PRIVACY AS PRETENSE: EMPIRICALLY MAPPING THE GAP BETWEEN LEGISLATIVE & JUDICIAL PROTECTIONS OF PRIVACY

Christopher Muhawe[†]
& Masooda Bashir[††]

Abstract

While many statutes recognize that violations of privacy cause harm—and some even provide for private rights of action to enforce privacy rights—scholars have speculated that the judicial doctrine of Article III standing could create a procedural hurdle to remedying privacy harms. This empirical study maps the extent of that hurdle by investigating the data privacy litigation landscape of the U.S. Federal Courts in light of the strict Article III injury requirement for addressing privacy violations. The results are striking: Close to 60% of the cases heard in federal courts from 2000 to 2020 were dismissed for a failure to satisfy the strict injury threshold of Article III standing requirements. The empirical analysis thus reveals a significant gap between what legislators intend privacy protection to do (and what privacy statutes provided for on their face), and the actual landscape of privacy protection as interpreted by courts.

TABLE OF CONTENTS

Introduction 259
I. Stakes in Information Privacy 262
A. The Private Right of Action in Data Privacy Statutes 263
B. Standing Doctrine and the Role of "Injury-in-Fact" 268
1. Progression of the Modern Standing Doctrine 268
a. Historical developments of the doctrine of standing 270
b. The narrowing definition of privacy harms in the standing inquiry 270
2. Standing and its Application in Privacy Litigation.....271

† Privacy Law Researcher, Attorney at Law, & J.S.D. 2023, College of Law and School of Information Sciences at the University of Illinois at Urbana Champaign.

†† Associate Professor, School of Information Sciences, University of Illinois; Associate Professor, Information Trust Institute University of Illinois; Adjunct Assistant Professor, Department of Industrial and Enterprise Systems Engineering, University of Illinois.

a. *Clapper v. Amnesty International USA* conception of Article III standing....271
b. *Spokeo v. Robins* conception of Article III standing....271
c. *TransUnion v. Ramirez* conception of Article III standing....272
II. Empirically Mapping the Role of the Standing Doctrine in Privacy Enforcement....273
A. Previous Studies....274
B. Methodology of the Study....275
1. Phase 1—Selecting search terms and phrases....276
2. Phase 2—Database selection and search query formulation....276
3. Phase 3—Manual selection of opinions for coding....278
4. Phase 4—Data collection and the code book....279
III. Results of the Study....280
A. Results of the Outcome of the Standing Inquiry....280
1. What is the frequency at which the standing motion is raised within the context of data privacy litigation?....280
2. To what extent does lack of injury hinder the enforcement of data privacy protection?....282
3. How has the proportion of dismissal for lack of injury varied from 2000 to 2020?....284
4. Are courts more likely to find standing for some types of privacy cases?....284
5. What role did the Spokeo decision have on data privacy violation cases?....286
IV. Discussion....287
A. The Quest to Characterize Privacy Harm in the Face of the Strict Standing Requirement....287
B. Revisiting the Separation of Powers Doctrine in the Standing Inquiry....289
C. Unpacking the TCPA in the Face of the Standing Inquiry....292
D. Finding Footing after the Spokeo Decision....294
E. The Social Inequalities Perpetuated by the Standing Doctrine in Data Privacy Litigation....295
IV. Potential Prescriptions, Limitations, and Opportunities for Future Work....297
A. Potential Prescriptions....297
B. Limitations and Opportunities for Future Work....298
V. Conclusion....298
Appendix A....299

INTRODUCTION

Reliance on the digital world has ushered in an unprecedented collection of personally identifiable information ("PII").[1] Private and public organizations collect massive amounts of personally identifiable information, and they have become strongrooms of sensitive personal information.[2] The collected private information ranges from names, dates of birth, social security numbers, health records, religious affiliations, political party affiliations, banking histories, location data, biometrics, shopping histories, and home addresses—and these are just the highlights of an endless list.[3]

The increased collection of personal information is a result of the dependence on the digital world for most human activities including health care, education, banking, shopping, hospitality, leisure, and social connectivity.[4] This certainly became true and more pronounced during the COVID-19 health crisis.[5]

The unrelenting quest for data collection has grown in tandem with increased data privacy violations.[6] Data privacy violations—including

1. *See* Huidong Sun et al., *Identifying Big Data's Opportunities, Challenges, and Implications in Finance*, 8(10) MATHEMATICS, Oct. 10, 2020, at 1 (stating that the number of electronic devices for personal and corporate use like internet modems, mobile phones, tracking devices, and computers generates large volumes of data daily in the advent of big data); *see also* DAVID T. BOURGEOIS ET AL., INFORMATION SYSTEMS FOR BUSINESS AND BEYOND 3, 9–10 (2nd ed. 2019) (stating that the ability to collect, process, store and share private information has been revolutionized by great improvements in technology). *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY & PRIVACY IN THE INFORMATION AGE 2 (Jack M. Balkin & Beth Simone Noveck eds., 2004) (discussing how society "should understand and protect privacy in light of . . . profound technological developments").

2. Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who is Using it)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection [https://perma.cc/DRV7-PYXP].

3. *Id.*; *see also Your Data is Shared and Sold . . . What's Being Done About it?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/SYQ9-JCAT] ("Every time you interact with [a] company [online], you should expect that the company is recording that information and connecting it to you.") (quoting Elea Feit, senior fellow at Wharton Customer Analytics and a Drexel marketing professor); *see generally* JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014) (documenting the author's year-long experiment of avoiding surveillance by business entities by using burner phones, avoiding using Google services, avoiding credit cards, using fake names when she was unable to pay using cash, and using a signal-blocking bag to prevent her smartphone from sending and receiving phone service signals; to the author's surprise, she recorded 50% success in her efforts to avoid commercial surveillance).

4. Terry Brown, *The Importance of Information and Communication Technology (ICT)*, IT CHRONICLES (May 18, 2020), https://itchronicles.com/information-and-communication-technology/the-importance-of-information-and-communication-technology-ict/ [https://perma.cc/KS3A-Z29P]; *see* Wonseok Oh et al., *ICT Challenges and Opportunities in Building a "Bright Society"*, 19 J. ASS'N FOR INFO. SYS. 58, 58–59 (2018) (noting issues with increased dependence on technology, including cyberbullying and its impact); BOURGEOIS, *supra* note 1, at 1 ("[I]nformation systems have progressed to being virtually everywhere, even to the point where you may not realize its existence in many of your daily activities."); Janna Anderson & Lee Rainie, *The Positives of Digital Life*, PEW RES. CTR. (July 3, 2018), https://www.pewresearch.org/internet/2018/07/03/the-positives-of-digital-life/ [perma.cc/2PNL-J77N] (describing how reliance on the digital realm, for most human activities, has vastly improved people's lives, habits, and expectations).

5. *See In Their Own Words, Americans Describe the Struggles and Silver Linings of the COVID-19 Pandemic*, PEW RES. CTR. (Mar. 5, 2021) https://www.pewresearch.org/2021/03/05/in-their-own-words-americans-describe-the-struggles-and-silver-linings-of-the-covid-19-pandemic/ [https://perma.cc/78W6-QBWS] (sharing that 13% of Americans reported that they were able to work remotely during the pandemic and considered this as positive).

6. *See The Cost of a Data Breach 2023*, IBM, https://www.ibm.com/reports/data-breach [https://perma.cc/QAA8-WQS2] (last visited Sept. 19, 2023) (reporting that data breach costs increased by 15%

unauthorized access to and misuse of an individual's electronic health records, stolen social security numbers, and misuse of addresses, biometric data, and phone numbers—have become shockingly common. In a recent *Pew* study, it is reported that over a quarter of Americans experience major data privacy violations each year.[7]

Over the years, legislatures both at the state and federal levels have responded to the problem of privacy violations through a sprawling patchwork of statutes that are aimed at protecting against privacy violations with the ensuing harms that are driven by technology.[8] These statutes protect many American consumers from being tracked and surveilled, whether through the apps on their phones or their online searches for different products for home use. The privacy statutes impose protections and obligations on particular sectors and participants.[9] These include financial institutions, health care entities, education institutions, and communication service providers or specific data categories such as children's data.[10]

To bring a lawsuit in the United States federal courts, a plaintiff must prove that he has been injured as per the Supreme Court's construction of Article III's

---

from 2020 to 2023); Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/7B85-8FJR] ("Cambridge Analytica, a political data firm hired by President Trump's 2016 election campaign, gained access to private information on more than 50 million Facebook users. The firm offered tools that could identify the personalities of American voters and influence their behavior.").

7. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/KY7G-9J2F] (reporting that 28% of the U.S population had "suffered at least one of three kinds of major identity theft problems in the previous 12 months": 21% had fraudulent charges on their credit or debit card, 8% had a takeover of their social media or email accounts, and 6% had someone attempt to open a credit line or get a loan in their name).

8. *See* Daniel Castro et al., *The Looming Cost of a Patchwork of State Privacy Laws*, INFO. TECH. & INNOVATION FOUND. (Jan. 24, 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/ [https://perma.cc/X8V6-QPRA] ("In the absence of a comprehensive federal law, a handful of large states, including California, Colorado, and Virginia, have passed or begun to enact data privacy legislation.").

9. *See* David Harrington, *U.S. Privacy Laws: The Complete Guide*, VARONIS (Mar. 10, 2023), https://www.varonis.com/blog/us-privacy-laws [https://perma.cc/7K85-48MG] (providing details on the various U.S. privacy laws, including laws particularly aimed at a given sector, such as medical fields and financial institutions).

10. *See* The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (covering the privacy of education records and information); The Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 100 Stat. 2548 (codified in scattered titles and sections of the U.S. Code) (providing privacy protection for health information); The Genetic Information Nondiscrimination Act (GINA), 42 U.S.C § 2000ff (providing privacy protection for genetic information); The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681–1681x (safeguarding information collected by consumer reporting agencies such as credit bureaus); The Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510–2523 (composing three titles: the Wiretap Act which regulates the interception of communication in transit; the Stored Communications Act which prohibits the unauthorized access or disclosure of certain electronic communications stored by internet service providers; and the Pen Register Act which prohibits installation of a "pen register" or "trap and trace device" without a court order); The Children's On-line Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (imposing particular responsibilities and restrictions on website operators with products directed towards children); The Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801–6809 (requiring financial institutions to provide background on information-sharing practices to their consumers).

standing requirement.[11] Article III provides the exercise of federal judicial authority to apply only to "cases" or "controversies."[12] Among the key elements of what the courts deem as a case or controversy is that the plaintiff must have suffered an injury-in-fact.[13] The requirement that the plaintiff shows that they have suffered injury-in-fact is a fundamental component of the Court's standing doctrine.[14] As a result of the Court's interpretation of the Article III standing doctrine, the injury-in-fact requirement applies even where the legislature has expressly provided for statutory damages.[15] With regards to privacy law, in 2016, the Supreme Court in *Spokeo, Inc. v. Robins*[16] declined to find that the plaintiff had standing to recover under the private right of action as provided for under the Fair Credit Report Act ("FCRA").[17]

Although standing doctrine serves important constitutional purposes, it also creates a potential procedural chokepoint in cases where Congress seeks to protect hard-to-define or intangible harms, such as those experienced when there is a privacy violation.[18] Since privacy claims fundamentally involve intangible, probabilistic, futuristic, and widespread harms, the standing doctrine risks freezing out privacy claims without providing meaningful remedies for many, most, or even all, plaintiffs.[19]

This paper presents the first empirical study attempting to quantify or measure how the U.S. federal courts have handled the question of data privacy injuries in the presence of the strict standing requirement. By reviewing and analyzing all privacy cases heard in federal courts between 2000 and 2020, the study provides the first descriptive answers to several fundamental questions about the role of standing in (federal) privacy suits, including the rate of

11. Lujan v. Defs. of Wildlife, 504 U.S 555, 560 (1992) (embodying one of the most influential decisions by the Supreme Court on standing requirements under Article III of the United States Constitution, wherein the Court emphatically stated that before a plaintiff brings a case to court, "the plaintiff must have suffered an 'injury in fact'—an invasion of a legally protected interest which is . . . concrete and particularized" that can be "redressed by a favorable decision").

12. U.S. CONST. art. III, § 2.

13. Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc., 528 U.S. 167, 181 (2000) (stating that the injury in fact requirement is satisfied only by demonstrating "injury to the plaintiff," as opposed to injury to another party).

14. *Id.* (holding that injury to the plaintiff is essential to satisfy the "injury in fact" requirement in Article III standing).

15. *See* Doe v. Chao, 540 U.S. 614, 627 (2004) ("The question before us is whether plaintiffs must prove some actual damages to qualify for a minimum statutory award . . . . We hold that they must.").

16. Spokeo, Inc. v. Robins, 578 U.S. 330, 333 (2016).

17. *Id.* at 337–42 (finding that even where Congress has created a private right of action for statutory violations, plaintiffs must demonstrate concrete and particularized harm to satisfy the injury in fact requirement under Article III standing).

18. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 798–99 (2016) ("For most courts, privacy and data security harms are too speculative and hypothetical, too based on subjective fears and anxieties, and not concrete and significant enough to warrant recognition."); *see also* Trayce A. Hockstad, *Rats and Trees Need Lawyers Too: Community Responsibility in Deodand Practice and Modern Environmentalism*, 18 VT. J. ENV'T. L. 105, 118 (2016) ("[The required] showing of individual injury has proven to be the most difficult element for environmental activists to show during the litigation process.").

19. *See* Seth F. Kreimer, "*Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 760 (2016) ("The outcomes of adjudication by the Court in the information age and the spooky characteristics of information itself demonstrate that today the constitutional test for a 'case' or 'controversy' cannot require that plaintiffs demonstrate harm to person, goods, or pocketbook.").

dismissal of privacy cases for lack of standing; the relative success of plaintiffs in establishing standing under different privacy statutes; and the way that various judicial applications of standing doctrine affect plaintiff success rates.

The overarching goal of this study is to help scholars, litigants, and policymakers more clearly understand how—and to what extent—standing doctrine prevents enforcement of privacy protections. This understanding is important for pragmatic and theoretical reasons. From a pragmatic perspective, the study provides a measure of the on-the-ground success of legislative attempts to protect privacy; this is considered a meaningful goal, if the extent of legislative activity in this realm is a good indicator of the importance and an issue of particular relevance to litigants seeking to craft successful privacy claims. More theoretically, evaluating the empirical enforcement of privacy rights reveals a gap between the law on the books and the law on the ground. As other scholars have noted, such gaps are problematic for both practical and normative reasons. At the least, it means that privacy laws do not effectively achieve the goals set by legislatures; at worst, it undermines the democratic functions of the legislative branch and the interpretive function of the judiciary.[20]

To illuminate these issues, the remainder of this article proceeds in the following fashion. Part I presents the key background regarding the private right of action as provided in data privacy statutes. This part also discusses the progression of the modern Article III standing doctrine as applied by federal courts and how it operates in data privacy litigation. Part II reviews previous studies on data privacy enforcement and sets out the methodology for empirically understanding the data privacy litigation landscape. Part III discusses the results of the study. Part IV presents a discussion and implication of the findings. Part V discusses potential prescriptions, limitations, and opportunities for future work that may build on this study. Part VI presents the conclusion of this paper.

I. STAKES IN INFORMATION PRIVACY

Privacy is valuable to the existence of humans in their individual capacity and has the potential of generating large positive spillovers for society as a collective.[21] Privacy protection is key in protecting marginalized and vulnerable persons, a key tenet in promoting a free, fair, and democratic society.[22] A 2019 *Pew Research Institute* survey on how American adults feel about the state of privacy in the U.S. report established that 79% of Americans are "concerned about the way their data is being used by companies" and that 64% of adults are

20. *Supra* notes 18–19; Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 ME. L. REV. 15, 16–20 (2022).

21. *See generally* Julie E. Cohen, *Configuring the Networked Citizen*, IMAGINING NEW LEGALITIES: PRIVACY AND ITS POSSIBILITIES IN THE 21ST CENTURY 129 (Austin Sarat et al. eds., 2012) ("The gradual, inexorable embedding of networked information technologies has the potential to alter, in largely invisible ways, the interrelated processes of subject formation and culture formation.").

22. *See* Michele Gilman & Rebecca Green, *The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization*, 42 N.Y.U. REV. L. & SOC. CHANGE 253, 255 (2018) (discussing the "Surveillance Gap," wherein certain marginalized groups do not have access to social resources, resulting in detrimental social effects both for the marginalized and society).

concerned about how their data is being used by the government.[23] The same survey reports that most Americans "feel they have little or no control over how these entities use their personal information."[24] This *Pew* research and previous surveys demonstrate that Americans are interested in having control over their data privacy.[25] This need to have control of one's privacy is for the right reasons because privacy promotes "liberty, autonomy, selfhood, [] human relations," and other civil liberties in the furtherance of the existence of a free society.[26] Indeed, philosopher Anita Allen, for example, has clearly illustrated that privacy is valuable for democratic societies in which people need the capacity to think independently.[27]

Several statutes provide for a private right of action as an avenue through which victims can seek relief from the court for the harm suffered as a result of privacy violations.[28] This Section further discusses the standing doctrine and, highlights the critical role that the Article III standing injury-in-fact requirement plays in the privacy enforcement regime.

A. The Private Right of Action in Data Privacy Statutes

Many data privacy laws provide for a private right of action.[29] The inclusion of a private right of action in these statutes offers a great platform for understanding the legislative intent in the context of privacy law enforcement.[30] Among other reasons, the inclusion of a private cause of action in a statute signals the remedial intention of such the statute and that a person's interest can be harmed by its violation.[31]

It can be argued that the several data privacy statutes that provide for a private right of action represent statutory recognition of privacy harm since

23. Auxier et al., *supra* note 7.

24. *Id.*

25. *See* Mary Madden & Lee Rainie, *Americans' Views About Data Collection and Security*, PEW RES. CTR. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/ [https://perma.cc/J79R-JJ22] ("Nine-in-ten adults feel various dimensions of control over personal information collection are 'very important' to them.").

26. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980); *see also* DAVID J. GARROW, LIBERTY AND SEXUALITY: THE RIGHT TO PRIVACY AND THE MAKING OF *ROE V. WADE* 252 (1st ed. 1994) (explaining that Americans' cherished decisional privacy rights are protected by the term "liberty," as found in the Constitution).

27. ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 23 (2011); ANITA L. ALLEN, WHY PRIVACY ISN'T EVERYTHING: FEMINIST REFLECTIONS ON PERSONAL ACCOUNTABILITY 5–7, 155 (2003).

28. *See* The Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510–2523 (comprising the Wiretap Act, the Stored Communications Act, and the Pen Register Act, which provide remedies for various privacy violations); 47 U.S.C. § 551(f) (providing a cause of action for those aggrieved under the Cable Communications Policy Act); 15 U.S.C. § 1681 (providing a cause of action to consumers who suffer harm as a result of willful or negligent violation of the Fair Credit Reporting Act); 18 U.S.C. § 2710 (c) (providing a cause of action for those aggrieved under the Video Privacy Protection Act); *see also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 160–61 (6th ed. 2019) (listing statutes protecting privacy interests with the private cause of action).

29. *See supra* note 28 (listing statutes with private causes of action).

30. *See* Becky Chao et al., *Enforcing a New Privacy Law*, NEW AM. (Nov. 20, 2019), https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/ [https://perma.cc/5PGM-9222] (explaining the importance in Congress carefully considering different privacy law schemes and remedies).

31. *See id.* (explaining the benefits of providing a private right of action for privacy violations, including acting as "an extension of democratic participation").

enforcement through such actions can be seen as a regulation tool.[32] It should be noted, however, that not all privacy statutes provide for a private right of action.[33] Among others, the following statutes do not provide a private right of action: the Health Insurance Portability and Accountability Act ("HIPAA") which provides for privacy and security rules that protect sensitive patient health information from being disclosed without the patient's consent or knowledge;[34] the Children's Online Privacy Protection Act ("COPPA") which requires companies which collect personal information from children under the age of 13 to post clear privacy policies and to notify parents and get their verifiable consent before collecting personal information about a child;[35] the Family Education Rights and Privacy Act ("FERPA") which regulates access to education information and records held by public entities;[36] and the Genetic Information Nondiscrimination Act ("GINA") which, among others, protects the privacy of and guards against the misuse of genetic information.[37]

When an intrusion occurs, the absence of a private right of action in these statutes means that citizens cannot in their individual capacity directly approach the court to enforce their privacy rights under the said statutes.[38] They can only file complaints to agencies appointed under these statutes.[39] It can be argued that the delegation of privacy enforcement authority to these different agencies does little in providing redress to and compensation of victims for privacy violations.[40] Privacy victims are further affected by the lack of comprehensive protection because these agencies and regulators are often troubled with limited resources and are therefore forced to cherry-pick which matters to enforce.[41] This grossly disadvantages the individuals who suffer privacy violations under the said statutes.

The existence of the private right of action in a statute may signal a private enforcement mechanism of the statute when an intrusion occurs.[42] This is more so because there is no written canon or guideline explaining when private harms attach. In this regard, the provision of the private right of action in a statute may

32. *See* Aditi Bagchi, *Distributive Injustice and Private Law*, 60 HASTINGS L.J. 105, 111 (2008) (discussing how private rights of actions often have a public component, at least in part because the government provides private parties for private rights of actions).

33. *See* Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. Rev. 1639, 1648–51 (2022) (discussing some examples of privacy statutes and regulations that are enforced by public agencies).

34. 42 U.S.C. § 1302.

35. 15 U.S.C. §§ 6501–6506.

36. 20 U.S.C. § 1232g.

37. 42 U.S.C § 2000ff.

38. Scholz, *supra* note 33, at 1648–51.

39. *See, e.g.*, 42 U.S.C. §§ 1320(d)–5, (detailing penalties for violating HIPPA, enforced by the Office for Civil Rights (OCR) under the U.S. Department of Health and Human Services); 15 U.S.C. §§ 6501–6506 (detailing penalties for violating COPPA, enforced by the Federal Trade Commission).

40. *See* Zoom Video Commc'ns, Inc., No. 192-3167, 2021 WL 363289, at *1 (F.T.C. Jan. 19, 2021) (Chopra, Comm'r, dissenting) (arguing that the settlement approach adopted by the FTC regulators and enforcers does not help victims of privacy violations in compensating the harms they suffer at the hands of violators).

41. *See* David A. Hyman & William E. Kovacic, *Why Who Does What Matters: Governmental Design and Agency Performance*, 82 GEO. WASH. L. REV. 1446, 1484 (2014) ("Agencies with inadequate talent and frail resources are prone to devise faulty programs or execute tasks ineffectively.").

42. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 821–22 (2022).

offer guidance for when harm attaches.[43] For instance, under the Fair Credit Reporting Act ("FCRA"), the law provides that any person who had previously violated the statute is liable in an amount equal to the sum of damages sustained by the consumer or "damages of not less than $100 and not more than $1000."[44] Other statutes including the Video Privacy Protection Act ("VPPA") and the Telephone Consumer Protection Act ("TCPA") provide for a private cause of action.[45]

A closer look at the statutes that provide for a private right of action could suggest a judicial recognition of harm to the extent that the plaintiff need not prove specific or tangible harm such as monetary or physical.[46] The case *FAA v. Cooper* demonstrates how the standing inquiry stands in the way of privacy enforcement even in the face of clear legislative intent by Congress in providing for the private right of action.[47] This case was reviewed by the Supreme Court after the Ninth Circuit's consideration.[48] In this case, the plaintiff, Cooper, was a pilot who disclosed his HIV-positive status to the Social Security Administration to receive medical benefits.[49] However, he withheld this information from the Federal Aviation Administration ("FAA"), and the Social Security Administration turned in his medical records to the FAA which in turn revoked his license.[50] He filed suit under the Privacy Act for the violation of his privacy for privacy harms including emotional distress resulting from the mishandling of his medical records when his HIV status was disclosed without his consent.[51] The Ninth Circuit had reasoned that under the Privacy Act, a plaintiff is permitted to recover non-pecuniary damages because the mental distress or emotional harm is sufficient to constitute an adverse effect.[52] With this construction of the provisions of the Act, the plaintiff would be allowed to establish standing for an injury that results in nonpecuniary harm, but that would not grant the claimant to pursue actual damages as such non-pecuniary injury would "frustrate the intent of Congress."[53] However, the Supreme Court overturned the Ninth Circuit's decision and held that the Privacy Act does not provide for compensation for nonpecuniary injuries such as mental or emotional distress.[54]

The case of *Doe v. Chao* demonstrates how the harm requirement further frustrates the enforcement mechanisms of statutes even when the legislative intent appears to be clear.[55] Here, a group of plaintiffs sued the Department of Labor for violating the Privacy Act of 1974.[56] The department published records

43. *Id.* at 810.
44. 18 U.S.C. § 2520(c)(1)(B).
45. 18 U.S.C. § 2710; 47 U.S.C. § 227(b)(3).
46. Citron & Solove, *supra* note 42, at 810–13.
47. *Id.* at 789; Fed. Aviation Admin. v. Cooper (*Cooper II*), 566 U.S. 284, 290–94 (2012).
48. *Cooper II*, 566 U.S. at 289–90.
49. *Id.* at 287–88.
50. *Id.* at 288.
51. *Id.* at 289.
52. Cooper v. Fed. Aviation Admin. (*Cooper I*), 622 F.3d 1016, 1030–31 (9th Cir. 2010).
53. *Id*.
54. *Cooper II*, 566 U.S. at 302.
55. Citron & Solove, *supra* note 42, at 798.
56. Doe v. Chao, 540 U.S. 614, 616–17 (2004).

of a group of miners that included their compensation claims, social security numbers, and their case numbers.[57] In this case, Doe claimed damages for emotional distress resulting from the disclosure.[58] Agreeing with the Fourth Circuit, the Supreme Court decided that an actual injury was required for Doe to receive the statutory minimum damages and that he had not met the harm requirement.[59]

The legislative history of the Privacy Act of 1974 may offer guidance on the legislative intent of Congress in providing the private right of action. The Privacy Act was enacted *inter alia*, to curb the illegal surveillance and investigation of private individuals by federal agencies.[60] The purpose of the Act is broadly stated as to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted privacy invasions stemming from federal agencies' collection, maintenance, use, and disclosure of personal information.[61]

Congress was concerned with the possible violations that would likely emanate from the increased use of computers in storing and retrieval of personal information.[62] Furthermore, the legislative history of the Act, more specifically the introductory remarks of Senator Sam J. Ervin, Jr. when he was presenting the 1974 Privacy Bill, offers an understanding of Congress' intention in enacting the Privacy Act.[63] Senator Ervin remarked that "[w]e must act now to create safeguards against the present and potential abuse of information about people."[64]

Even in the face of Congress' efforts in legislating on privacy and providing for the private right of action and the attendant statutory damages, Article III standing's injury-in-fact requirement appears to be at odds with these Act's enforcement mechanisms.[65] The Privacy Act provides for civil judicial enforcement by individuals affected by the violations of the Act.[66] True to the legislative intent, the Act provides for two causes of action by providing injunctive reprieve in the first place.[67] The remaining causes of action provide for compensatory reprieve and these appear in the shape of monetary damages lawsuits.[68]

---

57. *Id*.
58. *Id.* at 617–18.
59. *Id*.
60. COMM. ON GOV'T OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 6 (Comm. Print 1974) [hereinafter *Legislative History of the Privacy Act of 1974*].
61. *Id.* at 15–16.
62. *Id.* at 6.
63. *Id.* at 3–6.
64. *Id*.
65. *See* Wright v. United States, No. 4:17-CV-02101-KOB, 2018 WL 4854037, at *9 (N.D. Ala. Oct. 5, 2018) (dismissing Privacy Act claims because the plaintiff did not satisfy standing requirements due to lack of particularized injury in fact after the loss of personal information); Senne v. Vill. of Palatine, 784 F.3d 444, 445, 448 (7th Cir. 2015) (holding that a plaintiff could not demonstrate injury under the Driver's Privacy Protection Act after an officer issued the plaintiff a parking ticket with the driver's information on the ticket).
66. 5 U.S.C. § 552a(g)(1).
67. *Id.* § 552a(g)(3)(A).
68. *Id.* § 552a(g)(4).

What is odd is that even in the presence of clear legislative intent, the Supreme Court continues to hold that the statutory damages provision in the Privacy Act can only be available when the plaintiff demonstrates actual damages.[69] The Court's interpretation of the Privacy Act demands that "actual damages" are limited to pecuniary or economic harm.[70] Such an interpretation negates intangible harms, including emotional distress anxiety and other "injury to the feelings" of the privacy violation victims.[71]

Courts' strict requirement of injury-in-fact under the Article III standing doctrine appears to be standing in the way of the efforts Congress efforts to enforcement of privacy laws. The Supreme Court's instruction when assessing what constitutes injury-in-fact is that even when Congress creates a private right of action for statutory violations, plaintiffs must show concrete and particularized harm to satisfy the injury-in-fact requirement of Article III standing.[72] The Court, while referring to the *Lujan v. Defenders of Wildlife*[73] case stated that:

> [W]e said in *Lujan* that Congress may "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." . . . "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before."[74]

With the above statement, there is an acknowledgment that Congress can define concrete injury. However, the Court said that Congress' definition and prescription of injury "does not mean that a plaintiff automatically satisfies the injury-in-fact requirement" even when the statute says so.[75] The claimant has to satisfy the injury-in-fact requirement even when a statute grants a person a statutory right and appears to allow that person to sue to vindicate that right.[76] Article III standing requires a concrete injury regardless of the context of the violation—that is, the requirement is the same be it a statutory violation or not.[77]

The net effect is that even when Congress attempts to enforce privacy laws through the provision of the private right of action in various statutes, the threshold is not met. The doctrine of Article III standing and its strict injury requirement creates a judicial barrier that practically hinders the enforcement of

69. *See* Doe v. Chao, 540 U.S. 614, 624–25 (2004) ("[A]n individual subjected to an adverse effect has injury enough to open the courthouse door, but without more has no cause of action for damages under the Privacy Act.").

70. *Id.* at 625–26; Fed. Aviation Admin. v. Cooper (*Cooper II*), 566 U.S. 284, 299 (2012).

71. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 769–74 (2018) (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197 (1890)) (explaining how data breaches create a risk of future injury of identity theft or fraud and that these breaches may cause victims to experience anxiety about such risk). Injury to feelings is an attribute of an inviolate personality that makes us human in a free society. *Id.* at 769.

72. Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016) (determining that even when Congress creates a private right of action for statutory violations, plaintiffs must show concrete and particularized harm to satisfy the injury in fact requirement of Article III standing).

73. *Id.*

74. *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S 555, 580 (1992)).

75. *Id.*

76. *Id.* at 340–41.

77. *Id.*

privacy laws that should apply to all species of privacy harms, whether "concrete" or not.[78] By their very nature, privacy harms result in injury to feelings and sensibilities as well as more tangible human interests.[79] Privacy is a derivative right and embodies the values of what civilized and democratic societies, like the United States, strive to achieve including people's freedom, equality, and the pursuit of happiness.[80] Privacy is a key component of society and is valuable in shaping people's capacity to think independently in a bid to make different choices in life.[81] Therefore, the value of privacy cannot only be limited to actual harm given the intangible nature and attributes of privacy.[82] None of the positive individual and societal values and aspirations explained above can exist without the notion of privacy. Unfortunately, privacy, like any other attributes and aspirations of a free and democratic society, can easily be treasured when it no longer exists.[83]

B. Standing Doctrine and the Role of "Injury-in-Fact"

The standing doctrine has turned into a creed upon which any federal litigation in the U.S. federal courts must be premised.[84] As the Supreme Court put it: "[n]o concrete harm, no standing."[85] Therefore, federal courts have no business with any litigant if the strict Article III standing threshold is not satisfied. Courts have stated that an "asserted informational injury that causes no adverse effects cannot satisfy Article III."[86] Understanding the implications of the standing doctrine and its role in privacy litigation is key.

1. Progression of the Modern Standing Doctrine

As discussed earlier, standing is a doctrine that implements the "cases" and "controversies" provision in Article III of the U.S. Constitution.[87] Federal courts may hear a dispute only if the plaintiff has standing—that is if the plaintiff has shown that they have suffered injury that is "'fairly traceable' to the actions of

78. *See supra* notes 65–71 and accompanying text (explaining the impact a strict application of the Article III standing doctrine has on privacy laws); *see also* Spokeo, Inc. v. Robins, 578 U.S. 330, 337–42 (2016) (explaining the concrete requirement for showing injury-in-fact).

79. Solove & Citron, *supra* note 71, at 768–69.

80. *See* Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 845 (2013) ("Privacy is indeed valuable for democratic societies like ours, in which people need the capacity to think and act independently.").

81. *Id.*

82. *See id.* (explaining the importance of privacy for a functioning democratic society). *But see* Rudgayzer v. Yahoo! Inc., No. 5:12-cv-01399, 2012 WL 5471149, at *6 (N.D. Cal. Nov. 9, 2012) (holding that "[m]ere disclosure of [personal] information in and of itself, without a showing of actual harm, is insufficient" to support a breach of contract claim).

83. *See supra* notes 75–82 and accompanying text (describing the benefits of privacy and how the Article III standing requirement may prevent some of those benefits from actualizing).

84. *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021) ("To have Article III standing to sue in federal court, plaintiffs must demonstrate, among other things, that they suffered a concrete harm.").

85. *Id.*

86. Trichell v. Midland Credit Mgmt., Inc., 964 F.3d 990, 1004 (11th Cir. 2020).

87. U.S. CONST. art. III, § 2. Other doctrines under this constitutional provision include ripeness, mootness, and the restriction on hearing political questions. DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 352 (2006).

the defendant, and that the injury will likely be 'redressed by a favorable [court] decision.'"[88] Federal courts have set these requirements as a threshold for satisfying Article III standing as a jurisdictional requirement.[89]

In order to have standing, a plaintiff must have suffered an "injury in fact."[90] That injury must be "distinct," "palpable," and "concrete,"[91] and it must have occurred or been imminent.[92] In highlighting the injury requirement, the Supreme Court has emphasized that the injury must be "actual or imminent, not conjectural or hypothetical."[93] The injury must also be "fairly traceable" to the actions of the defendant, and it must be susceptible to be "redressed by a favorable decision."[94] These standing requirements apply in all types of suits brought in federal court.[95] If a plaintiff fails to meet these requirements, the federal court must dismiss the case for lack of jurisdiction.[96] It should be noted that state courts are not generally bound by the Article III standing requirement.[97]

The Supreme Court has stated that the standing doctrine is constructed on the principles of the separation of powers.[98] These principles ensure that the courts do not usurp the role of the other branches of government by confining the judicial power to resolving disputes that were "traditionally amenable to and resolved by the judicial process."[99] The Supreme Court has stated that the traditional role of courts is to resolve the rights of individuals, and the injury-in-fact test as dictated by Article III standing enables courts to serve that role by acting only when necessary to remedy individual injuries.[100]

88. Bennett v. Spear, 520 U.S. 154, 162 (1997) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992)).

89. Robert J. Pushaw Jr., *Article III's Case/Controversy Distinction and the Dual Functions of Federal Courts*, 69 NOTRE DAME L. REV. 447, 512–17 (1994).

90. *Lujan*, 504 U.S at 560.

91. Allen v. Wright, 468 U.S. 737, 751, 756 (1984).

92. Summers v. Earth Island Inst., 555 U.S. 488, 492 (2009).

93. Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc., 528 U.S. 167, 180 (2000).

94. *Lujan*, 504 U.S at 560–61.

95. *Id.* (qualifying Article III standing as "the irreducible constitutional minimum" for lawsuits).

96. *See Friends of the Earth, Inc.*, 528 U.S. at 168 ("[The] [c]ourt has an obligation to assure itself that [plaintiff] had Article III standing at the outset of the litigation.").

97. Peter N. Salib & David K. Suska, *The Federal-State Standing Gap: How to Enforce Federal Law in Federal Court Without Article III Standing*, 26 WM. & MARY BILL RTS. J. 1155, 1160 (2018) ("State courts are not subject to Article III and its standing requirement."); ASARCO Inc. v. Kadish, 490 U.S. 605, 617 (1989) ("We have recognized often that the constraints of Article III do not apply to state courts, and accordingly the state courts are not bound by the limitations of a case or controversy . . . .").

98. 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."); *see also* Summers v. Earth Island Inst., 555 U.S. 488, 492–93 (2009) ("[Standing] is founded in concern about the proper—and properly limited—role of the courts in a democratic society.") (internal quotations and citations omitted); Allen v. Wright, 468 U.S. 737, 752 (1984) ("[S]tanding is built on a single basic idea—the idea of separation of powers.").

99. Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 102 (1998).

100. *See Lujan*, 504 U.S. at 577 ("[U]nder Article III, Congress established courts to adjudicate cases and controversies as to claims of infringement of individual rights whether by unlawful action of private persons or by the exertion of unauthorized administrative power.") (internal quotations and citations omitted).

a. Historical developments of the doctrine of standing

From a historical perspective, standing was not always a jurisdictional principle necessary for protection of the separation of powers doctrine. It was not deemed to have this role during the first 150 years of U.S. independence.[101] The federal courts' power to hear a dispute was dependent on whether the plaintiff invoked the proper form of action.[102] When courts determined that a plaintiff lacked standing, the use of the term was about the fact that the plaintiff did not present a remedial interest—it did not implicate Article III.[103] Standing was a determination on the merits of the plaintiff's claim.[104] The court's resolution of no standing implied that the plaintiff had failed to state a cause of action under which he was entitled to relief.[105] The situation changed between the 1950s and 1970s, when federal courts were perceived as giving an easy ride to plaintiffs in satisfying the standing requirement.[106] The court established the standing doctrine under Article III in the twentieth century to limit an individual's ability to question government actions and policies.[107]

b. The narrowing definition of privacy harms in the standing inquiry

In recent years, the Supreme Court has concluded that extensive standing threatened the doctrine of separation of powers because it allowed persons to approach the court with matters which would be more appropriately addressed by the legislative branch of government.[108] This approach has seriously narrowed the category of injuries that may suffice data privacy litigation, specifically in the standing inquiry.[109] To this extent, courts have stated that standing cannot be based on generalized grievances, for example, an individual's injury resulting from the government's presumed illegal expenditure of taxes or on some uneasiness felt by the government's omission to enforce a given law.[110]

Satisfaction of the standing requirement operates as the standard mandatory requirement for a plaintiff to invoke the jurisdiction of the federal

101. F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 290–91 (2008) ("Standing first flourished as an independent doctrine in the early 1900s.").

102. *See* Osborn v. Bank of the U.S., 22 U.S. 738, 819 (1824) (explaining that the judiciary rules only when a plaintiff asserts their rights, "[i]t then becomes a case, and the constitution declares, that the judicial power shall extend to all cases arising under the constitution, laws, and treaties of the United States").

103. Steven L. Winter, *The Metaphor of Standing and the Problem of Self-Governance*, 4 STAN. L. REV. 1371, 1424 (1988).

104. *Id.* at 1425.

105. *Id.*

106. Michael E. Solimine, *Congress, Separation of Powers, and Standing*, 59 CASE W. RSRV. L. REV. 1023, 1027–28 (2009).

107. *See* Robert J. Pushaw, Jr., *Justiciability and Separation of Powers: A Neo-Federalist Approach*, 81 CORNELL L. REV. 393, 458–59 (1996) ("For example, the Court embraced the Brandeisian strategy of invoking justiciability to shield progressive legislation from conservative substantive due process challenges.").

108. Heather Elliot, *The Functions of Standing*, 61 STAN. L. REV. 459, 460–62 (2008).

109. *See, e.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330, 342–43 (2016) (holding that the standing requirement must be satisfied even when Congress explicitly provides for a private cause of action when a privacy statute is violated).

110. Elliot, *supra* note 108, at 479–80.

courts.[111] The standing inquiry being hinged on the existence of an injury-in-fact serves to distinguish standing from the merits. Whether a plaintiff has suffered factual injury does not involve adjudication of their legal rights.[112] The question is whether the plaintiff suffered factual harm.

2. Standing and its Application in Privacy Litigation

We will now examine the leading cases as decided by the Supreme Court that have shaped the current jurisprudence of privacy litigation in the face of data privacy injuries requirement under Article III standing. The cases discussed in this part are (a) *Clapper v. Amnesty International USA*;[113] (b) *Spokeo v. Robins*;[114] and (c) *TransUnion v. Ramirez*.[115]

a. *Clapper v. Amnesty International USA* conception of Article III standing

In this case, the plaintiffs challenged the provisions of Section 702 of the Foreign Intelligence Surveillance Act ("FISA").[116] The plaintiffs argued that the provision creates new procedures for authorizing government electronic surveillance and that they were being forced to take costly measures to ensure the confidentiality of their international communications.[117] Writing for the majority, Justice Alito[118] determined that the plaintiffs did not have standing under Article III because no injury-in-fact had occurred to them.[119] The Court stated that the plaintiffs' asserted harm was too speculative to satisfy the injury-in-fact requirement.[120] The injury must be imminent to be cognizable, and that meant it had to be "certainly impending."[121]

b. *Spokeo v. Robins* conception of Article III standing

Through *Spokeo*, the Supreme Court demonstrated the nature of an injury that is sufficient to satisfy the standing requirement in a privacy case.[122] The plaintiff sued Spokeo, a site providing information on people's backgrounds, for violating the Fair Credit Reporting Act ("FCRA"), which requires firms to take

111. *See* Whitmore v. Arkansas, 495 U.S. 149, 154–55 (1990) ("Article III, of course, gives the federal courts jurisdiction over only 'cases and controversies,' and the doctrine of standing serves to identify those disputes which are appropriately resolved through the judicial process.") (internal quotations and citations omitted).

112. *See id.* ("Our threshold inquiry into standing 'in no way depends on the merits of the [petitioner's] contention that particular conduct is illegal . . . .'") (internal quotations and citations omitted).

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

114. Spokeo, Inc. v. Robins, 578 U.S. 330 (2016).

115. TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021).

116. *Clapper*, 568 U.S. at 401.

117. *Id.* at 401–02.

118. *Id.* at 401.

119. *Id.* at 401–02.

120. *Id.*

121. *Id.*

122. Spokeo, Inc. v. Robins, 578 U.S. 330, 333–34 (2016).

reasonable steps to ensure the accuracy of the data they hold.[123] The defendant had published incorrect information about the plaintiff.[124] Robins argued that the errors hurt his employment chances by representing that: (1) he was overqualified for the positions he applied for, or (2) that he might not be able to relocate to job sites because he had a family.[125]

The district court held that while Robins correctly sued under the FCRA's provision providing a private right of action, he did not demonstrate how the erroneous information included in the credit report satisfied the injury-in-fact requirement under Article III.[126] On appeal to the Supreme Court, it was emphasized that even when Congress creates a private right of action for statutory violations, the plaintiff must show concrete and particularized injury as required by the injury-in-fact requirement under Article III.[127]

c. *TransUnion v. Ramirez* conception of Article III standing

Just like *Spokeo*, *TransUnion* considered Article III standing in the context of the FCRA.[128] *TransUnion* was aimed at curing *Spokeo*'s vagueness.[129] In this case, the court concluded: "[n]o concrete harm, no standing."[130] *TransUnion* was a class action in which the plaintiff class received credit reports that falsely labeled them as probable terrorists or drug traffickers.[131]

Writing for the Court, Justice Kavanaugh held that class members whose false credit reports were not distributed to third parties did not possess Article III standing.[132] They did not suffer concrete injury as required by Article III standing requirement.[133] Interestingly, the Court stated that if the judicial and legislative branches disagree as to whether harm merits redress, it is the legislative branch that must bow.[134] This runs counter to the stated reasons for the Court's strict adherence to Article III standing—the respect of separation of powers.[135]

In contextualizing the above-discussed cases, privacy violation victims must not only allege an invasion of their privacy rights, but also that such invasion caused enough damage to satisfy a judge that a case merits adjudication

123. *Id.* at 333–35.
124. *Id.* at 336.
125. *Id.* at 350 (Ginsburg, J., dissenting).
126. *Id.* at 336.
127. *Id.* at 339.
128. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2202 (2021).
129. *See* Jacob Phillips, TransUnion, *Article III, and Expanding the Judicial Role*, 23 FEDERALIST SOC'Y REV. 186, 196 (2022) ("Though *Spokeo*'s vagueness permitted jurisprudential divergence, *TransUnion* does not.").
130. *TransUnion*, 141 S. Ct. at 2214.
131. *Id.* at 2101–02.
132. *Id.* at 2214.
133. *Id.*
134. *See id.* at 2205 ("Congress's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III . . . .").
135. *See* 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.").

as per the Article III injury-in-fact requirement.[136] This approach leaves out victims of privacy harms who suffer injuries that have not been accepted by courts, including psychological harms in the form of emotional distress among others.[137]

These cases clearly show that, although at common law, the invasion of a privacy right was by itself sufficient to establish jurisdiction. At least as it pertains to statutory private rights, that is no longer the case.[138] In such contexts, litigants must now allege and eventually show not only an invasion of their privacy rights, but also that such invasion caused enough damage to show the judge that a case merits adjudication as per the Article III injury-in-fact requirement.[139] This requirement is regardless of whether a violation occurred or not.[140]

II. EMPIRICALLY MAPPING THE ROLE OF THE STANDING DOCTRINE IN PRIVACY ENFORCEMENT

Research on data privacy litigation is a quickly emerging topic.[141] However, there is a dearth of empirical investigations that have been undertaken to appreciate the litigation landscape in this area of the law. Classic studies of this area of the law have concentrated on the normative and doctrinal aspects, with little to no emphasis on the empirical aspects.[142] Researchers have explored the critical questions that emerge from data privacy violations and the ensuing litigation questions that emerge therefrom.[143] Some studies in this area have interrogated the injury question as required by the federal courts, especially from a normative perspective.[144] However, as noted in the subsequent part, there is no empirical study that has comprehensively studied the body of cases, as filed in the federal courts spanning 20 years, in order to understand the state of events.[145] This study will use empirical legal methods to understand the landscape of how courts have handled data privacy violations.

136. *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 337–42 (2016) (discussing how an injury that is sufficient to satisfy the standing requirement in a privacy case must show concrete and particularized injury, as required by the injury-in-fact requirement under Article III).

137. Solove & Citron, *supra* note 71, at 746.

138. The federal courts have yet to address whether common law legal injuries of breach of contract, which data privacy law litigants raise, present no factual injury, where the plaintiff would have been entitled to nominal damages. Perhaps an analysis should be done on how the courts apply Article III's standing-factual injury requirement of common law causes of action as compared to statutory causes of action to see if there is a difference in application and outcome.

139. *Spokeo*, 578 U.S. at 337–42.

140. *Id.* at 352.

141. Solove & Citron, *supra* note 71, at 747; Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 361 (2014); Thomas D. Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193, 1194–95 (2020).

142. *See* Solove & Citron, *supra* note 71, at 745 ("In this Article, we focus on data-breach harms. We explore why courts have struggled with the issue, and we offer an approach to address data-breach harms that has roots in existing law.").

143. *Id.* at 745–46.

144. *See id.* at 737–38 (explaining the issue with the Supreme Court's current standing jurisprudence as applied to privacy claims).

145. *See infra* Section II.A (discussing previous studies on cases adjudicating privacy violation claims).

A. Previous Studies

As previously noted, past scholarship in the area of data privacy litigation have long speculated that the standing doctrine could create a barrier for the enforcement of privacy laws.[146]

Solove and Citron proposed the notion of data breach harm: risk and anxiety for those individuals whose information has been compromised by a data breach.[147] The risk and anxiety from the exposure of data subjects' information to bad actors who may use that information leading to injuries could include (1) the cost of fraudulent transactions passed onto the data subject, (2) increased risk of future identity theft resulting from a breach, and (3) the burden of closing affected accounts and opening new ones.[148]

While considering the issue of harm in privacy litigation, Ryan Calo[149] observes that the requirement of harm presents an especially grave challenge. In the context of privacy, courts demand that the plaintiff demonstrate "not just harm, but concrete, fundamental, or 'special' harm before" the court grants any redress.[150]

Thomas D. Haley investigated the precedential influence of the *Clapper v. Amnesty International*[151] case in data privacy litigation.[152] He states that "probabilistic standing is at the heart of much data-protection litigation."[153] He concludes that there is heavy reliance on the *Clapper* decision in determining standing, yet it has little application to issues posed by data privacy violation cases.[154] His study further observes that "federal courts get standing wrong . . . by focusing on the particular scraps of information collected or lost via data breach to find plaintiffs have not suffered an 'injury in fact.'"[155]

While there have been previous studies by eminent scholars on the question of privacy harms in data privacy litigation, to our knowledge, this is the first comprehensive study examining the problem from an empirical perspective by leveraging over a thousand hand-coded federal court opinions. Previous studies examined various data privacy violations and the existing legal procedural substantive impediments that complicate the enforcement of privacy via litigation.[156] However, these studies were devoid of an examination of the existing challenge in empirical terms. The findings of this study paint a numerical picture from which several inferences may be drawn to address the problem. Credit is due to existing scholarship, as their theories and expositions were instrumental in informing and shaping the foundation upon which the

146. *See* Solove & Citron, *supra* note 71, at 748–49 (discussing the frequent early dismissals in privacy litigations due to a lack of standing).
147. *Id.* at 774.
148. *Id.* at 773–74.
149. Calo, *supra* note 141, at 361.
150. *Id*. (quoting Doe v. Individuals, 561 F. Supp. 2d 249, 257 (D. Conn. 2008)).
151. Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
152. Haley, *supra* note 141, at 1198.
153. *Id.* at 1202.
154. *Id.* at 1220, 1227.
155. *Id.* at 1193.
156. *Supra* notes 147–55 and accompanying text.

research questions of this empirical study were developed. Most importantly, the previous studies were authoritative in developing a systematic research methodology as espoused in the next part.[157]

B. Methodology of the Study

This study was created to answer the question of whether (and if so, how) standing doctrine interacts with federal privacy law. The study was conducted through various phases that were largely informed by the existing scholarly literature on data privacy harms. One of its chief contributions, however, was that it looks at all federal privacy claims over a 20-year period. For purposes of this research, the word "data" is inclusive of personal information that is personally identifiable information ("PII").[158] This is specifically for information on the natural person as differentiated from legal persons. This research is based on data that were collected from federal courts' docket reports that were accessed through the U.S. Public Access to Court Electronic Records ("PACER") service. PACER provides electronic public access to and retrieval of federal court records.[159] PACER docket reports were accessed using the Bloomberg Law database.[160]

Bloomberg Law was used to access PACER because it provides links to all cases from all federal courts under one system under set parameters, whereas PACER used by itself provides service access to individual court sites.[161] For purposes of this research, the collected data were concerning privacy litigation information on data harms across the U.S. federal courts. The data collection process was undertaken through systematic consecutive phases explained below.

157. *Infra* Section II.B.

158. *See generally* John M.M. Rumbold & Barbara K. Pierscionek, *What are Data? A Categorization of the Data Sensitivity Spectrum*, 12 BIG DATA RSCH. 49, 53–55 (2018) (detailing the various levels of sensitivity of personal data, wherein data on healthcare, genetics, and occupation are the most sensitive).

159. PUB. ACCESS TO CT. ELEC. RECS., https://pacer.uscourts.gov/ [https://perma.cc/546L-294Q] (last visited Sept. 21, 2023); Bobbie Joshnson, *Recap: Cracking Open US Courtrooms*, GUARDIAN (Nov. 11, 2009, 15:45 PM), https://www.theguardian.com/technology/2009/nov/11/recap-us-courtrooms [https.perma.cc/2MPB-QW45].

160. PACER includes information on each court-filed or appealed case, including the list of parties involved in a case, the chronology of the court's process, and all filed court documents on a case up to the opinion of the court. The study used PACER as the service that would give access to the original documents as filed by the parties as reflected in the docket files. PACER service provides access to court documents on a court-by-court basis; that is, if a researcher wants opinions of all the circuit courts, they would have to retrieve them by searching one circuit after the other. However, commercial law databases like Westlaw Edge, Lexis, and Bloomberg Law can provide access to all opinions in all courts at one go as per the researcher's set search query. The study used Bloomberg Law as it provides access to PACER service and provides court dockets, unlike other commercial databases. Electronic records provided by Bloomberg Law include links to copies of documents filed in a case, such as a complaint, the answer, motions, and briefs, up to the last opinion of the court depending on the stage at which the case is.

161. Using Bloomberg Law meant that we did not have to search each individual federal court to have access to all the cases of interest. Bloomberg's tools enabled us to get access to the pool of our cases of interest at one go.

1. Phase 1—Selecting search terms and phrases

The first phase consisted of selecting search terms and phrases from court decisions, scholarly works, and commentaries that use different words and phrases in describing issues around data privacy litigation and the question of privacy harm.[162] To understand and assemble different words and phrases used in describing the issue at hand (data privacy injury as required by Article III standing), the most cross-cited federal opinions as discussed in scholarly literature and commentaries were carefully studied.[163] This activity was undertaken through a purposeful study of scholarly literature and commentaries.[164] Every individual court opinion was investigated from start to finish, starting from its complaint to the final court's opinion. Any other supporting documents, as filed by the parties, were also examined. After surveying and scrutinizing different federal court opinions with the filed documents under each case, the frequently used terms and phrases included the following: "injury," "harm," "data privacy," "information privacy," "data injury," "data harms," "data privacy injury," "data privacy harm," "data breach," "data misuse," "data privacy violations," "data violation," "information privacy," and "standing."

2. Phase 2—Database selection and search query formulation

In the second phase, while laying a foundation for the whole study, a pilot study was first conducted with the subsequent methodology and results presented to a committee of subject experts for review. The pilot study used Westlaw Edge to access a pool of cases. 10% of the cases were studied, coded, and eventually analyzed. Upon presenting the results from the pilot study to experts, including Professor Anita Allen,[165] their assessment confirmed the

---

162. "Data privacy" is interchangeably referred to as "information privacy." Nonetheless, they both mean the responsible handling of sensitive PII and confidential information such as business information and intellectual data. This paper, however, investigates litigation concerning the information of a personal nature.

163. The following scholarly literature were carefully studied: Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 315 (2019); Ignacio N. N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1044–46 (2018); Matthew S. DeLuca, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2443–46 (2018); Cobun Keegan & Calli Schroeder, *Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms*, 15 J.L. ECON. & POL'Y 19, 22–25 (2019); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C.L. REV. 93, 95–105 (2014); Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 141–48 (2019); Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 J. L. & POL'Y INFO. SOC'Y 485, 496–500 (2015); Gilman & Green, *supra* note 22, at 256–60; Max Roser et al., *Technological Change*, OUR WORLD IN DATA, https://ourworldindata.org/technology-adoption [https://perma.cc/2BWW-TVMN] (last visited Feb. 1, 2023).

164. Sources cited *supra* note 163. The following cases were also carefully studied: Spokeo, Inc. v. Robins, 578 U.S. 330 (2016); Doe v. Chao, 540 U.S. 614 (2004); TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); Fed. Aviation Admin. v. Cooper (*Cooper II*), 566 U.S. 284 (2012); Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134 (2011); Lambert v. Hartman, 517 F.3d 433, 438 (6th Cir. 2008) (citing Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 261 (1977)); Remijas v. Neiman Marcus Grp., 794 F.3d 688 (7th Cir. 2015); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

165. *Anita L. Allen*, PENN CAREY L., law.upenn.edu/faculty/aallen2 [https://perma.cc/M8DD-DMNA] ("[Anita] Allen is internationally renowned as an expert on philosophical dimensions of privacy and data protection law, ethics, bioethics, legal philosophy, women's rights, and diversity in higher education.").

viability of the study and the proposed methodology. The committee further advised that the final study encompass an assessment of the complete body of data privacy cases filed in the U.S Federal courts between 2000 and 2020. The selected timeframe of the study, spanning from 2000 to 2020, holds particular significance due to the rapid advancements and widespread adoption of digital technology during this period.[166] This period registered rapid and widespread adoption of technology.[167] These advancements have resulted in an exponential increase in the collection, storage, and sharing of personal data.[168] The emergence of social media and wide usage of mobile devices, alongside other data-collecting technologies, have created unprecedented opportunities for data collection while simultaneously rendering individuals more susceptible to privacy violations.[169]

Furthermore, the period in question was marked by notable breaches that exposed sensitive personal information of a multitude of individuals.[170] Notable examples include the ChoicePoint data breach in 2007,[171] Target's breach in 2014,[172] and the Equifax data breach,[173] among others. Additionally, the latter half of the considered timeframe witnessed significant data breaches affecting technology leaders like Microsoft, Wattpad, and Meta/Facebook, among others.[174] These incidents garnered significant public attention, resulting in heightened awareness regarding the risks associated with data breaches and consequently contributing to a surge in the number of data privacy lawsuits filed.[175]

Therefore, the selected timeframe provides a comprehensive dataset for examining the impact and or influence of Article III injury-in-fact requirement on data privacy litigation. This takes into account the rapid technological advancements, increasing vulnerability of individuals, and the notable incidents

166. Alexander Hammond, *The 20 Biggest Advances in Tech Over the Last 20 Years*, FEE STORIES (Jan. 2, 2020), fee.org/article/the-20-biggest-advances-in-tech-over-the-last-20-years [https://perma.cc/B3U9-W4BC] (exploring the 20 most significant technological advancements from 2000 to 2020).

167. SOLOVE, *supra* note 1, at 3–4.

168. *Id.*

169. *Social Media Privacy*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/consumer-privacy/social-media-privacy/ [https://perma.cc/2J2R-YL8Z] (last visited Sept. 21, 2023) ("The massive stores of personal data that social media platforms collect and retain are vulnerable to hacking, scraping, and data breaches, particularly if platforms fail to institute critical security measures and access restrictions.").

170. *See infra* notes 171–75 and accompanying text (detailing several large data breaches in recent years).

171. Jon Brodkin, *ChoicePoint Details Data Breach Lessons*, NETWORK WORLD (June 11, 2007, 12:00 AM), https://www.networkworld.com/article/2291190/choicepoint-details-data-breach-lessons.html [https://perma.cc/JZY2-QY27].

172. Jim Finkle & David Henry, *Exclusive: Target Hackers Stole Encrypted Bank Pins - Source*, REUTERS (Dec. 24, 2013, 11:45 PM), https://www.reuters.com/article/us-target-databreach/exclusive-target-hackers-stole-encrypted-bank-pins-source-idUSBRE9BN0L220131225 [https://perma.cc/8FLH-F6J3].

173. Caitlin Kenny, *The Equifax Data Breach and the Resulting Legal Recourse*, 13 BROOK. J. CORP. FIN. & COM. L. 215, 222 (2018).

174. David Armillei et al., *Private Data Breach Litigation Comes of Age*, JD SUPRA (Oct. 14, 2022), https://www.jdsupra.com/legalnews/private-data-breach-litigation-comes-of-2442552 [https://perma.cc/Q985-2TNZ].

175. *See* David Basler et al., *INSIGHT: Data Breach Litigation Trends to Watch*, BLOOMBERG L. (Mar. 4, 2019, 3:01 AM), https://news.bloomberglaw.com/privacy-and-data-security/insight-data-breach-litigation-trends-to-watch [https://perma.cc/WA47-NAM5] ("Data breaches frequently make headlines and engender litigation brought by consumers and financial institutions, as well as regulatory enforcement actions.").

that have shaped public perception and legal action surrounding data privacy breaches.

The keywords and phrases identified in phase one were followed by crafting a comprehensive search query using Bloomberg Law search connectors. To ensure the query's robustness, multiple iterations were performed using several word and phrase combinations. From this activity, a final search string/query, believed to be all-inclusive, was formulated.[176] Additionally, distinct search strings were employed in Westlaw Edge and Lexis Advance to identify and minimize potential database-specific biases.[177] Notably, the data as separately retrieved from Westlaw Edge and Lexis Advance closely paralleled the results from Bloomberg Law.

Subsequently, with the search parameters established and the choice of database determined, the study's timeframe was delimited to the period spanning January 1, 2000, to December 31, 2020, using Bloomberg date filters. The twenty-year scope was selected due to the consistent and substantial growth within the information and communication technology ("ICT") sector during this timeframe.[178] The study exclusively focused on civil cases. Upon applying the search query and Bloomberg Law filters described above, this process yielded a population of 3,155 opinions for the period under consideration.[179]

3. Phase 3—Manual selection of opinions for coding

The third phase involved manual selection of opinions for coding. Once the processes and criteria in phase two had been undertaken, the next step was to identify a cohort of cases for eventual coding. This phase involved a manual investigation and careful review of all the filed documents for each of the 3,155 opinions, starting from the plaintiff's complaint to the court's final ruling. This first population of cases was subjected to this initial review to determine if an individual case was specifically about data privacy, and more so with specific consideration of personal information privacy. Cases that did not consider information privacy were also excluded from the final dataset.[180]

It should be noted that by default, the Bloomberg database organizes cases under different subject headings such as copyright, civil procedure, and

176. Search string used: privacy AND ("data breach" OR "data harm" OR "data injury" OR "data misuse" OR harm OR injury OR "data violat!" OR "data infring!" OR PII OR "personal identifiable information") AND (standing).

177. Each query was modified for each of the two databases. Each database has its specific way of how the connectors are specially used to suit their proprietary demands. *See* Ahmed E. Taha, *Data and Selection Bias: A Case Study*, 75 UMKC L. REV. 171, 173 (2006) (discussing publication bias within publication databases).

178. *See* Hubert Strauss & Besik Samkharadze, *ICT Capital and Productivity Growth*, 16 EIB PAPERS 8, 11 (2011). ("[T]he US has seen a striking increase in TFP [("total factor production")] growth after 2000 (the end of the ICT boom).").

179. This number of cases may as well be referred to as the "sample." Though the research sought to study and review the entire corpus of all federal cases on data privacy violations from 2000 to 2020, it cannot be said with great certainty that all the opinions over the years appeared in the dataset.

180. *See* Citron & Solove, *supra* note 42, at 796–97 (explaining the differences between information privacy and physical privacy, including the judicial treatment of the two).

technology among others.[181] A party may file a matter with different causes of action, with some minimally including data privacy matters. By Bloomberg's proprietary system, such a case is distributed under different subject headings, including privacy inclusive.[182] An omnibus inclusion of such cases in our data is misaligned. Overcoming this challenge would call for a systematic review of the entire dataset under different subject headings to decipher the cases that relate to the questions that we want to answer.

For this study, the questions of interest were only on individual information privacy violations and how federal courts resolve them in the face of the strict Article III injury requirement. The process was designated as the inclusion and exclusion criteria, albeit with set considerations and reasons, as explained and demonstrated in Appendix A.[183] Having undertaken the exclusion criteria as demonstrated, a total of 1,753 cases passed for the final cohort of cases for coding and eventual analysis.

4. Phase 4—Data collection and the code book

A cohort of 1,753 cases was subjected to a second detailed and purposeful manual review to extract information as per the variables of interest for our study. A codebook was developed with the details of where in the docket reports and the case files each variable of interest was to be extracted.[184] The codebook was reviewed periodically and revised to address unanticipated permutations in the coding process. Two coders undertook the process of manually extracting the information as per the set variables and observations. The coders constantly reviewed and double-checked each other's work to ensure consistency and accuracy.

For purposes of the study, the data collection process took the form of extracting information as per two schemes: descriptive information and content analysis information. Descriptive information is the information that is typically used to identify the case, key dates in the cases, and the different important players in the case including parties and judges. The content analysis coding scheme considered information as provided by the case and its attendant documents in the docket report for example the forum, cause of action, source of the law for the claim, and the court's opinion.[185] All 1,753 cases were systematically coded and double-checked by the two coders and were ready for analysis.

181. See *The Best Legal Research Database for All Your Needs*, BLOOMBERG L., https://pro.bloomberglaw.com/legal-research-database/ [https://perma.cc/9MCC-FVNV] (last visited Sept. 21, 2023) (explaining the benefits of using Bloomberg Law research tools).

182. *Id.*

183. Some cases falling under specific headings were excluded ("exclusion status") and others were included as they appeared in the original dataset ("inclusion status").

184. *See infra* Appendix A (explaining rationales of including or excluding cases based on terms used and statutes evaluated).

185. *See id.* (discussing variables used to determine inclusion and exclusion criteria).

III. RESULTS OF THE STUDY

The federal courts have addressed many disputes involving data privacy violations for the twenty years under consideration in this study (2000–2020).[186] This Section discusses how federal courts have addressed data privacy, focusing particularly on the role and use of standing doctrine within privacy cases. As it shall explain, these results show that standing is explicitly addressed in most (80%) of federal standing cases and that the doctrine of injury-in-fact alone causes the majority of privacy protection cases (almost 60%) to fail. This evidence shows for the first time the full extent of the impact of courts' interpretations of Article III standing requirements on the function of federal privacy laws.

A. Results of the Outcome of the Standing Inquiry

Standing outcome is defined as how often the defendants raised standing issues under the Article III cognizable injury requirements and the Court's consideration of the same. This part of the analysis will examine the outcomes on motions of standing as raised by the defendants. The results below show how courts have been fairing in answering the question of injury under the standing doctrine.

1. What is the frequency at which the standing motion is raised within the context of data privacy litigation?

Defendants often use the Article III standing motion as the first line of defense in data privacy litigation.[187] This is because a plaintiff's failure to prove harm is as good as a silver-bullet defense that is available to defendants in the federal courts.[188] For this reason, this part investigates how often defendants raised the standing motion in data privacy litigation cases.

The data show that 80% of the defendants raised Article III constitutional standing motions in data violation cases.[189] In effect, the defendants moved to dismiss the claimant because they could not satisfy the strict interpretation of Article III's injury-in-fact requirement.[190] The requirement is that federal courts may hear a dispute only if the plaintiff has standing—that is if the plaintiff has shown that they have suffered an injury that is "'fairly traceable' to the actions of the defendant, and that the injury will likely be redressed by a favorable decision" from the court.[191]

186. *Supra* Section II.B.4. (finding 1,753 cases were appropriate for this study).

187. *Infra* note 189.

188. *See* Warth v. Seldin, 422 U.S. 490, 498 (1975) ("In essence the question of standing is whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues.").

189. The 80% rate appears high. However, by the time of writing these results, there was no research to show how other areas of the law fair as to how often objections of Article III standing are raised by the defendants.

190. *See, e.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016) (explaining that the constitutional minimum of standing demands that the plaintiff suffered an injury in fact).

191. Bennett v. Spear, 520 U.S. 154, 162 (1997) (quoting Lujan v. Defs. of Wildlife, 504 U.S 555, 560–61 (1992)).

The specific patterns that trigger the defense of Article III standing vary depending on the context and specific circumstances. For example, cases that involved identity theft or fraud had a higher rate at which the defendants raised the standing defense.[192] "When an individual's personal information is stolen, there is no guarantee that it will be used fraudulently."[193] Only 2% of stolen credit card information from data breaches is subject to misuse. Of all identity theft reports, only 1.5 to 4% are the result of stolen credit card information. "This probability goes down even further when the volume of personal information is large—since identity thieves can only make use of a small number of accounts."[194] The argument often raised by defendants is that there was no immediate injury to the plaintiffs and hence their claims are merely speculative. For example, in *Blahous v. Sarrell Regional Dental Center for Public Health*, the federal court dismissed the lawsuit against the defendant, which exposed the personal information of over 10,000 patients.[195] The court found that the plaintiffs did not have standing to sue, as they had not suffered any concrete harms as a consequence of the data breach.[196] The court emphasized that the plaintiffs were not likely to suffer any future harm, as there was no evidence that any of the plaintiffs had been a victim of identity theft or fraud.[197]

In class action lawsuits, it is common for defendants, particularly technology companies, to raise the Article III standing defense.[198] This defense is often invoked due to the requirement in class actions that each plaintiff show that they have suffered similar injuries because of the defendant's conduct.[199] Defendants rely on this defense for various reasons, including the need to establish a commonality of harm among the plaintiffs, as a result of the alleged defendant's conduct.[200] This can be difficult to do, especially in data privacy cases where the plaintiff's injuries are intangible, such as emotional distress. For example, in In re *Facebook*, the plaintiffs alleged that their privacy rights had been violated by collecting and storing their personal information without their consent.[201] The court denied the motion for class certification under a finding that some plaintiffs alleged that they had been the victim of identity theft, while others alleged that they had been harassed or discriminated against.[202]

Defendants commonly exploit the strict first-hand tool of standing, which is at their disposal to frustrate the plaintiffs' efforts to seek court redress when

192. *See generally* Jacob W. Schneider, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 B.U.J. SCI. & TECH. L. 279, 281–82, 287–88 (2009) (explaining that the risk of identity theft has grown annually at a rapid rate, but there it is not certain that stolen identity will be used fraudulently).

193. *Id*. 287–88.

194. *Id*. at 288.

195. Blahous v. Sarrell Reg'l Dental Ctr. for Pub. Health, No. 2:19-cv-798-RAH-SMD, 2020 WL 4016246, at *8 (M.D. Ala. July 16, 2020).

196. *Id.* at *7.

197. *Id*. at *6, *8.

198. IAN C. BALLON, E-COMMERCE AND INTERNET LAW: LEGAL TREATISE WITH FORMS § 26.15 (2d ed. 2019).

199. *Id.*; FED. R. CIV. P. 23(a)(3).

200. BALLON, *supra* note 198, § 26.15 n.225.

201. *In re* Facebook, Inc. Secs. Litig., 405 F. Supp. 3d 809, 820 (N.D. Cal. 2019).

202. *Id*. at 849–50.

they suffer data privacy violation.[203] It should be noted that the standing motion does not inquire into the merits of the substantive case.[204] As stated earlier, data privacy injuries do not manifest themselves like other physical injuries, which may be a challenge to the victims, and thus present an inherent challenge quantification because of their intangible nature.[205]

With these results, it can be concluded that the standing doctrine has turned into a creed upon which any federal litigation in the U.S. federal courts must be premised.[206] For example, in *Spokeo Inc. v. Robins*, the Court emphasized that the standing doctrine is fundamental in data privacy litigation.[207] The Supreme Court emphasized the requirement of concrete and particularized injury-in-fact for plaintiffs to have standing to sue under the FCRA.[208] The Court held that a mere statutory violation without any concrete harm or risk of real harm does not automatically confer standing.[209] The *Spokeo* decision highlighted the importance of demonstrating actual harm in data privacy cases, establishing the standing doctrine as a crucial factor in determining the viability of such lawsuits.[210]

2. To what extent does lack of injury hinder the enforcement of data privacy protection?

Having considered how often defendants raise the Article III standing motion, which translates into the question of the plaintiff's need to prove cognizable injury, the next logical question is: How have the federal courts answered questions raised by the defendants? To answer this question, this part is divided into three subparts with corresponding figures. The first part, as illustrated by Figure 1, shows the general outlook of the data, on the outcome of the motion for dismissal for lack of injury under Article III standing. This demonstrates the outlook of the data with all federal courts combined. The second part, represented by Figure 2, shows data on how the district courts answered defendants' motions for dismissal for lack of injury. The third part shows how the circuits of appeals handled the appeals stemming from the district courts while addressing the same question of cognizable injury in data privacy violation cases.

How often do courts find that litigants in privacy protection suits have failed to satisfy Article III standing results?

---

203. BALLON, *supra* note 198, § 26.15.

204. *See* Whitmore v. Arkansas, 495 U.S. 149, 154 (1990) ("[B]efore a federal court can consider the merits of a legal claim, the person seeking to invoke the jurisdiction of the court must establish the requisite standing to sue.").

205. *See* Kreimer, *supra* note 19, at 780 (emphasizing the incompatibility of the standard of concrete injury and intangible injuries).

206. *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021) ("To have Article III standing to sue in federal court, plaintiffs must demonstrate, among other things, that they suffered a concrete harm. No concrete harm, no standing.").

207. Spokeo, Inc. v. Robins, 578 U.S. 330, 337–38 (2016).

208. *Id*. at 339.

209. *Id.* 341.

210. *Id*. at 341–42.

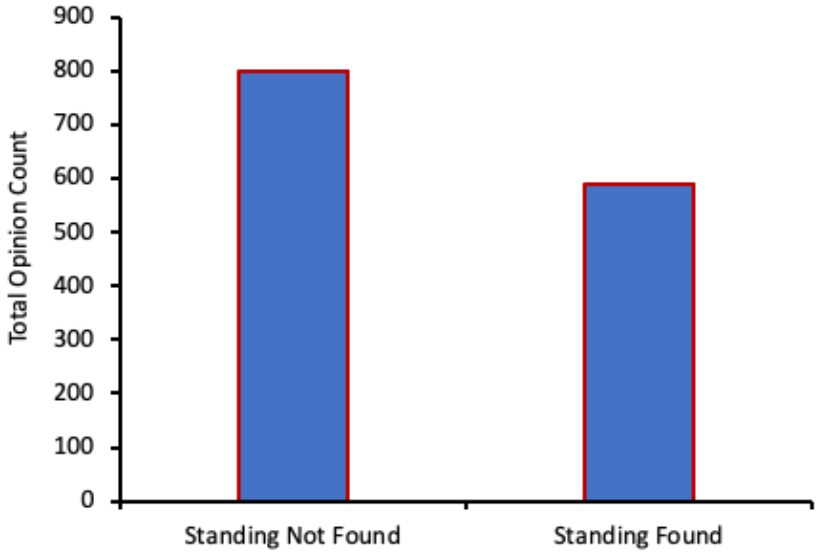

Figure 1

The data show that courts found no injury in 57.55% of cases where a defendant raised a motion to dismissal for lack of cognizable injury under Article III standing.[211] By implication, close to 60% of the time, the plaintiff ran short of satisfying the strict threshold of Article III standing, which requires a showing, when a data privacy violation claim is lodged, that the plaintiff suffered an injury-in-fact that is fairly traceable from the defendant's conduct and that the court is likely to redress it with a favorable decision. The degree of proof required to ascertain standing varies at various stages of the proceeding.[212] These cases were not allowed to move forward to a full trial.

211. This finding combines the descriptive results of all federal courts. By combining the data, a descriptive picture is painted of how federal courts have been answering the question of injury under Article III constitutional requirements without necessarily breaking down the different jurisdictional levels of these courts. The breakdown of the results for each court is in the proceeding results.

212. *See* Lujan v. Defs. of Wildlife, 504 U.S 555, 561 (1992) ("At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice. . . . In response to a summary judgment motion, however, the plaintiff can no longer rest on such 'mere allegations,' but must 'set forth' by affidavit or other evidence 'specific facts,' . . . which for purposes of the summary judgment motion will be taken to be true.") (internal citations omitted).

3. How has the proportion of dismissal for lack of injury varied from 2000 to 2020?

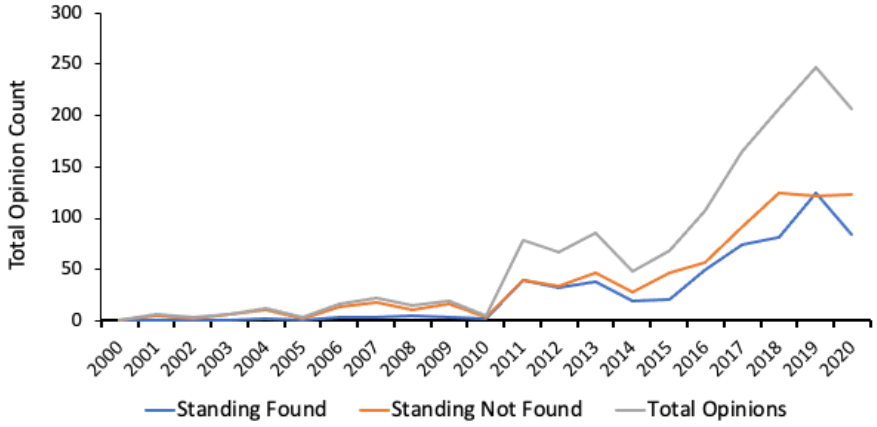

Figure 2

From 2000 to 2010, there were at most twenty qualifying opinions in a year, with the majority of opinions determining that standing was not found. From 2011 to 2020, the number of opinions dramatically increased. For a time, the number of opinions that found standing and did not find standing were almost split evenly between the two. But as the years go by, more courts find no standing exists when a standing issue is raised. The dismissal rate for lack of standing became increasingly prevalent after 2016, as indicated by Figure 2. It could be argued that the *Spokeo* decision, with its strict injury requirement in data privacy cases, likely played a role in the shift as it raised the bar for establishing standing in data privacy cases.[213] Consequently, many data privacy violation cases were dismissed due to the heightened Article III standing requirement after 2016.

4. Are courts more likely to find standing for some types of privacy cases?

During the data collection stage, we observed that claims based on the Telephone Consumer Protection Act (TCPA) appeared to fair better in surviving the standing challenge.[214] Courts' willingness to grant standing did not generally vary according to the statute that purported to grant privacy protection rights. There was, however, one exception: Privacy claims brought under TCPA were significantly more likely to survive a standing analysis.

213. *Spokeo*, 578 U.S at 339–40 (holding that a plaintiff in data privacy violation cases must show actual injury to recover damages, stating that the mere fact that a person's data has been collected or used without their consent is not enough to establish a claim for damages).

214. *See* Susinno v. Work Out World, Inc., 862 F.3d 346, 352 (3d Cir. 2017) (holding that the customer's receipt of unsolicited calls on her phone in violation of the Telephone Consumer Protection Act was sufficiently concrete to satisfy the Article III standing requirement).

This finding seemed mysterious on its face. Pointed and deliberate investigation of these cases, isolated from the rest of the dataset, was conducted. The first task in the TCPA cases analysis was to filter out TCPA cases from the rest of the dataset and analyze both sets separately—the original dataset without TCPA cases and the data set with only TCPA cases.

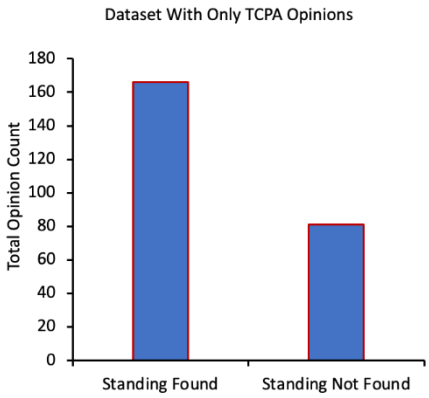

Figure 3

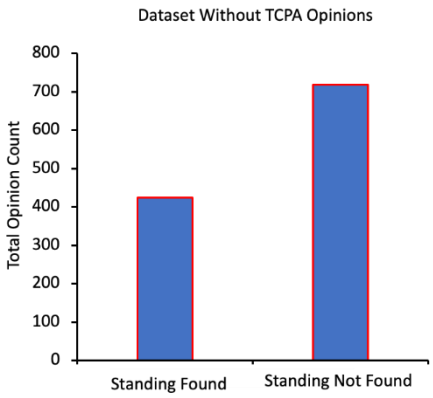

Figure 4

Figure 3 presents an outlook of data from only TCPA opinions and Figure 4 presents data from the whole dataset without TCPA opinions.

The results in Figure 4 show that when analyzing the data of only TCPA opinions, courts found that 67.21% of the claimants had standing and only 32.79% of the plaintiffs did not have standing. By contrast, the results in Figure 5 show the data after filtering out TCPA opinions. The analysis of these data show that 37.10% of cases survived the standing inquiry and 62.90% of the cases did not survive the standing challenge. In effect, the latter results show that 62.90% of the plaintiffs did not satisfy the injury-in-fact requirement under the Article III standing doctrine.

When comparing whether standing was found between all opinions and the "Dataset Without TCPA Opinions," there was a statistically significant difference ($p = 0.00623$),[215] implying that TCPA cases had an influence on the outcome of the standing results throughout the whole dataset. The highlight here is that there is a statistically significant difference in the outcome of the standing results when comparing opinions related to the TCPA with the rest of the dataset. This suggests that the TCPA cases had a notable impact on the overall standing outcome. The implication is that the presence of TCPA cases within the dataset influenced the results of the standing inquiry results in a distinct way compared to other cases which had no TCPA claims. This finding could potentially indicate that the unique provisions, or considerations associated with TCPA

215. A chi-square analysis was conducted to compare whether standing was found between the whole dataset (all opinions) and the dataset after filtering out TCPA opinions (TCPA cases - filtered out dataset).

cases, played a significant role in shaping the results with the broader dataset. Further exploration of the specific factors and dynamics surrounding TCPA cases may provide valuable insights into the broader understanding of standing in relation to privacy and consumer protection laws.

5. What role did the Spokeo *decision have on data privacy violation cases?*

The *Spokeo* decision is often touted as having had a profound impact on how courts determined the standing inquiry in data privacy violation cases.[216] The case "raised the bar" for plaintiffs in their claims for violations of the FCRA and other data privacy protection laws.[217] For instance, in the case of *Frank v. Gaos*, the Supreme Court stated that "[a]fter reviewing the supplemental briefs, we conclude that the case should be remanded for the courts below to address the plaintiffs' standing in light of *Spokeo*."[218] This demonstrates the extent to which *Spokeo* might have an impact on how courts resolve the standing challenge in data privacy violation cases going forward. With the *Spokeo* decision considered to have had a significant impact on how courts resolved standing questions, the study undertook an analysis to understand the veracity of this claim.

An analysis of the data from the district courts' opinions while considering the standing challenge in the pre-*Spokeo* era shows that 54.71% of the cases were dismissed for lack of standing and in 45.29% of the cases, the district courts found that the plaintiff had standing. What the data show is that in the pre-*Spokeo* era, courts were more likely to find that plaintiffs had standing to sue for data violations. This is because courts were more likely to find that the plaintiff had standing if they could show that they had suffered an injury, which is a broader concept.[219]

When compared to the post-*Spokeo* era, district courts found that in 62.50% of the opinions they handed down, the plaintiffs did not have standing. It was only in 37.50% of the opinions that the district courts found that the plaintiff had standing. The data show that the courts' rate of dismissal of data privacy violations for lack of injury as required by Article III standing requirement increased by 7.79%.

Following the *Spokeo* decision, the analysis indicates that courts adopted a stricter approach to the Article III standing requirement. The precedential impact of *Spokeo* is evident, as lower courts frequently cite the case to underscore the necessity for plaintiffs to demonstrate concrete injury to establish standing.[220]

---

216. Brett Watson & Karl Riley, *FDCPA Rulings Show* Spokeo*'s Influence, 5 Years Later*, LAW 360 (May 25, 2021, 5:13 PM), https://www.law360.com/articles/1385932/fdcpa-rulings-show-spokeo-s-influence-5-years-later? [https://perma.cc/4HC5-C3C2] (stating that the Spokeo decision is a "game-changer" in consumer protection violations statutes).

217. *Id*.

218. Frank v. Gaos, 139 S. Ct. 1041, 1046 (2019).

219. *See, e.g.*, Spokeo, Inc. v. Robins, 578 U.S 330, 339 (2016) ("Particularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be 'concrete.'").

220. *See, e.g.*, Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 15–17 (2d Cir. 2017) (holding plaintiffs failed to show a risk of real harm from an alleged unencrypted transmission of their face scans and citing *Spokeo* for support); Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 910–12 (7th Cir. 2017)

Notably, Spokeo narrowed the interpretation of data injury, emphasizing the need for plaintiffs to establish tangible injury to proceed with the lawsuit. As a result, plaintiffs face greater challenges in data privacy suits due to the heightened requirement for showing concrete harm.[221] Courts removed the broader concept of interpreting data injury and held that the plaintiffs must show that they have suffered concrete harm in order to have standing to sue.[222] The common theme is that *Spokeo* made it difficult for plaintiffs to succeed in data privacy laws suits.[223]

When comparing the pre- and post-*Spokeo* district court decisions on whether standing was found, there was a statistically significant difference ($p = 0.00774$) in the determination of standing. This suggests that *Spokeo* potentially influenced the approach taken by district courts when addressing standing challenges. The findings indicate a notable impact from *Spokeo* on the handling of standing issues within the federal judicial system.

IV. DISCUSSION

We will now address the significance of the study in the face of the results from the analysis. This study is the first comprehensive empirical investigation of data privacy violation cases in the U.S. federal courts. The results demonstrate the landscape of data privacy litigation in the U.S. federal courts using empirical legal methods. The study was mainly focused on understanding how federal courts, being bound by the injury-in-fact requirement under Article III standing, have resolved data privacy violation cases.

A. The Quest to Characterize Privacy Harm in the Face of the Strict Standing Requirement

With the digital realm being integral to most human activities in the modern world, courts are integral in the quest of preserving individuals' privacy.[224] Great effort should be geared towards creating a harmonized position in defining the

(holding the plaintiff lacked standing because he did not allege that "any of the personal information that he supplied to the company . . . had leaked and caused financial or other injury to him or had even been at risk of being leaked" and citing *Spokeo* for support); Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 929–31 (8th Cir. 2016) (dismissing for lack of standing because of a procedural violation under *Spokeo*).

221. *See* TransUnion LLC, v. Ramirez, 141 S. Ct. 2190, 2200 (2021) ("To have Article III standing to sue in federal court, plaintiffs must demonstrate, among other things, that they suffered a concrete harm. No concrete harm, no standing."); Church v. Accretive Health, Inc., 654 F. App'x 990, 992 (11th Cir. 2018) (finding a plaintiff suing under the FDCPA had standing only after showing "she suffered a concrete injury"); Heagerty v. Equifax Info. Servs. LLC., 447 F. Supp. 3d 1328, 1335 (N.D. Ga. 2020) (putting forth defendants' arguments after *Spokeo* that not "all violations of the FCRA necessarily result in concrete harm"); *In re* Vizio Inc., Consumer Priv. Litig., 238 F. Supp. 3d. 1204, 1214–15 (C.D. Cal. 2017) (finding plaintiff did have standing, despite various *Spokeo* arguments).

222. Patrick J. Lorio, *Access Denied: Data Breach Litigation, Article III Standing and a Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 86–90 (2017).

223. *Id.* at 82, 91.

224. *See* BALLON, *supra* note 198, § 26.15 ("Since 2010, there has been an explosion of data privacy-related putative class action suits filed against Internet companies, social networks, social gaming sites, advertising companies, application providers, mobile device distributors, and companies that (regardless of the nature of their business) merely advertise on the Internet, among others.").

harm that accrues when there is a data privacy violation. Such characterization of privacy injury is key to the federal courts preserving privacy in the digital world.[225]

Recall, the precise characterization of data privacy injury, as required by the Article III standing requirement, appears to be evasive. The quest to characterize privacy harms is even more important; the data from the study shows that in some cases, violation of a procedural right granted by a statute affecting intangible harm, such as being denied information Congress required to be publicly available, can be insufficient to constitute an injury-in-fact.[226] The Supreme Court stated that as much as Congress has the power to define new injuries, including intangible harms and new rights under a statute, a plaintiff does not automatically satisfy the cognizable injury requirement merely by suing to enforce or vindicate that statutory right.[227] Because of this, federal courts have struggled with fitting data privacy harms within the traditional understanding of harm.[228]

The results of this study provide an empirical perspective to what many privacy scholars have long stated: That data privacy violation cases are dismissed for lack of injury, as required by Article III standing.

The results show that close to 60% of the cases heard in federal courts from 2000 to 2020 were dismissed for a failure of satisfying the strict injury threshold of Article III standing. In other words, most data privacy cases are dismissed because of the injury-in-fact requirement for standing. This has a remarkable impact on the broader social and economic well-being of individuals given the importance of privacy to humans.[229]

The strict injury requirement by federal courts is a major bottleneck in protecting data subjects.[230] Unlike other areas of the law where consumer protection takes center stage, especially in ensuring that consumers are not subjected to unconscionable transactions, data privacy law falls short of the same benefits, as the data show that it is plagued with strict requirements of physical and monetary injury.[231]

---

225. *See id.* ("Earlier waves of Internet privacy litigation had largely proven unfruitful for plaintiffs' lawyers because of the absence of any monetary injury . . . .").

226. Spokeo, Inc. v. Robins, 578 U.S. 330, 342 (2016).

227. *Id.* at 341–42.

228. *See* Forbes v. Wells Fargo Bank N.A., 420 F. Supp. 2d 1018, 1019, 1021 (D. Minn. 2006) (finding there was "no present injury or reasonably certain future injury to support damages for any alleged increased risk of harm" after the theft of computers containing "unencrypted customer information including names, addresses, Social Security numbers and account numbers). Data privacy injuries are futuristic and do not attach immediately.

229. *See* Kreimer, *supra* note 19, at 753 ("[I]nformation plays an increasingly dominant role in our social, economic, political, and cultural life.").

230. *See id.* at 753–54 (arguing that "a conception of 'injury in fact' that takes the requirement of 'concrete' injury to mean injury that has some 'tangible' physical or economic manifestation rests in obvious tension with a legal system and society . . . built around information" because "[i]nformation is by nature intangible," "can be used by an infinite number of persons," "is difficult to cabin use of," and as a result, "violations of duties regarding information will result in injuries that are 'general' by definition").

231. *See* study results *infra* Section III (showing that the doctrine of injury-in-fact causes the majority of privacy protection cases to fail).

The non-manifestation of privacy harms in the immediate future should not be interpreted to mean that a victim of a privacy violation has not suffered an injury.[232] For instance, when a data breach occurs, there is no accurate prediction that the data which is obtained by bad actors will be used immediately or used at all.[233] To this extent, a plaintiff's ordeal of stress, frustration, anxiety, and other forms of emotional distress should be considered as actual harm to confer standing.[234] Anything to the contrary should be calculated to be an erroneous starting point given that many data privacy violation victims will not get courts' redress.[235] For example, under the Privacy Act of 1974, it is unclear whether mental and emotional distress resulting from the violation of the Act will afford redress to the victim.[236] Thus, using the traditional yardstick to determine data privacy injuries may freeze out remedies available to privacy victims.[237] The fact that data injuries are abstract should not be interpreted to mean that they are non-existent.[238]

B. Revisiting the Separation of Powers Doctrine in the Standing Inquiry

As explained earlier, the Supreme Court's justification for the strict standing requirement is to maintain the sanctity of the doctrine of separation of powers.[239] The Supreme Court has frequently emphasized that standing is a core principle of the doctrine of separation of powers.[240] Modern Article III standing requirement is that the plaintiff has to prove "concrete and particularized injury," plus legal injury.[241] This strict requirement appears to continuously negate the contextual link between the judiciary and legislature and, to some extent, the executive arms of the government which have the regulator function through agencies created by the executive arm.[242] The Court has underscored that without injury-in-fact and other attendant requirements, federal courts will

232. Kreimer, *supra* note 19, at 753–54.

233. *See* Schneider, *supra* note 192, at 287–88 ("When an individual's personal information is stolen, there is no guarantee that it will be used fraudulently.").

234. *See* Solove & Citron, *supra* note 71, at 745 ("Risk and anxiety are injuries in the here and now. Victims of data breaches have an increased risk of identity theft, fraud, and reputational damage.").

235. *See id*. at 744–45 (explaining that recent standing precedent in relation to data privacy claims have caused confusion and few cases to go forward).

236. *See* Fed. Aviation Admin. v. Cooper (*Cooper II*), 566 U.S. 284, 304 (2012) ("[T]he Privacy Act does not unequivocally authorize an award of damages for mental or emotional distress.").

237. *See* Schneider, *supra* note 192, at 280 ("To date, judges have been quick to dismiss data breach negligence suits because consumer class plaintiffs have difficulty showing injuries appropriate for legal relief.").

238. *See id*. at 280–81 (demonstrating that injuries can be in the form of "future credit monitoring fees," "losses from fraudulent activity and reissuing credit cards," and losses from identity theft).

239. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 577–78 (1992) (explaining that the courts are permitted "to participate in law enforcement," with respect to statutes "empowering administrative agencies," "only to the extent necessary to protect justiciable individual rights against administrative action fairly beyond the granted powers").

240. Allen v. Wright, 468 U.S. 737, 752 (1984) ("[S]tanding is built on a single basis idea—the idea of separation of powers.").

241. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2206 (2021).

242. Put another way, the standing inquiry as it stands not only threatens the data subjects seeking a court's relief for data privacy violations, but also limits the federal courts' judicial power when Article III is strictly interpreted as it currently is.

contravene the functions of the coordinate arms of the federal government.[243] This upholds the separation of power doctrine.[244]

Contrary to how Article III standing has been interpreted—as aiming to actualize and serve the separation of powers doctrine—the injury requirement under Article III has, in practical terms, distorted the relationship between the judiciary and the legislative branches.[245] While quoting the earlier Supreme Court opinion of *Lujan v. Defenders of Wildlife*,[246] Justice Thomas, in his dissenting opinion in *Ramirez*, stated that "[n]ever before has this Court declared that legal injury is *inherently* insufficient to support standing."[247] He continued to state that "never before has this Court declared that legislatures are constitutionally precluded from creating legal rights enforceable in federal court if those rights deviate too far from their common-law roots."[248] Justice Thomas suggested that, with the approach taken by the majority, "courts alone have the power to sift and weigh harms to decide whether they merit the Federal Judiciary's attention."[249] "In the name of protecting the separation of powers, . . . this Court has relieved the legislature of its power to create and define rights."[250]

With the injury requirement, it appears that the judiciary has at times (and with judicially elaborated reasoning) objected to what the legislature prescribes as injury under the FCRA and the Privacy Act of 1974.[251] Congress' duties are to identify the rights and interests of people and define conduct that violates these private rights.[252] With Congress having executed its duty thus far, federal courts have strictly construed Article III standing and have required litigants to show more than what Congress has prescribed being the factual injury.[253] A close look at the statistical outlook of the standing inquiry outcome at the district level and the general outlook for the results of federal courts combined shows a

243. *See Lujan*, 504 U.S. at 560–61 (stating that "the doctrine of standing" is "[o]ne of those landmarks, setting apart the 'Cases' and 'Controversies' that are of the justiciable sort referred to in Article III—'serving to identify those disputes which are appropriately resolved through the judicial process'") (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

244. *See id.* at 559–60 ("[T]he Constitution's central mechanism of separation of powers depends largely upon common understanding of what activities are appropriate to legislatures, to executives, and to courts.").

245. FCRA sets out the circumstance when injury attaches, yet the court in *TransUnion* adds the factual injury requirement. TransUnion v. Ramirez, 141 S. Ct. 2190, 2211–12 (2021).

246. *See Lujan*, 504 U.S. at 578 ("Nothing in this contradicts the principle that 'the . . . injury required by Art. III may exist solely by virtue of "statutes creating legal rights, the invasion of which creates standing."'") (quoting Warth v. Seldin, 422 U.S. 490, 514 (1975)).

247. *TransUnion*, 141 S. Ct. at 2221 (Thomas, J., dissenting) (emphasis in original).

248. *Id.*

249. *Id.*

250. *Id.*

251. The FCRA, by its direct reading, grants the consumer with no injury whatsoever an opportunity to file claims regarding technical statutory violations while seeking statutory damages. However, in *Spokeo*, the Court held that purely technical violations of a statute are not sufficient to satisfy Article III's standing requirement. Spokeo, Inc. v. Robins, 578 U.S. 330, 342–43 (2016).

252. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring) (opining that "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before" and that "Congress must at the very least identify the injury it seeks to vindicate and relate the injury to the class of persons entitled to bring suit").

253. Article III standing has gained a status where the phrase "cases and controversies" has been translated to mean a jurisdictional control where the judiciary may limit what and when the legislature may determine as to when injury attaches. *See e.g.*, *Lujan*, 504 U.S. at 575–78 (finding there is not an automatic cause of action just because Congress found some injury—Article III standing must be satisfied to the satisfaction of the court).

small difference of 0.02%, which would likely show that all federal courts, regardless of the jurisdiction, are approaching motions to dismiss for lack of injury under Article III standing requirement in a similar manner.[254] For example, In *Hagy v. Demers & Adams*, the Sixth Circuit Court, while citing *Spokeo*, stated that even though "Congress may 'elevate' harms that 'exist' in the real world before Congress recognized them to actionable legal status, it may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is."[255] In particular, the Supreme Court has often rejected the suggestion that "a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[256]

The challenge presented by the Supreme Court's instruction as to the injury-in-fact is that it has somewhat reestablished a right-centered notion of standing by stating that an injury is considered sufficient for standing, only if that injury is "judiciary cognizable."[257] The argument advanced here is that whether an injury is cognizable should depend on the content of the law as passed by the legislative arm of government—an injury should be deemed cognizable if the law deems it as such and capable of redress.[258] Where the net effect in the realm of data privacy violations presents intangible injury, the existence of standing should be dependent on whether the plaintiff (data subject whose data privacy has been violated) has raised a legal right that is capable of enforcement by the court, not necessarily whether the plaintiff has raised an injury-in-fact.[259] The factual injury resulting from data violation that is cognizable by law is likely to be elusive given the nature of data injuries.[260]

---

254. Given the size of the data, a difference of 0.02% appears to be too small to cause a significant difference.

255. Hagy v. Demers & Adams, 882 F.3d 616, 622 (6th Cir. 2018) (citing Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016)).

256. *Spokeo*, 578 U.S. at 341.

257. *See* Allen v. Wright, 468 U.S. 737, 755–56 (1984) (declining to find standing for an "abstract stigmatic injury" because "such injury is not judiciary cognizable"); Robins v. Spokeo, Inc., 867 F.3d 1108, 1113 (9th Cir. 2017) (making a telling proposition "that an alleged procedural violation [of a statute] can by itself manifest concrete injury where Congress conferred the procedural right to protect a plaintiff's concrete interests and where the procedural violation presents a risk of real harm to that concrete interest") (internal quotations omitted) (citations omitted). The question in the case of *Spokeo v. Robins*, as discussed earlier, was whether Congress can authorize a cause of action based on a violation of a federal statute and therefore confer Article III standing on a plaintiff who has suffered concrete harm. The case went up to the Supreme Court, which held that the standing principles of Article III mean that a plaintiff cannot bring a claim that alleges "a bare procedural violation" under the FCRA and that the lower courts must examine the elements of the injury-in-fact requirement in its entirety. *Spokeo*, 578 U.S. at 341.

258. *See* Vt. Agency of Nat. Res. v. United States *ex rel*. Stevens, 529 U.S. 765, 772–73 (2000) ("The interest [sufficient to confer standing] must consist of obtaining compensation for, or preventing, the violation of a legally protected right."); Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992) (stating, while commenting on the standing, that "[n]othing in this contradicts the principle that 'the . . . injury required by Art. III may exist solely by virtue of "statutes creating legal rights, the invasion of which creates standing"'") (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975)).

259. *See* Solove & Citron, *supra* note 71, at 747–49 (explaining the difficulties in meeting the standing requirement for data privacy harms, but that those affected have still suffered and could be redressed).

260. *See id.* at 741 ("[T]he majority of courts have ruled that injuries from data breaches are too speculative and hypothetical, too reliant on subjective fears and anxieties, and not concrete or significant enough to warrant recognition.").

C. Unpacking the TCPA in the Face of the Standing Inquiry

As previously discussed, results from the analysis of the TCPA cases were distinct and had statistical significance.[261] An analysis of the dataset without TCPA cases[262] demonstrates that 62.90% of the cases did not survive the standing challenge, whereas only 37.10% of cases survived the standing challenge after omitting cases that involved the TCPA. The results from this analysis are telling. While considering the dataset that includes all cases before filtering out TCPA cases, as stated above, 57.55% of the cases were dismissed for lack of proof of cognizable injury under the Article III standing requirement. The results show a difference of 5.35% between the two datasets, which is significant. The general data outlook of the standing outcome looks different when TCPA cases are excluded from the dataset.

The data show that courts considered TCPA cases in a different light and were likely to find standing in TCPA-based claims.[263] In *Romero v. Department Stores National Bank*,[264] the Ninth Circuit indicated that an individual has standing to pursue TCPA claims even when the calls are not answered, establishing that violations occur for unanswered calls.[265] In this case, the Court, while referring to its earlier decision in *Van Pattern v. Vertical Fitness Group*,[266] stated that "a violation of the TCPA is a concrete, *de facto* injury."[267]

The TCPA was enacted in response to many consumer complaints about the abuse of telephonic technology.[268] In *Mims v. Arrow Financial Services*,[269] the Supreme Court makes a summary of Congress' findings and stated that:

> "Unrestricted telemarketing," Congress determined, "can be an intrusive invasion of privacy." . . . In particular, Congress reported, "[m]any consumers are outraged over the proliferation of intrusive, nuisance [telemarketing] calls to their homes." . . . "[A]utomated or prerecorded telephone calls" made to private residences, Congress found, were rightly regarded by recipients as "an invasion of privacy."[270]

From the results of the study and a closer review of the case, the TCPA has been positioned as a remedial statute that is entitled to broad construction in the data privacy litigation realm. For instance, while addressing the question of injury under Article III standing, a court concluded that "the invasion of privacy,

261. There was a statistically significant difference ($p = 0.00623$) between the two datasets (that is, there was a statistically significant difference between the whole dataset (all opinions) and the dataset of TCPA cases only). This implies that TCPA cases influenced the outcome of standing challenges in the whole dataset (all opinions) compared to the dataset after filtering out TCPA opinions (TCPA cases - filtered out dataset).

262. This dataset combines both District Court and Appellate Courts cases.

263. *See* Susinno v. Work Out World, Inc., 862 F.3d 346, 351–52 (3d Cir. 2017) (holding that a customer's receipt of unsolicited calls on her cell phone in violation of the Telephone Consumer Protection Act was sufficiently concrete to grant her standing).

264. Romero v. Dep't Stores Nat'l Bank, 725 F. App'x 537 (9th Cir. 2018).

265. *Id.* at 539–40.

266. Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037 (9th Cir. 2017).

267. *Romero*, 725 F. App'x at 539 (citing *Van Patten*, 847 F.3d at 1043).

268. Mims v. Arrow Fin. Servs., LLC, 565 U.S 368, 370–71 (2012).

269. *Id.*

270. *Id.* at 372 (internal citations omitted).

annoyance and wasted time associated with robocalls is sufficient to demonstrate concrete injury."[271]

In *Maydwell v. Ciara Financial Services*, the court agreed with the plaintiffs that harm suffered in violation of the TCPA can be in the form of "emotional distress, increased risk of personal injury resulting from the distraction caused by the never-ending calls, increased usage of [] telephone services, loss of cellular phone capacity, diminished cellular phone functionality, decreased battery life on [a] cellular phone, and diminished space for data storage" and would be enough for standing.[272] In contrast, in *Bell v. Acxiom*,[273] a non-TCPA-related case, the court found that receiving unsolicited mailing advertisements and an increased threat of identity theft was insufficient to constitute harm, and thus the plaintiffs did not have standing.[274]

To some extent, the TCPA enjoys preferential treatment. Most of the harms that the court in the *Maydwell* case determined as being concrete enough to satisfy the standing requirement are the same harms that most data privacy violations cause.[275] The courts agree that an allegation that the plaintiff had to endure the nuisance of unwanted calls satisfies the injury-in-fact requirement for TCPA claims.[276] In these cases, the defendant had placed multiple calls that "would annoy or harass a reasonable person."[277] The receipt of an unsolicited cellular "text" by a telemarketer is treated the same as receiving a "telephone call" under the TCPA.[278] In finding that there is a violation of the TCPA in the *Van Patten v. Vertical Fitness Group* case,[279] the court explained that a single telephone call in violation of the TCPA creates a violation of privacy and nuisance.[280] Courts have also "consistently held that allegations of nuisance and invasion of privacy in TCPA actions are sufficient to state a concrete injury," as required under Article III.[281]

It can be argued that the TCPA's standard, in describing privacy injury under Article III standing, sets a platform upon which other privacy laws should be couched, rather than a narrow understanding of data privacy injuries which has resulted in many cases being dismissed. With the TCPA numbers in comparison to the other cases, judges seem to suggest that some intangible privacy harms are real, whereas others are not.[282]

---

271. Abante Rooter & Plumbing, Inc. v. Pivotal Payments, Inc., No. 16-CV-05486-JCS, 2017 WL 733123, at *6 (N.D. Cal. Feb. 24, 2017).

272. Maydwell v. Ciara Fin. Servs., Inc., No. 3:19-CV-00051-BT, 2019 WL 5102716, at *2 (N.D. Tex. Oct. 10, 2019).

273. Bell v. Acxiom Corp., No. 4:06-CV-00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006).

274. *Id.* at *2.

275. *See Maydwell*, 2019 WL 5102716, at *2 (listing the various injuries suffered by the plaintiff, including diminished cell phone capacity).

276. Cunningham v. Florio, No. 4:17-CV-00839-ALM-CAN, 2018 WL 4473792, at *4 (E.D. Tex. Aug. 6, 2018).

277. *Id.*

278. *See* Satterfield v. Simon & Schuster Inc., 569 F.3d 946, 948 (9th Cir. 2009) ("[W]e hold that it is reasonable to interpret 'call' under the TCPA to include both voice calls and text messages.").

279. Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037 (9th Cir. 2017).

280. *Id.* at 1041–43.

281. Smith v. Blue Shield of Cal. Life & Health Ins. Co., 228 F. Supp. 3d 1056, 1063–64 (C.D. Cal. 2017).

282. *Supra* notes 261–67 and accompanying text.

D. Finding Footing after the Spokeo *Decision*

The data suggest that the Supreme Court's decision in *Spokeo*[283] had a significant impact on how lower courts approached the standing question.[284] In particular, the analysis examined how the Supreme Court's decision affected plaintiffs' suits while testing the concreteness of alleged privacy injuries.[285] This analysis was undertaken by looking at the data before the Supreme Court's decision and the data after the Supreme Court's decision. The results showed that there was an increased dismissal rate of data privacy violation cases after the *Spokeo* decision.

The Supreme Court's opinion in *Spokeo v. Robins* was handed down in May 2016.[286] The provision that Robins relied on for his claim under the FCRA was that consumer reporting agencies should "follow reasonable procedures to assure maximum possible accuracy" while compiling consumer reports[287] and that:

> "[A]ny person who willfully fails to comply with any requirement [of the Act] with respect to any [individual] is liable to that [individual]" for, among other things, either "actual damages" or statutory damages of $100 to $ 1,000 per violation, costs of the action and attorney's fees, and possibly punitive damages.[288]

With this provision coupled with facts and Robins' claim, the case gravitated around the standing question in the face of the elaborate provision of the law that Robins relied on for his claim.

A close review of the *Spokeo* case decision reveals that the Supreme Court did not directly tackle the issue of "[w]hether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm, and who therefore could not otherwise invoke the jurisdiction of a federal court, by authorizing a private right of action based on a bare violation of a federal statute."[289] The Supreme Court found that Robins had not suffered a concrete injury, and therefore was not vested with standing as required under Article III.[290]

The results, as demonstrated by the data, show how the injury requirement after the *Spokeo* decision freezes out a lot of cases, particularly those under the FCRA, since injuries resulting from the violation of this statute do not easily manifest.[291]

---

283. Spokeo, Inc. v. Robins, 578 U.S. 330 (2016).
284. Watson & Riley, *supra* note 216.
285. *Id.*
286. *Spokeo*, 578 U.S. at 333.
287. 15 U.S.C. § 1681e(b).
288. *Spokeo*, 578 U.S. at 335 (quoting 15 U.S.C § 1681n(a)).
289. *No-Injury Class Action Plaintiffs Suffer Concrete Harm in Supreme Court's Decision on the Requirements for Article III Standing*, MARSHALL DENNEHEY (Sept. 1, 2017), https://marshalldennehey.com/articles/no-injury-class-action-plaintiffs-suffer-concrete-harm-supreme-court%E2%80%99s-decision [https://perma.cc/984K-KKC9].
290. *Spokeo*, 578 U.S. at 342–43.
291. *Infra* Section III.A.5.

The question that remains is how and when a party can rely on FCRA's provisions that allow a plaintiff to claim actual and statutory damages when there is a statutory violation, or whether the statute in effect has been amended to reflect the Supreme court's decision in *Spokeo*.[292] While Spokeo is based on the FCRA, the net effect of the Supreme Court's decision, in this case, creates a confining element in the application and discharge of other data privacy statutes. Data subjects must prove more injury than that statutorily created by data privacy protection statutes, including the TCPA, the Privacy Act of 1974, and the VPPA, among other statutes.[293] Congress fashioned a private right of action in these statutes and stipulated statutory damages to compel compliance by the data collectors, but the *Spokeo* decision demands a showing beyond what Congress stipulated. This in itself has constitutional implications for separations of power, which is the same concern that underlies standing doctrine to begin with.[294]

E. The Social Inequalities Perpetuated by the Standing Doctrine in Data Privacy Litigation

The standing doctrine, as applied in data privacy litigation, promotes social inequalities, because it appears to favor the privileged against the marginalized.[295] Major data violations are at the hands of large organizations, which in theory would have the ability to hire the best lawyers to represent them.[296] Data subjects are often ordinary citizens who may not readily know when a data violation happens.[297] They may not have enough resources to find out, unlike the data collectors who are often big-tech giant companies.[298] The companies are often the repeat players in the court system, whereas ordinary data privacy violation victims are "one-shotters," as defined by Marc Galanter.[299] In his work *Why the "Haves" Come Out Ahead*, Marc Galanter stated that "repeat players" are those persons and organizations that anticipate to have repeat litigation and have resources to pursue long-term interests, shape the development of law, and engage in a litigation game quite differently than

292. *Spokeo*, 578 U.S. at 342–43 (reversing and remanding the case for the lower court to "fully appreciate the distinction between concreteness and particularization" to determine "whether the Ninth Circuit's ultimate conclusion—that Robins adequately alleged an injury in fact—was correct.").

293. Telecomm. Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (amended as at 47 U.S.C. § 227(b)(2)(C)); Priv. Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified at 5 U.S.C. ch. 5 § 552a); Video Priv. Prot. Act, Pub. L. No. 100-618, 102 Stat. 3196 (1988) (codified at 18 U.S.C. § 2710).

294. 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.").

295. *See* Gene R. Nichol, Jr., *Standing for Privilege: The Failure of Injury Analysis*, 82 B.U.L. REV. 301, 304 (2002) (explaining how the standing doctrine "systematically favors the powerful over the powerless").

296. *See* Kenny, *supra* note 173, at 216 (explaining the Equifax data breach that exposed the data of over 145 million American adults).

297. KNOWLEDGE AT WHARTON, *supra* note 3 (explaining how data is tracked in more meaningful ways than typically perceived by Americans).

298. *See id.* (giving examples of "Google, Facebook, Amazon, Apple, and others" as the main companies managing data and, sometimes, promoting data protections).

299. Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 L. & SOC'Y Rev. 95, 97 (1974).

do one-shotters, who are those persons and organizations that deal with the legal system infrequently.[300] The one-shotters and repeat players situation, as seen in the data privacy litigation landscape, creates an undesirable social system where the plaintiffs will be at a disadvantage.[301]

It is not unrealistic to imagine that most data collectors stand in the positions of the repeat players and the data subjects who are often the victims of data violations stand in the position of one-shotters. As Marc Galanter illustrates, there is an imbalance in terms of resources and know-how when in the litigation scheme between the two described subjects.[302] Certainly, when it comes to data privacy litigation, the defendant's go-to first line of defense is an objection based on Article III standing's strict requirement of cognizable injury.[303]

As the data in this research show, close to 60% of the data privacy violation cases are dismissed on the Article III standing inquiry. It would not be farfetched to conclude that the imbalances created by the repeat players versus one-shotters play a great role in the injury-in-fact probe under the Article III standing requirement.

There is a significant social inequality gap that will continue to be created by the standing inquiry because the majority of the data subjects are one-shotters.[304] The resulting effect is that the "haves" will continue creating and shaping the direction of the privacy legal order and then subsequently influence the public order that dominates all forms of private order.[305] With the repeat players calling the shots in the judicial system as to what and when privacy injury attaches in many cases filed by the data subjects who may be one-shotters, it could be concluded that they may be shaping the data privacy legal system. The repeat players are not only shaping the data privacy legal agenda in court systems, but also in the legislature.[306] Technology companies spend a lot of money on their lobbying agenda with an aim of muzzling the enacting of privacy laws.[307] With this in mind, data subjects ought to be protected by the law to narrow the gap that is being created between the data subjects and the data collectors.[308]

---

300. *Id.* at 97–98.

301. *Id.* 98–102.

302. *Id.*

303. *See supra* Section III.A.2 (explaining that data show that courts found no injury in 57.55% of cases where a defendant raised a motion to dismiss for lack of cognizable injury under Article III standing).

304. *See* Galanter, *supra* note 299, at 98, 108–09 (explaining that repeat players have resources to pursue long-term interests, while one-shotters typically do not).

305. *See* Shauhin A. Talesh, *The Privatization of Public Legal Rights: How Manufacturers Construct the Meaning of Consumer Law*, 43 L. & SOC'Y REV. 527, 551–55 (2009) (explaining how public policy and laws are frequently shaped by private actors).

306. *See id.* at 536, 539, 555 (explaining how private actors impact passed legislation).

307. Issie Lapowsky, *Tech Lobbyists Push to Defang California's Landmark Privacy Law*, WIRED (Apr. 29, 2019, 3:09 PM), https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/ [https://perma.cc/6DEC-U57B].

308. *See* Martin Tisne, *Collective Data Rights Can Stop Big Tech from Obliterating Privacy*, MIT TECH. REV. (May 25, 2021), https://www.technologyreview.com/2021/05/25/1025297/collective-data-rights-big-tech-privacy/ [https://perma.cc/2NSP-WYB8] ("Congress should . . . use the lessons from implementing [the Public Health Emergency Privacy Act] to develop laws that focus specifically on collective data rights."); Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021) https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

V. POTENTIAL PRESCRIPTIONS, LIMITATIONS, AND OPPORTUNITIES FOR FUTURE WORK

A. Potential Prescriptions

This study has shown that the standing doctrine, at least as currently interpreted by courts, creates a systematic gap between what the words of many federal privacy statutes promise—protection of privacy—and what courts in fact deliver.

What can be done about this gap? The constitutional basis of the standing doctrine makes the answer to this question difficult, at least so long as courts interpret injury-in-fact requirements to follow from their constitutional position as judging cases and controversies.[309] Of course, interpretations of what constitutes a judicially cognizable injury-in-fact could be resolved by a revisitation of what it means to have injury-in-fact by the Supreme Court, or the adoption of special privacy-based rules for standing, such as what has been suggested for environmental harms.[310] Such approaches can only be addressed by the Supreme Court, however. Besides this approach, advocacy geared towards creating awareness among federal legislators that privacy statutes will often fail, absent of some kind of particularized, perhaps monetizable, injury attached to the privacy harm, would cause desirable outcomes.[311] Plus, state courts may need to play a particularly important role in protecting privacy given the federal standing doctrine does not apply to them.[312]

Having discussed earlier that Article III standing is only a doctrine of *federal* courts and that state courts are not bound by this doctrine, perhaps an approach to state courts' implementation and enforcement of data privacy is the key to the problem.[313] The Illinois Biometric Information Privacy Act, for example, is an Act of the kind that provides for a private cause of action for any person aggrieved by a privacy violation protected under this statute.[314] It appears that state courts and state law may offer a solution to the challenge at hand.[315] Perhaps the next project—a similar empirical study of how state courts have used state law to protect privacy—is ideal. Key stakeholders including

[https://perma.cc/Z6E9-PNHA] (arguing for stronger privacy laws, which will result in many benefits, including a benefits to a user's "day-to-day experience").

309. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 559–60 (1992) (affirming the core component of standing, that is, being rooted in "cases" or "controversies").

310. *See* Jan G. Laitos, *Standing and Environmental Harm: The Double Paradox*, 31 VA. ENVT'L L.J. 55, 97 (2013) ("Allowing organizations standing to protect the environment or some natural object would redirect the focus from human harms to the injured natural object.").

311. *See* Citron & Solove, *supra* note 42, 796–99 ("Harm has become one of the biggest challenges in privacy law. The law's treatment of privacy harms is a jumbled, incoherent mess. Countless privacy violations are left unremedied not because they are unworthy of being addressed but because of the law's failure to recognize harm.").

312. Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE AGRIC. & NAT. RES. L. 349, 352 (2015).

313. *See id.* (explaining that state courts have evaluated and implemented their own constitutional requirements for standing, including adopting some elements of *Lujan*).

314. 740 ILL. COMP. STAT. 14/20 (2023).

315. *See id.* (providing a statutory right of action); Sassman, *supra* note 312, at 398 (explaining that different states offer different solutions to the constitutional standing doctrine).

policymakers, litigants, and scholars need to understand how privacy protections work on the ground, not just how they appear on paper.[316]

B. Limitations and Opportunities for Future Work

Although we methodically compiled a comprehensive data set for this study, it has limitations. The first limitation is that the study majorly relies on federal court docket files that were accessed through Bloomberg. While there were attempts to compare the results from Bloomberg with other commercial legal databases like Westlaw Edge and Lexis, we cannot accurately state that all cases under the period of study were included.

While the final cohort of cases was selected using the inclusion and exclusion mechanism, with stated and appraised reasons for the considered criteria, there could have been some honest subjectivity. This subjectivity could have cropped in because of the manual selection of the cases and eventual manual coding for the various variables. Some cases were missing docket information, though attempts were made to locate the missing information. Another limitation of the study was that it was rather challenging to use judicial opinions for a systematic study and we cannot eliminate some degree of unobserved reasoning and selection bias in hand-coding of the different variables.

A future project should investigate the course of action that is undertaken by the plaintiffs whose cases are dismissed for lack of concrete injury. As mentioned earlier in the paper, a majority of cases in the U.S. are settled.[317] However, there is no research yet as to the nature of these settlements and which data collectors are likely to settle more than others.[318] There is also no research on the disposition of cases that litigants file in their state courts which are not bound by stringent Article III standing requirements.[319] A consideration is necessary to asses of how state courts perform in offering redress to the victims of data privacy violations.

VI. CONCLUSION

This work is the first comprehensive empirical study to evaluate the extent to which the standing doctrine affects the enforcement of privacy protections. Importantly, the results of the study show that close to 60% of the data privacy

316. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE i–iv (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf [https://perma.cc/F786-WU5M] (proposing a framework for businesses and policymakers on how to protect consumer privacy as applied "in the real world").

317. *See, e.g.*, Jeffrey Johnson & Adam Ramirez, *Personal Injury Settlement Amounts Examples (2023 Guide)*, FORBES (Sept. 22, 2022, 12:54 PM), https://www.forbes.com/advisor/legal/personal-injury/personal-injury-settlement-amounts/ [https://perma.cc/TER4-MKWC] ("Estimates vary, but somewhere between about 95% of civil cases reach settlements at some stage.").

318. *See generally id.* (estimating the percentage of cases in the U.S that settle, but not describing the nature of the settlements nor which cases are more likely to settle than others).

319. Sassman, *supra* note 312, at 398.

violation cases have been dismissed because of failure to satisfy the strict injury requirement under the Article III standing requirement of the U.S. Constitution. The results of the study establish that standing is a potent barrier to enforcing privacy rights and that *most* privacy cases in federal court fail because of the requirement to satisfy the injury-in-fact requirement of the standing doctrine.

This empirical finding provides hard evidence to back up what past scholars in this area of the law have long anecdotally suspected: that the requirement for injury-in-fact creates an important barrier to meaningful recovery for privacy harms.[320]

APPENDIX A

Subject heading excluded	**Exclusion Rationale**
Actions filed under the Freedom of Information Act ("FOIA") request cases	The cases involve a request for the release of records held by a government agency. Such records often involve private information. When there is a FOIA challenge, the defense is often that disclosure of such records would constitute an invasion of personal privacy.[321] Objections as to the existence of injury rarely form part of the inquiry.
Sealing motions[322] **and motions for protective orders**[323]	The main claim in such cases is often that the documents for sealing contain confidential or sensitive information protected under the parties' stipulated protective order. The claim is that providing public access to such documents can be used as a source of business information that might harm a litigant's competitive advantage. A party's interest is often in the privacy of its financial records and terms of confidential agreements which they claim stand high in the public's right to access court records. The same is with applications for protective orders regarding "protected material." These cases

320. Citron & Solove, *supra* note 42, at 796.

321. FOIA request cases generally involve challenges to denials to requests and the release of private records held by public agencies. The question of harm rarely arises as the reason for which these cases were eliminated from the final dataset. *See* Daily Caller v. U.S. Dep't of State, 152 F. Supp. 3d 1, 3 (D.D.C 2015) (seeking to accelerate an agency's processing of an outstanding FOIA request against Hillary Clinton's use of a private email server during her time in the U.S. Department, which involved e-requests for private information, but there was no question of harm raised like in many of the other FOIA cases).

322. Courts often sign protective orders permitting parties to designate the discovery they wish to keep confidential among themselves. Sometimes parties may not summarily agree on what to seal or redact in court records as confidential information. These cases by implication involve information that parties may want to keep confidential and not available as public record. The question of harm is not critical in these cases. What is critical is the public interest in access to all court documents. *See* McNabb v. Marshal Mize Ford, Inc., No. 1:16-CV-115-PLR-CHS, 2016 BL 239418, at *1–2 (E.D. Tenn. Jul. 26, 2016) (stating that "[f]iling a motion to seal which simply states that the parties have designated the document as confidential will not be sufficient to place the document or information under seal," with no question of injury for the court to interrogate in the first instance); *In re* Google Inc. Gmail Litig., No. 5:13-MD-02430-LHK, 2014 BL 229284, at *5–6 (N.D. Cal. Aug. 06, 2014) (involving plaintiffs who used Gmail or exchanged emails with Gmail users, who filed a case against Google for privacy violations in the operation of Gmail accounts; the parties settled but before settlement, there were several Motions to File a seal filed by Google and the plaintiffs). Such a motion appeared in the dataset because the original case was an information privacy matter, but the motion was for sealing exhibits deemed as having confidential matters. The "Sealing Motion" did not involve data injury issues at all.

323. *See* Uniloc 2017 LLC v. Microsoft Corp., No. 8:18-CV-02053-AG, 2019 BL 42502, at *1 (C.D. Cal. Feb. 5, 2019) ("Discovery in this action is likely to involve confidential, proprietary, or private information requiring special protection from public disclosure and from use for any purpose other than this litigation. Thus, the Court enters this Protective Order.").

	appear where a party or non-party designates information or items for protection for instance, "protected data," "confidential," "highly confidential—attorney eyes only" or "highly confidential source—source code."[324] These cases were excluded because the issue before the court was often on the privacy of financial records and trade secrets and devoid of personal information privacy violation and the resulting violations which are the subjects under investigation. What is of interest in the research is individual information privacy violation and the resulting litigation in courts.[325]
Cases on terms of service	Cases involving challenges to "Terms and Conditions and Privacy Policy." The challenges brought to court often take a shape of cases where a plaintiff was required to click a box with "I agree to Terms of Use & Privacy Statement" when creating an account or an online account to access a service. The cases in the original dataset that were eliminated would be those that were challenging the "Terms of Use" only as divorced from those that based their issues and or claims on the "privacy policy." All cases that were based on the "Terms and Conditions and Privacy Policy" were carefully reviewed, and the elimination criteria explained above were used before the exclusion or inclusion of such cases in the final dataset.[326]
Motion to proceed under a pseudonym	Opinions on motions to proceed under a pseudonym were excluded. The reason for exclusion is the motions are not based on privacy violation but rather on privacy protection and preservation. The study is on the courts' opinions on injury after a privacy violation. Thus, opinions on motions to proceed anonymously or pseudonymously were excluded. What is often at issue in pseudonym cases is whether the party "has a substantial privacy right which outweighs the customary and constitutionally-embedded presumption of openness in judicial proceedings."[327] These motions are based on the claim that the litigation involves matters that are highly sensitive with personal reasons for which the court should grant a motion to proceed anonymously and that a party's identity and details should be kept confidential.[328] The court would be invited to determine whether the moving party has substantial privacy that outweighs the customary and potentially embedded presumption of openness in judicial proceedings.
Right of publicity cases, trade secrets cases, and trademarks cases	Cases involving competing claims that may be protected by privacy were reviewed and those that could not present typical individual privacy protection were excluded. For instance, cases on the "right of publicity" can be protected under the privacy protection regime. However, the rationale for the inclusion or exclusion of such a case depended on whether the claim for the protection of privacy was for a commercial interest resulting from a violation of the right of publicity for a famous individual but being claimed under the data

324. *Id.*

325. *See, e.g.*, Bingham v. BayCare Health Sys., No: 8:14-CV-73-T-23JSS, 2016 BL 350146, at *2 (M.D. Fla. Oct. 20, 2016) ("The parties each move to file certain exhibits under seal in support of their respective motions for summary judgment on the basis that such exhibits contain confidential or sensitive information protected under the parties' Stipulated Protective Order. The parties do not object to the filing of the designated exhibits under seal.").

326. *See* Davis v. USA Nutra Labs, 303 F. Supp. 3d 1183, 1187, 1189 (D.N.M. 2018) (deciding whether the defendant could compel arbitration and stay proceedings as dictated by a "Terms of Use" agreement, which were often bundled with a "Privacy Statement," but the case in its totality does not discuss any privacy issues).

327. Headhunter, LLC v. Does, No. 5:17-CV-00069, 2018 BL 342583, at *3 (W.D. Va. Sept. 21, 2018).

328. *See* Roe v. Does, No. 20-CV-3788-MKB-SJB, 2020 BL 405855, at *4–19 (E.D.N.Y. Oct. 14, 2020) (evaluating ten factors to determine whether or not a plaintiff is allowed to proceed under a pseudonym).

	privacy law regime. The consideration for elimination was that if the individual was a famous person trying to enforce their commercial interest, such a case would be excluded. The reverse consideration would be a "common man" trying to enforce the right to privacy coupled with the right to publicity. Such cases presented a violation of the owner's right to use and license and would border privacy violation.[329] Cases on trade secrets,[330] trademarks, and copyrights[331] were excluded, especially as they were not aimed at addressing individual privacy violations.

329. *See* The Milton H. Greene Archives, Inc. v. CMG Worldwide, Inc., 568 F. Supp. 2d 1152, 1155 (C.D. Cal. 2008) (asserting, according to the plaintiff, that the Milton Green Archives owned the "right of publicity in Monroe's name, image and likeness;" the actions in the case sought to have the court resolve competing claims as to the ownership of "the legal right to use, license, and distribute certain photographs of Marilyn Monroe"). This case was unique because the United States common law right to privacy is considered a personal right and thus is only applicable to the living and does not recognize the privacy interests of the deceased.

330. *See* Moreland Apartments Assocs. v. LP Equity LLC, No. 5:19-CV-00744-EJD, 2019 BL 6771792, at *7 (N.D. Cal. Dec. 12, 2019) ("[T]he Court, like [the] [d]efendant, are dubious such 'privacy' terms are appropriate in the trade secret context. . . . "[T]he issue in trade secret law is whether the information is secret, someone's expectation of privacy in that information is irrelevant.") (citing Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others.").

331. *See* Sony BMG Music Ent. v. Doe, No. 5:08-CV-109-H, 2008 BL 381545, at *1 (E.D.N.C. Oct. 21, 2009) (discussing an alleged unlawful distribution of music over the internet and, particularly, the defendant's motion to quash a subpoena intended to uncover the identity of the defendant on the ground that it violated his qualified right to anonymous expression under the first amendment; the case had privacy questions, but these questions were not up to the threshold required for this research).