighth Circuits have not found standing in that context.[125] There is also a third category – solely occupied by the Fourth Circuit – where standing in data breach litigation without actual injury was rejected in one instance and granted in another.[126] In addition, the First and Eleventh Circuits have not made post-*Clapper* rulings on the

Fundamentals 205-07 (5th ed. 2019). They point to four cases in which standing was found in a data breach case despite no actual injury. *Id.* First is *Attias v. Carefirst, Inc.,* which found "standing based on a heightened risk of identity theft when customers' sensitive information is stolen during the breach, 'plausibly' including social security and credit card numbers[.]" *Id.* (citing Attias v. Carefirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017)). Second is *In re Horizon Healthcare Services Inc. Data Breach Litigation*, which found "standing for improper disclosure of personal data because such disclosure in violation of the FRCA constitutes a cognizable injury[.]" *Id.* (citing *In re* Horizon Healthcare Services Inc. Data Breach Litigation, 846 F.3d 625, 640-41 (3rd Cir. 2017). Third is *Galaria v. Nationwide Mutual Insurance Co*., which found "standing based on increased risk of fraud and identity theft because when a data breach targets personal information, it is reasonable to infer that the hackers will use the victims' data for fraudulent purposes[.]" *Id.* (citing Galaria v. Nationwide Mutual Insurance Co., 663 F. App'x 384, 387 (6th Cir. 2017)). Lastly, is *Lewert v. P.F. Chang's China Bistro, Inc.*, which found "standing based on future risk of identity theft or fraud and on time and resources spent on credit monitoring[.]" *Id.* (citing Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016).

123. This occurred in *Krottner v. Starbucks Corp.*, which found "standing based on future risk of identity theft when plaintiff's personal information was stolen but not misused[.]" Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals 207 (5th ed. 2019) (citing Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).

124. *In re* Zappos.co, Inc., Customer Data Security Breach Litigation, 888 F.3d 1020, 1023 (9th Cir. 2018) (finding that *Krottner*, the court's 2010 decision on standing, was still "good law").

125. Daniel J. Solove's and Paul M. Schwartz's compilation also includes cases where standing was denied without an actual injury. Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals 205-07 (5th ed. 2019). They point to three cases in which standing was found in a data breach case despite no actual injury. First is *Whalen v. Michaels Stores, Inc.*, which found "no standing from the exposure of plaintiff's credit card information following a data breach because plaintiff neither alleged any actual charges on her credit card, nor, with any specificity, that she had spent time or money monitoring her credit[.]" *Id. (*citing Whalen v. Michaels Stores Inc., 689 F. App'x 89, 90 (2d Cir. 2017)). Second is *Peters v. St. Joseph Services Corp.*, which found "no standing based on future risk of identity theft or fraud because the risk of future harm following a hospital's data security breach was merely hypothetical[.]" *Id.* citing (Peters v. St. Joseph Services Corp., 74 F. Supp. 3d 847, 854 (S.D. Tex. 2015)). Third is *In re SuperValu, Inc.*, which concluded that "plaintiffs failed to sufficiently allege a substantial risk of identity theft to support standing, but finding standing for one plaintiff who alleged an actual present injury from fraudulent credit card charges[.]" *Id.* (citing *In re* SuperValu, Inc., 870 F.3d 763, 771-72 (8th Cir. 2017)).

126. SOLOVE & SCHWARTZ, *supra* note 122. *Compare* Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 621-22 (4th Cir. 2018) (finding standing based on an imminent threat of identity theft when hackers used and attempted to use plaintiffs' personal information to open credit card accounts, constituting a concrete injury), *with* Beck v. McDonald, 848 F.3d 262, 276-77 (4th Cir. 2017) (not finding standing because the plaintiff's allegations that 33% of those affected by the breach will become victims of identity theft was insufficient to establish a substantial risk of harm).

issue of standing in data breach litigation.[127] Finally, in addition to the apparent confusion created by the Supreme Court's precedent standing cases, the circuit split is also due to the fact-focused nature of the disputes that come before the federal appellate courts.[128]

After *Clapper*, the Seventh Circuit was the first federal appellate court to find Article III standing following a data breach in *Remijas v. Neiman Marcus Group, LLC*.[129] This case warrants a close review given its thorough analysis of standing in the data breach context[130] and its role as a *first mover*.[131] Neiman Marcus, a luxury department store, suffered a cyberattack by unknown hackers, resulting in the theft of its customers' credit card numbers.[132] Neiman Marcus learned that some of its customers experienced fraudulent charges on their credit cards and subsequently announced the security breach to the public.[133] As more customers reported fraudulent activity, class action litigation followed, where the plaintiffs introduced several theories for relief, including negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws.[134] Specifically, the affected plaintiffs alleged injury regarding:

> *1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to*

127. These cases are also summarized by Daniel J. Solove's and Paul M. Schwartz's compilation. Daniel J. Solove & Paul M. Schwartz, Privacy Law Fundamentals 205-07 (5th ed. 2019). The First Circuit denied standing in this context before *Clapper* in *Katz v. Pershing*, which found "no standing when the plaintiff failed to show that the breach resulted in an identifiable breach to her own personal security[.]" *Id.* citing (Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012)). The Eleventh Circuit found standing in a data breach lawsuit before *Clapper* in *Resnick v. AvMed, Inc.*. which found "standing when unencrypted laptops containing health care plan members' sensitive information were stolen because the members' identity thefts were fairly traceable to the plan operator's failure to protect the stolen information[.]" *Id.* (citing Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012)).

128. In the case of *In re* SuperValu, Inc., the Eighth Circuit considered the circuit split and noted that the "cases came to differing conclusions on the questions of standing . . . because the cases ultimately turned on the substance of the allegations before each court." *SuperValu, Inc.*, 870 F.3d at 769.

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

130. *See* Opderbeck*, supra* note 12, at 607 (opining that "other courts may apply the Seventh Circuit's *Remijas* analysis and allow some [data breach] claims to proceed" to trial).

131. The "developing consensus" is following the Seventh Circuit. Alison Frankel, *7th Circuit Kills Another Big Data Breach Class Action Defense*, REUTERS (Apr. 12, 2018, 5:29 PM), https://www.reuters.com/article/us-otc-databreach/7th-circuit-kills-another-big-data-breach-class-action-defense-idUSKBN1HJ3F8.

132. *Remijas*, 794 F.3d at 689-90.

133. *Id.*

134. *Id.* at 690-91.

> *cybersecurity, and 4) lost control over the value of their personal information.*[135]

The rest of the class had not yet experienced those adverse effects, but the complaint nonetheless characterized the harm as an injury-in-fact.[136] The Seventh Circuit framed the question at bar as whether the allegations satisfied *Clapper*'s requirement that the future injury be "certainly impending."[137] The court then began its analysis with a firm and consequential interpretation of the Supreme Court's standing doctrine: namely, that *Clapper* did not "foreclose any use whatsoever of future injuries to support Article III standing."[138] The court justified its interpretation with the Supreme Court's notable footnote in *Clapper*, which stated that precedent did "not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' . . . ."[139] The Seventh Circuit readily found that the plaintiffs met the substantial risk standard and therefore satisfied Article III standing, positing that there was no other plausible reason why hackers would steal consumer credit card data from Neiman Marcus if not for malicious and fraudulent purposes.[140]

The court concluded its analysis with a pointed warning: "it is important not to overread *Clapper*."[141] Whereas *Clapper* analyzed a speculative harm for an event that was not confirmed to have affected any plaintiffs, the facts in *Remijas* were the opposite: a data breach was explicitly recognized by the defendant.[142] This is a crucial distinction for the data breach context, where litigation is more likely to reflect the circumstances in *Remijas* rather than *Clapper*.[143]

135. *Id.* at 692.

136. *Id.*

137. *Id.*

138. *Id.* at 693.

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

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

141. *Id.* at 694.

142. *Id.*; *Clapper*, 568 U.S. at 401.

143. Breached organizations routinely recognize that a data breach occurred and may bring about adverse circumstances for the affected individual. *See supra* note 1; *see also infra* Part IV.C.

Article III Standing

IV. A New Way Forward for Data Breach Litigation

A. Distinguishing Modern Data Breach Litigation from the Seminal Standing Cases

The Supreme Court has never addressed the specific question of whether data breach victims generally satisfy Article III standing.[144] In fact, many of the Supreme Court's landmark standing doctrine cases have concerned considerably different factual circumstances with no connection to the data breach context whatsoever.[145] While it is unnecessary to compare and contrast the quintessential data breach case with every Supreme Court case on standing, *Lujan* and *Clapper* illuminate critical differences that help explain why standing has become "Mount Everest."[146]

In *Lujan*, the respondent-plaintiffs challenged an administrative interpretation of the Endangered Species Act, proposing various theories of harm.[147] Ultimately, the respondent-plaintiffs were concerned that certain endangered species and natural habitats would be destroyed, which would prevent respondents from using or observing those species in the future.[148] The facts of *Lujan* could not be further removed from the data breach context. To demonstrate the disparity, one of the plaintiffs in *Lujan* alleged that although she traveled to Sri Lanka ten years ago and was unable to view certain endangered species, the disputed administrative rule would harm her chances of observing those species when she intended to return to Sri Lanka in the future.[149] As the Court noted, the respondent-plaintiffs' allegations revolved around "some day" intentions and lacked the requisite concreteness and specificity for Article III standing. [150] In contrast, the typical data breach case contains far more concreteness and specificity because litigation only begins *after* an adverse event occurs and is recognized by the defendant.[151] This crucial factual difference has been recognized by at least one federal appellate court.[152]

The facts of *Clapper* were similarly distant from the data breach context. The Court in *Clapper* reduced the respondent-plaintiff's theory of harm into five discrete events before categorizing them as a "highly attenuated chain of possibilities."[153] In

144. *See* Bradford 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, 1327 (2016-2017) (arguing that "[i]n light of the continuing split in the circuits regarding Article III standing in data breach . . . cases, the Supreme Court will eventually have to address this important question").

145. *See infra notes* 144-49, 150-55 and accompanying text.

146. *See supra* note 14 and accompanying text.

147. *See supra* Part II.B.

148. Lujan v. Defs. of Wildlife, 504 U.S. 555, 562 (1992).

149. *Id.* at 563.

150. *Id.* at 564.

151. *See supra* note 143 and accompanying text.

152. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) (recognizing that the defendant "does not contest the fact that the initial breach took place").

153. *See supra* notes 90-91 and accompanying text.

addition to the lack of clarification on what would have created standing in that series of contingencies, data breach litigation is even further removed from the factual contours of *Clapper* because the chain is simplified from five events to two events: (1) a data breach occurs and (2) plaintiffs allege a substantial risk of future harm due to fraud and/or other misuses of personal information.[154] Whereas in *Clapper* the Court emphasized that the respondent-plaintiffs lacked actual knowledge of even the first necessary event in their theory of harm,[155] data breach litigation always begins from an objective truth: that sensitive information was exposed.[156] In essence, the Court's exercise in mapping out the respondent-plaintiffs' theory was to show there were too many *what-ifs*.[157] But in data breach litigation, there are significantly fewer unknowns surrounding the facts that underpin the proposed theory of harm. Normally the only major question to resolve is if the plaintiff's information will be chosen from the collection of stolen data over another victim and if that satisfies the injury-in-fact element of standing.[158] This principal distinction has also been recognized by at least one federal appellate court, which made the argument that standing after *Clapper* has proven to be particularly onerous because of the facts in that case.[159]

B. Assessing Commonly Proposed Theories of Harm

As has been shown, the defining issue in data breach lawsuits is *harm*.[160] In the deluge of litigation that data breach victims, as individuals and as classes, have unleashed upon the federal courts,[161] complaints have alleged a wide variety of

154. *Id.*

155. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 411 (2013) (stating that "respondents fail to offer any evidence that their communications have been monitored" under the challenged statute).

156. *See supra* note 143 and accompanying text. Even when data breach victims are not alerted by the organizations that suffered the breach, in many cases the victims may discover their stolen information on paste sites, deep and dark web forums, independent security services, and other third-party collectors. *See* Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Apr. 17, 2020, 3:00 AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

157. *See supra* note 153.

158. The dissent finds credence in cases that have proposed similar theories of harm. *Clapper*, 568 U.S. at 435 (Breyer, J., dissenting) (stating that "courts have often found *probabilistic* injuries sufficient to support standing").

159. *In Re* Zappos.co, Inc., Customer Data Sec. Breach Litigation, 888 F.3d 1020, 1026 (9th Cir. 2018) (arguing that "*Clapper*'s standing analysis was 'especially rigorous' because the case arose in a sensitive national security context involving intelligence gathering and foreign affairs, and because the plaintiffs were asking the courts to declare actions of the executive and legislative branches unconstitutional").

160. Solove & Citron, *supra* note 110, at 739.

161. *See* Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 93 (2014) (noting the 231 federal data-breach lawsuits from 2000-2011).

both common-law (focused on tort and contract) and statutory causes of action.[162] These complaints frequently allege negligence, privacy torts, and breach of fiduciary duty.[163] Other allegations include violations of state unfair and deceptive commercial acts and practice statutes ("UDAP" laws), state data security laws, the federal Privacy Act of 1974, and the federal Fair Credit Reporting Act ("FRCA").[164] Still, other plaintiffs have alleged the benefit of the bargain damages, the loss of value of personal information, foreseeable out-of-pocket costs, unjust enrichment, and overpayment for products and/or services lacking adequate and reasonable security measures.[165] Empirical analysis of data breach litigation has revealed commonalities in the underlying facts of these myriad allegations: plaintiffs seek relief for (1) actual loss from identity theft; (2) emotional distress; (3) the cost of preventing future losses; and (4) the increased risk of future harm.[166]

Due to the reluctance of courts to find standing for common and traditional causes of action, litigants and scholars have constructed increasingly creative theories of harm in an attempt to overcome the standing barrier.[167] One popular emerging theory revolves around the harm to a breach victim's mental capacity and/or physical wellness.[168] This might include the stress and time associated with cancelling accounts and replacing government-issued documents after a data breach and the attendant loss in productivity.[169] Another view is that anxiety and risk, both together and alone, deserve recognition as compensable harms in these types of suits.[170] This view contends that risk and anxiety from data breaches bring about immediate and concrete injuries: victims have an increased risk of identity theft, fraud, reputational damage, and can be discouraged from job and house-hunting, among other activities.[171] While these effects are certainly real and verifiable, they may be too nominal to support a bulwark theory of harm for data breach victims.[172]

162. *Id.* at 76.

163. Solove & Citron, *supra* note 110, at 749.

164. *Id.*

165. Selznick & LaMacchia, *supra* note 113, at 231.

166. Romanosky et al., *supra* note 161, at 76.

167. *See supra* note 9.

168. *See supra* notes 166-167 and accompanying text.

169. Selznick & LaMacchia, *supra* note 113, at 231.

170. Solove & Citron, *supra* note 110, at 744.

171. *Id.* at 745.

172. *See* Erika Harrell, *Victims of Identity Theft, 2016*, BUREAU OF JUST. STAT. (Jan. 2019), https://www.bjs.gov/index.cfm?ty=pbdetail&iid=6467 (showing that ten percent of identity-theft victims reported experiencing severe emotional distress).

C. Finding "Substantial Risk" Through State Data Breach Statutes: A Quantitative Approach to Standing

In adherence with the emerging appellate consensus[173] on standing in data breach litigation – namely, that the substantial risk standard is still good law – this Comment finds that one of the most conclusive and reliable methods of encouraging standing is by relying on state data breach notification laws and accompanying primary source documents.[174] Because there is no single federal law governing cybersecurity, data breaches, and related matters, states have adopted varying regulatory approaches.[175] These state laws are under-studied and largely ignored in modern data breach litigation but nonetheless contain a wealth of relevant information on norms and standards.[176]

The most critical part of state data breach statutes is the condition upon which the breached entity is required to notify affected individuals.[177] Twenty-two states and the District of Columbia compel notification if the breached entity determines that a data breach has occurred.[178] In contrast, 28 states compel notification to affected individuals if the breached entity conducts an investigation and finds that the compromised data has actually been misused, or that there is a likelihood that it will be misused.[179] Because the former category institutes a blanket requirement while the latter places an affirmative obligation on breached organizations, the second group of states presents a better case study of when organizations make their own determination that the breach poses a substantial risk of future harm to their clients and consumers.

These statutes contain several variations but are ultimately cohesive in the manner in which they delegate the determination of whether harm is very likely to follow the data breach. For example, Maryland's data breach statute[180] requires:

173. *See supra* Part II.B.

174. *See infra* notes 175-176 and accompanying text.

175. *See* Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. ILL. L. REV. 811, 813 (2020) (explaining that U.S. "cybersecurity law" consists of a "cluster of state and federal laws").

176. *See supra* note 31 and accompanying text.

177. In other words, whether the data breach statute has a contingency or an obligation regarding notification is the focal point. *See infra* notes 178-181 and accompanying text.

178. These states consist of Arizona, California, Delaware, Georgia, Hawaii, Illinoi, Iowa, Kentucky, Massachusetts, Minnesota, Montana, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Pennsylvania, Rhode Island, South Dakota, Tennessee, and Texas. *Data Breach Notification in the United States and Territories*, PRIV. RTS. CLEARINGHOUSE (Dec. 18, 2018), https://privacyrights.org/resources/data-breach-notification-united-states-and-territories.

179. This group of states is composed of Alabama, Alaska, Arkansas, Colorado, Connecticut, Florida, Idaho, Indiana, Kansas, Louisiana, Maine, Maryland, Michigan, Mississippi, Missouri, Nebraska, New Hampshire, Ohio, Oklahoma, Oregon, South Carolina, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. *Id.*

180. Maryland Personal Information Protection Act, MD. CODE ANN., COM. LAW. § 14-3504.

Article III Standing

> *A business that owns, licenses, or maintains computerized data that includes personal information . . . when it discovers or is notified that it incurred a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach. [I]f, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the owner . . . of the computerized data shall notify the individual of the breach.*[181]

Alabama's data breach statute compels a similar result but includes language that is more closely aligned with the Supreme Court's standing doctrine tests. [182] Covered entities are required to notify affected individuals if: ". . . as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause *substantial* harm to the individuals to whom the information relates . . . ."[183] Whether or not a state's data breach statute uses the term "substantial" when it compels notification should not be dispositive in recognizing that the intent of these statutes, collectively, is to hold breached organizations accountable when they make the objective determination that there is an increased likelihood of harm to affected individuals.[184]

Data collected on these statutory notifications suggest that breached entities regularly and continuously make the independent determination that their consumers face a substantial risk of future harm as a result of a data breach.[185] These objective conclusions should be given greater weight in future data breach litigation.[186] A subgroup of the 28 states that compel notification after a determination of increased likelihood of harm have also made data breach notices

181. *Id.* § 14-3504(b)(1)-(2).

182. Alabama Data Breach Notification Act of 2018, ALA. CODE § 8-38-1-12.

183. *Id.* § 8-38-5 (emphasis added).

184. For example, although Maryland's data breach statute, does not explicitly provide *what* the likelihood that personal information has been or will be misused, the Maryland Attorney General's Office has provided official guidance that "[i]f the investigation shows that there is a *reasonable* chance that the data will be misused, that business must notify the affected consumers." *Guidelines for Businesses to Comply with the Maryland Personal Information Protection Act*, MD. OFF. OF THE ATT'Y GEN., https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/businessGL.aspx (emphasis added) (last visited Aug. 16, 2021) (referencing MD. CODE ANN., COM. LAW. § 14-3504).

185. *See infra* note 188 and accompanying text.

186. This is common in other areas of law where courts look at the objective actions and understanding of litigants. For example, a foundational principle of contract law is that courts apply an objective test that considers the parties' words and conduct rather than their subjective beliefs and intentions. *See* RESTATEMENT (SECOND) OF CONTRACTS §§ 17-18, 23 (KESSLER ET AL. 2014).

served to state residents publicly available online.[187] Between 2006 and the present, this eight state subgroup has received over 17,000 data breach notices from businesses and organizations, each of which was statutorily obligated to conduct an internal investigation for actual misuse or an increased likelihood of misuse of breached personal information.[188] Collectively, these notices account for approximately 75% of the all data breach notices indexed and mirrored by the Data Breach Archives project.[189]

This finding is significant, and the ramifications warrant an explicit explanation: over 17,000 investigations were conducted by breached organizations and businesses, and although each of those found actual misuse or an increased likelihood of misuse of personal information, the affected consumers were left without recourse under current law.[190] Going forward, courts should attribute greater significance to these state data breach statutes, which serve as a legislative expression of a legally cognizable interest.[191]

Plaintiffs have not relied on state data breach statutes (which establish that unauthorized access to their residents' information is a *de facto* harm) as a prominent litigation theory.[192] However, recent litigation in adjacent areas of law demonstrates how courts can successfully rely on state privacy statutes to find Article III standing.[193] In *Patel v. Facebook, Inc.*, the Ninth Circuit found standing when plaintiffs alleged that Facebook violated their rights under the Illinois Biometric Information Privacy Act ("BIPA") when Facebook implemented its "tag suggestions" facial-recognition feature without obtaining the plaintiffs' explicit consent.[194] The court analyzed whether the BIPA was established to protect the plaintiffs' concrete interests (as opposed to purely procedural rights), and if so, whether the specific statutory violations alleged actually caused harm, or presented a material risk of harm to the concrete interests.[195] The court concluded that (1) the BIPA protected concrete interests in privacy because of the legislature's intent to

187. This subgroup consists of Indiana, Maine, Maryland, New Hampshire, Oregon, Vermont, Washington, and Wisconsin. *See supra* note 179.

188. *Id.*

189. *Id.* (listing the other states tracked by the Data Breach Archives project as: California, Delaware, Iowa, Massachusetts, and Montana, which all require notification without investigation).

190. *See supra* note 9 and accompanying text.

191. Justice Stevens' concurrence in *Lujan* gives credence to this notion by encouraging deference to Congress when considering what may be a legally cognizable interest. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 582 (1992) (Stevens, J., concurring).

192. *See supra* Part III.

193. *See* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019); Pretrial Order No. 20: Granting in Part and Denying in Part Motion to Dismiss First Amended Complaint, *In re* Facebook, Inc., Consumer Privacy User Profile Litigation, 402 F. Supp. 3d 767 (N.D. Cal. 2019).

194. 932 F.3d at 1268.

195. *Id.* at 1270-71.

safeguard the public welfare through the regulation of biometric information, and (2) that the plaintiffs alleged a concrete and particularized harm because Facebook's alleged activities were the very acts targeted by the statute.[196] Although *Patel* was primarily concerned with direct violation of a right granted by statute – which does not reflect the typical data breach case – it nonetheless demonstrates how a court can look to the privacy interests protected by state law to find harm sufficient for standing.[197]

V. ADDRESSING POSSIBLE CRITICISMS OF THE PROPOSED SOLUTION

A. This Comment's Proposal is Consistent with Evolving Jurisprudence on Data-Centric Issues

Courts are increasingly realizing the unique and innate power of data in society and are adapting legal frameworks accordingly.[198] For the Supreme Court, this has been most evident in the Fourth Amendment context.[199] Although data breach litigation does not usually involve Fourth Amendment issues, the principles espoused by the Court in this area of law can reasonably be applied to other areas of law where the presence of data makes a given doctrine unworkable.[200]

The most notable example is the Court's doctrinal shift away from the third party doctrine, which holds that individuals are not entitled to an expectation of privacy in information they voluntarily provide to third parties.[201] Established in the 1970s,[202] the third party doctrine began to face serious scrutiny from the Court over thirty years later in *United States v. Jones*, which asked whether warrantless GPS tracking of the defendant' vehicle over 28 days violated the Fourth Amendment.[203] After finding that the conduct did violate the defendant's Fourth Amendment rights, Justice Sotomayor, in her concurrence, laid the groundwork to diminish the third party doctrine's applicability in future data cases.[204] Justice Sotomayor

196. *Id.* at 1273-74.

197. *See supra* notes 194-196 and accompanying text.

198. *See infra* notes 199-200 and accompanying text.

199. "In its recent Fourth Amendment jurisprudence, the Supreme Court has recognized that advances in technology can increase the potential for unreasonable intrusions into personal privacy." *Patel*, 932 F.3d at 1272.

200. The Supreme Court has generally observed in the Fourth Amendment context that technological advances provide "access to a category of information otherwise unknowable" and "implicate privacy concerns" in a manner different from tradition intrusions. *Id.* at 1272-73 (citing Riley v. California, 573 U.S. 373, 393 (2014)).

201. RICHARD THOMPSON, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 1 (2014).

202. *See* Smith v. Maryland, 442 U.S. 735 (1979).

203. United States v. Jones, 565 U.S. 400 at 403 (2012).

204. *Id.* at 417 (Sotomayor, J., concurring) (stating "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties").

explicitly noted that the third party doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[205]

The third party doctrine came under attack a few years later in *Carpenter v. United States* where the Court majority held that law enforcement officers violated the Fourth Amendment by subpoenaing the petitioner's cell-site location information ("CLSI") from his telephone provider.[206] The Court stopped short of renouncing the third party doctrine, instead declining to extend it to cover the circumstances it was confronted with, noting the "unique nature of cell phone location records . . . ."[207] In carving out a CLSI exception to the third party doctrine, the majority reasoned that the information was "deeply revealing" because of "its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection," and therefore was not less deserving of Fourth Amendment protection simply because the data was gathered by a third party.[208]

The Court could fairly transpose that analysis onto the data breach context in continued recognition of the shortcomings of traditional standards for novel circumstances. To be clear, the data at issue in *Carpenter*'s Fourth Amendment and data breach contexts are the same: electronic files, records, and logs that are "deeply revealing" because of their "depth, breadth, and comprehensive reach" are unavoidable in modern society.[209] But the Court's precedent leads to convoluted and inconsistent outcomes; for example, if a GPS or CSLI provider suffered a data breach, which has happened, leaked data would enjoy Fourth Amendment protection by default under the *Carpenter* ruling but would not receive reciprocal treatment or recognition for standing purposes in civil litigation.[210] In addition to the data at issue sharing the same qualitative characteristics in these contexts, both instances are primarily concerned with surviving a pre-trial motion (i.e., a motion to suppress in the former, and a motion to dismiss in the latter).[211] In summary, the Court should decline to extend its stringent standing doctrine to data breach cases

205. *Id.*

206. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (finding that "[t]he location information obtained from [petitioner]'s wireless carriers was the product of a search").

207. *Id.*

208. *Id.* at 2223.

209. *Id.*

210. *See* Thomas Ricker & Chris Welch, *Garmin Confirms Cyber Attack as Fitness Tracking Systems Come Back Online*, THE VERGE (July 27, 2020 1:11 PM), https://www.theverge.com/2020/7/27/21339910/garmin-back-online-recovery-ransomeware; Stephen Schroeder, *Top 11 Worst Location Data Privacy Breaches*, TURTLER (Sep. 25, 2017), https://turtler.io/news/top-11-worst-location-data-privacy-breaches.

211. *See* Karlsgodt, *supra* note 42 (explaining the various theories used in data breach litigation and their likelihood of surviving a motion to dismiss).

just as it declined to extend the third party doctrine to cover CLSI cases because of circumstantial parity.[212]

B. Existing Safeguards that Will Prevent a Surge of Litigation

An additional anticipated criticism is that a flood of litigation will follow if standing is more easily satisfied in these cases.[213] In addition, other than Article III standing, several barriers remain in place that are likely to minimize the number of claims which can proceed. One of the foremost hurdles is class certification and proving "predominance" – i.e., that questions of law or fact predominate over any questions affecting only individual members.[214] Notably, this was the issue on remand in *Remijas v. Neiman Marcus* after the Seventh Circuit found that the plaintiffs had standing to sue.[215] The trial court found that the "class as it is currently composed has a fundamental conflict that undermines the adequacy of the representation of the class."[216] Class decertification in a case that initially propelled a noteworthy interpretation of Article III precedent shows that satisfying standing is only the beginning.[217]

CONCLUSION

Data breaches cause rampant and verifiable harm in society, and the law is well equipped to provide redress without the need for a new doctrine or framework.[218] Indeed, this Comment recommends that courts interpret the Supreme Court's development of the standing doctrine in a manner that does not abrogate the substantial risk test, which appears to be the emerging federal appellate consensus.[219] Once the factual differences and policy implications that predicated the seminal standing cases are accounted for, it becomes clear that the data breach litigation context is wholly distinct and should satisfy Article III standing more often than the current rate.[220] In addition, an emerging body of data breach research shows that breached businesses and organizations routinely find that their consumers' data has been misused or faces a high likelihood of future misuse, yet these determinations have not factored into the discussion of remedying the

212. *Carpenter*, 138 S. Ct. at 2217.

213. This concern might be moot due to the current quantity of cases. *See supra* notes 12, 161 and accompanying text.

214. FED. R. CIV. P. 23(b)(3).

215. Remijas v. Neiman Marcus Grp., LLC, 341 F. Supp. 3d 823, 825 (N.D. Ill. 2018).

216. *Id.* at 828.

217. *Id.*

218. *See supra* Part IV.

219. *See supra* Part II.

220. *See supra* Part IV.A.

associated harms.[221] Thus, the state statutes which govern those data breach investigations and notifications serve as a legislative expression of a legally cognizable interest that should be afforded greater deference in the standing analysis.[222] Finally, the proposed way forward is in line with evolving jurisprudence on data-centric issues and is not likely to create an influx of litigation beyond what currently exists.[223]

221. *See supra* Part IV.C.

222. *Id.*

223. *See supra* Part V.