Fordham Law Review

Volume 86 | Issue 5 Article 4

2018

The Hunt for Privacy Harms After *Spokeo*

Matthew S. DeLuca
Fordham University School of Law

The Hunt for Privacy Harms After *Spokeo*

Erratum

Law; Torts; Privacy Law; Courts; Legal Remedies; Litigation; Internet Law; Supreme Court of the United States

NOTES

THE HUNT FOR PRIVACY HARMS AFTER *SPOKEO*

*Matthew S. DeLuca**

In recent years, due both to hacks that have leaked the personal information of hundreds of millions of people and to concerns about government surveillance, Americans have become more aware of the harms that can accompany the widespread collection of personal data. However, the law has not yet fully developed to recognize the concrete privacy harms that can result from what otherwise seems like ordinary economic activity involving the widespread aggregation and compilation of data.

This Note examines cases in which lower federal courts have applied the Supreme Court's directions for testing the concreteness of alleged intangible privacy injuries, and in particular how that inquiry has affected plaintiffs' suits under statutes that implicate privacy concerns. This Note proposes that, in probing the concreteness of these alleged privacy harms, the courts, through the doctrine of standing, are engaging in work that could serve to revitalize the judiciary's long-dormant analysis of the nature of privacy harms. It suggests that courts should look beyond the four traditional privacy torts to find standing for plaintiffs who bring claims against entities that collect and misuse personal information. This Note urges courts to make use of a nexus approach to identify overlapping privacy concerns sufficient for standing, which would allow the federal judiciary to more adequately address emerging privacy harms.

* J.D. Candidate, 2019, Fordham University School of Law; B.A., 2011, Boston College. Google Policy Fellow at the Center for Democracy & Technology, Summer 2017. I would like to thank Professor Joel Reidenberg for his thoughts and consideration. I would also like to thank my family and friends, as well as the editors and staff of the *Fordham Law Review*, without whom this Note would not have been possible.

INTRODUCTION

Americans say they want privacy but are often not quite sure how much and seem unwilling to pay for it.[1] Millions of people send messages, search for information, and post photos using free online services, and frequently give up some personal data in these exchanges.[2]

As a society that privileges the unhampered flow of information,[3] Americans have long sensed a potential tension between values of free

1. Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RES. CTR. (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ [https://perma.cc/R9M3-JRQB]; *see also* Adrienne LaFrance, *The Convenience-Surveillance Tradeoff*, ATLANTIC (Jan. 14, 2016), https://www.theatlantic.com/technology/archive/2016/01/the-convenience-surveillance-tradeoff/423891/ [https://perma.cc/3PS2-9CTN].

2. Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1384–86 (2017); Mark Hachman, *The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers*, PCWORLD (Oct. 1, 2015, 3:00 AM), https://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html [https://perma.cc/MQ4P-CYN3]; *We Want You to Understand What Data We Collect and Use*, GOOGLE, https://privacy.google.com/your-data.html [https://perma.cc/BQL8-6BKU] (last visited Mar. 15, 2018).

3. *See* Whitney v. California, 274 U.S. 357, 373–76 (1927) (Brandeis, J., concurring), *overruled in part by* Brandenburg v. Ohio, 395 U.S. 444 (1969) (per curiam).

expression and the seemingly deep-rooted desire to have certain areas of life remain off limits, not just to government but to prying private parties as well.[4] And even as the internet becomes more solidly imbricated in the routines of work and private life, there appears to be some feeling that perhaps people are being asked to give up too much of their privacy in the process.[5]

This Note examines the way in which these American intuitions—and ambivalences—are very much alive and topics of ongoing debates in the federal courts.[6] The U.S. Supreme Court's holding in *Spokeo, Inc. v. Robins*,[7] a 2016 case in which the Court expounded on the "concreteness" an injury must have to merit access to the federal judiciary,[8] demonstrates the difficulties of this debate and has spurred a new phase in courts' consideration of the nature of privacy harms. As might be expected, the holdings of subsequent cases expose the varied strands, value judgments, and doctrinal failures and successes of American privacy law.

Part I of this Note explores the nature of privacy law in America and the doctrine of standing, along with its constitutional roots. It also outlines the development of what has been referred to as the "data economy,"[9] a robust marketplace built on the collection and processing of massive amounts of data by private enterprises. It begins by providing the background for these two complicated and unresolved areas of law, standing and privacy, and casts them against the rapid growth of commercial enterprises premised on the collection and processing of information. This Part then demonstrates the confrontation between a growing sense[10] of potential harms and the Article III constraints on what sorts of injuries allow access to federal courts. It notes the judicial skepticism that operates as a restraining influence on the development of American privacy law and outlines the Supreme Court's holding in *Spokeo*.

---

4. *See* Paul Gewirtz, *Privacy and Speech*, 2001 SUP. CT. REV. 139, 139–40; Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1160 (2005).

5. *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/PY6J-WK7H].

6. Margot E. Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. REV. 413, 418–19 (2017); Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1362–63 (2017).

7. 136 S. Ct. 1540 (2016).

8. *Id.* at 1548–49.

9. Adam B. Thimmesch, *Transacting in Data: Tax, Privacy, and the New Economy*, 94 DENV. L. REV. 145, 147–48 (2016).

10. Fifty-five percent of respondents to one survey said they decided not to make a purchase online because they were concerned about privacy. *Companies That Fail to See Privacy as a Business Priority Risk Crossing the 'Creepy Line,'* KPMG (Nov. 6, 2016), https://home.kpmg.com/sg/en/home/media/press-releases/2016/11/companies-that-fail-to-see-privacy-as-a-business-priority-risk-crossing-the-creepy-line.html [https://perma.cc/X2CS-SQJN]; *see also* Lee Rainie & Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RES. CTR. (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ [https://perma.cc/9BGR-DPUH] (describing "findings suggesting that Americans are becoming more anxious about their privacy").

Part II notes the various ways that lower courts have applied *Spokeo* to reach standing conclusions when plaintiffs bring claims under statutes that implicate a privacy interest. It addresses the manner in which courts have analyzed statutory privacy interests in relation to common law causes of action when they inspect whether plaintiffs' alleged privacy injuries are sufficiently concrete. This Part also explores the problems that may arise when encouraging courts to explore what this Note refers to as "common law analogues"[11] in the context of privacy claims.

The final section, Part III, suggests that the instruction the Supreme Court gave in *Spokeo* to lower courts—to look to "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts"[12]—may provide an opportunity for a reinvigorated judicial approach to privacy harms. This Part—evoking the historical context of American privacy law, which has often developed in response to changing technology[13]—proposes that *Spokeo* could in fact initiate renewed judicial consideration of the nature of privacy harms, bringing vitality to a long-stagnant area of American jurisprudence. It considers compelling theories of privacy harm advanced by scholars and encourages courts to go beyond the four privacy torts famously laid out by William Prosser.[14] It suggests that *Spokeo* leaves room for courts to look beyond these four torts to other long-recognized harms by examining the place for a nexus approach to identify privacy harms, an approach that can already be observed at work in recent district and circuit court opinions.

I. PRIVACY AND STANDING: BRANDEISIAN BRAIN CHILDREN COLLIDE

In recent years, and certainly since the Supreme Court's decision in *Spokeo*, privacy concerns and the doctrine of standing—the set of initial requirements that plaintiffs must establish to get out of the gate in federal court[15]—appear to have come into conflict.[16] Part I.A outlines the rudiments of standing, including injury in fact. Part I.B sketches the development of American privacy law over the past nearly 130 years and the more recent rapid growth of an economic model for internet businesses based primarily on easily collected data.[17] Part I.C probes the extent to which American

11. This phrase for framing the inquiry is borrowed from the U.S. Court of Appeals for the Fourth Circuit. Dreher v. Experian Info. Sols., Inc., 856 F.3d 337, 345 (4th Cir. 2017). While the phrase is useful, however, it is also somewhat misleading: *Spokeo*'s instruction that courts may look to traditional bases for lawsuits in assessing concreteness does not restrict them to forms of injury recognized at common law. *Spokeo*, 136 S. Ct. at 1549.

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

13. Mary G. Leary, *The Missed Opportunity of* United States v. Jones*: Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 U. PA. J. CONST. L. 331, 351 (2012).

14. *See infra* Part I.B.1.

15. Heather Elliot, *The Functions of Standing*, 61 STAN. L. REV. 459, 465 (2008).

16. Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 439 (2017).

17. *See* Thomas C. Redman, *4 Business Models for the Data Age*, HARV. BUS. REV. (May 20, 2015), https://hbr.org/2015/05/4-business-models-for-the-data-age [https://perma.cc/

judges sometimes exhibit skepticism toward privacy claims. Part I.D then discusses *Spokeo* in detail and draws out the key portions of the opinion as they pertain to plaintiffs who seek to bring statutory privacy claims in federal court.

A. What Is Standing?

In its simplest formulation, standing doctrine demands that plaintiffs who seek to avail themselves of the power of a federal court must, at a minimum, satisfy three requirements before the court will consider the merits of their claims[18]: (1) they must have suffered an injury in fact that is "concrete and particularized" and "actual or imminent," (2) the injury must be traceable to the allegedly unlawful conduct of the defendant, and (3) the injury must have the potential to be effectively redressed by a favorable outcome in the court.[19] These three elements constitute an "irreducible constitutional minimum," a "core component of standing."[20] Challenges to standing can be brought at any time in the course of a suit in federal court because they implicate the court's jurisdiction over the claims.[21] This Note will only consider the first of standing's requirements, injury in fact, which was at issue in *Spokeo* and which, for now, poses a significant hurdle for privacy plaintiffs.[22]

Part I.A.1 below discusses the development of the doctrine of standing. Part I.A.2 particularly examines the requirement of injury in fact.

1. Development of the Doctrine

In explaining its rationale for demanding standing for all cases brought in the federal courts, the Court has said that the three elements of standing are required by the Constitution.[23] The Court has stated that the requirements of standing emanate from Article III's limitation of the federal courts' jurisdiction to "[c]ases" and "[c]ontroversies."[24] The doctrine is justified as

6LUG-SGKU]; Douglas Rushkoff, *When the Data Bubble Bursts, Companies Will Have to Actually Sell Things Again*, FAST COMPANY (May 13, 2016), https://www.fastcompany.com/3059722/when-the-data-bubble-bursts-companies-will-have-to-actually-sell-things-again [https://perma.cc/C9AP-8BB7].

18. Gregory R. Manring, Note, *It's Time for an Intervention!: Resolving the Conflict Between Rule 24(a)(2) and Article III Standing*, 85 FORDHAM L. REV. 2525, 2535–37 (2017).

19. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992); *see also* William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 229 (1988) ("The essence of a true standing question is the following: Does the plaintiff have a legal right to judicial enforcement of an asserted legal duty?"); Robert J. Pushaw, Jr., *Justiciability and Separation of Powers: A Neo-Federalist Approach*, 81 CORNELL L. REV. 393, 395 (1996).

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

21. FED. R. CIV. P. 12(b)(1).

22. *See* Eric S. Boos et al., *Damages Theories in Data Breach Litigation*, 16 SEDONA CONF. J. 125, 126 (2015); Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 539 (2017); Lexi Rubow, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007, 1011–12 (2014).

23. *Lujan*, 504 U.S. at 560–61; *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).

24. *Lujan*, 504 U.S. at 559–61.

a necessary safeguard to ensure that cases are brought in a genuinely adversarial setting that draws in the proper disputing parties, as a check against generalized grievances and advisory opinions, and as a means to ensure that the federal judiciary does not overstep its proper role or impinge on the powers of the elected branches.[25]

While the Court has sometimes spoken in conclusive tones about the elements of standing, at other times it has seemed much more uncertain about whether the outlines of standing can be definitively articulated.[26] While scholars dispute the extent to which standing has always, under other names, been an aspect of Article III jurisdiction,[27] it seems clear that standing as the Court understands it today developed in the early twentieth century and is at least partly attributable to the judicial innovations of Justice Louis Brandeis.[28] While standing doctrine may frequently be viewed today as a judicially imposed barrier for plaintiffs,[29] it began its modern history as a check on judges, a mechanism to make it harder for the Court to strike down democratically enacted statutes amid the growth of the regulatory state.[30]

It was Justice Brandeis who, in 1922, wrote for the Court in *Fairchild v. Hughes*,[31] a case in which a plaintiff sought to have the Nineteenth Amendment declared unconstitutional.[32] The Court found that the plaintiff's claims did not "afford a basis for [the] proceeding."[33] What is now recognized as the first of the three elements of standing, injury in fact, does not appear explicitly in *Fairchild*. A case decided one year later,

25. Fletcher, *supra* note 19, at 222.

26. *Compare Lujan*, 504 U.S. at 560 (stating that "the core component of standing is an essential and unchanging part of the case-or-controversy requirement"), *with* Ass'n of Data Processing Serv. Orgs. v. Camp, 397 U.S. 150, 151 (1970) (declaring that "[g]eneralizations about standing to sue are largely worthless as such"), *and* Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 475 (1982) (observing that "[w]e need not mince words" in saying that the Court has not defined Article III standing "with complete consistency").

27. *See, e.g.*, Richard H. Fallon, Jr., *The Fragmentation of Standing*, 93 TEX. L. REV. 1061, 1064–65 (2015); Fletcher, *supra* note 19, at 224–26; F. Andrew Hessick, *The Separation-of-Powers Theory of Standing*, 95 N.C. L. REV. 673, 679–80 (2017); Laveta Casdorph, Comment, *The Constitution and the Reconstitution of the Standing Doctrine*, 30 ST. MARY'S L.J. 471, 479–81 (1999).

28. "[T]he modern doctrine of standing is a distinctly twentieth century product that was fashioned out of other doctrinal materials largely through the conscious efforts of Justices Brandeis and Frankfurter." Steven L. Winter, *The Metaphor of Standing and the Problem of Self-Governance*, 40 STAN. L. REV. 1371, 1374 (1988); *see also* F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 291 (2008); Cass R. Sunstein, *Standing and the Privatization of Public Law*, 88 COLUM. L. REV. 1432, 1437 (1988).

29. Heather Elliott, *Standing Lessons: What We Can Learn When Conservative Plaintiffs Lose Under Article III Standing Doctrine*, 87 IND. L.J. 551, 563–86 (2012).

30. *Id.* at 557; Richard J. Pierce, Jr., *Is Standing Law or Politics?*, 77 N.C. L. REV. 1741, 1767 (1999); Cass R. Sunstein, *What's Standing After* Lujan*?: Of Citizen Suits, "Injuries," and Article III*, 91 MICH. L. REV. 163, 179–80 (1992).

31. 258 U.S. 126 (1922).

32. *Id.* at 127.

33. *Id.* at 129.

Frothingham v. Mellon,[34] is generally pointed to as the first modern standing case.[35]

The Court in *Frothingham* faced, in part, a taxpayer challenge to the Maternity Act, which directed funds to the states with the purpose of improving health care and reducing mortality rates for mothers and newborns.[36] The civilian plaintiff alleged that the additional taxes to support the Act would "increase the burden of future taxation and thereby take her property without due process of law."[37] Stating that the Court had never before directly decided this issue, and that the question had theretofore passed "sub silentio" or that the determination of it had been "expressly withheld,"[38] the Court held that taxpayer status alone was not sufficient to present a justiciable issue.[39] Grounding its reasoning on a separation-of-powers rationale, the Court said that it may "review and annul acts of Congress" as violations of the Constitution only when a plaintiff alleged "some direct injury suffered or threatened, presenting a justiciable issue."[40]

2. Injury in Fact

The first Supreme Court case to explicitly demand injury in fact as a requirement for standing was *Ass'n of Data Processing Service Organizations v. Camp*.[41] The petitioners in that case were in the business of selling data-processing services.[42] The Court declared that the primary question in determining whether a plaintiff has established standing is whether the plaintiff alleges an "injury in fact, economic or otherwise."[43] This injury-in-fact requirement has remained a basic element of the Article III standing analysis ever since it developed within the administrative law context presented in *Data Processing*.[44]

Since injury in fact's full-fledged arrival in *Data Processing*, judges have had to determine what sorts of injury should even be visible to the discriminating eye of the judiciary.[45] Scholars have argued that Justice Antonin Scalia's formulation of injury in fact as laid out for the Court in

34. 262 U.S. 447 (1923).

35. Karl S. Coplan, *Ideological Plaintiffs, Administrative Lawmaking, Standing, and the Petition Clause*, 61 ME. L. REV. 377, 427–28 (2009); Linda Sandstrom Simard, *Standing Alone: Do We Still Need the Political Question Doctrine?*, 100 DICK. L. REV. 303, 309 n.35 (1996).

36. *Frothingham*, 262 U.S. at 479.

37. *Id.* at 486.

38. *Id.*

39. *Id.* at 488.

40. *Id.*

41. 397 U.S. 150 (1970); *see id.* at 152; Kimberly N. Brown, *Justiciable Generalized Grievances*, 68 MD. L. REV. 221, 237 n.79 (2008); Fletcher, *supra* note 19, at 230.

42. *Data Processing*, 397 U.S. at 151.

43. *Id.* at 152.

44. Fletcher, *supra* note 19, at 230.

45. Courtney M. Cox, *Risky Standing: Deciding on Injury*, 8 NE. U. L.J. 75, 94–95 (2016).

Lujan v. Defenders of Wildlife[46] tightened the requirements[47] by providing that a congressional grant of standing, in this case in the Endangered Species Act, was inadequate for Article III purposes.[48]

B. The Evolving Nature of Privacy Harms

Theoretical justifications for privacy law have ranged from "the right to be let alone" to a right to control information about one's self.[49] The task of defining the harm has an important role in privacy law.[50] Part I.B.1 discusses the development of privacy law in America, and Part I.B.2 explores the growth of an economic model dependent on the acquisition of data. Part I.B.3 introduces the challenges that face privacy plaintiffs attempting to secure standing in federal court.

1. The Path of American Privacy Law

The very idea of privacy law has a decidedly "uneven history" in America.[51] While the common law privacy torts form an important part of the story of American privacy law,[52] the federal court system, and in particular the Supreme Court and its Justices, has been intimately involved in concerns about privacy, and technological encroachments upon it, for more than a century.[53] It was future Supreme Court Justice Brandeis who, along with Samuel Warren, penned the 1890 *Harvard Law Review* article[54] that

46. 504 U.S. 555 (1992).

47. Seth F. Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 750 (2016); Zachary D. Sakas, *Footnotes, Forests, and Fallacy: An Examination of the Circuit Split Regarding Standing in Procedural Injury-Based Programmatic Challenges*, 13 U. BALT. J. ENVTL. L. 175, 185 (2006). In a law review article published before he became a Supreme Court Justice, Antonin Scalia argued that standing doctrine is a "crucial and inseparable element" of the principle of separation of powers. Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 881 (1983). Scalia wrote that standing achieves this by enforcing a boundary "restricting the courts to their assigned role of protecting minority rather than majority interests." *Id.* at 895. Justice Sandra Day O'Connor, who wrote in *Allen v. Wright*, 468 U.S. 737 (1984), that "the law of Art[icle] III standing is built on a single basic idea—the idea of separation of powers," *id.* at 752, joined Justice Harry Blackmun's *Lujan* dissent, which criticized Justice Scalia's majority opinion for its "anachronistically formal view of the separation of powers," *Lujan*, 504 U.S. at 602 (Blackmun, J., dissenting).

48. Richard J. Pierce, Jr., Lujan v. Defenders of Wildlife*: Standing as a Judicially Imposed Limit on Legislative Power*, 42 DUKE L.J. 1170, 1172–73 (1993).

49. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1099–111 (2002).

50. Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 889 (2000).

51. Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 432 (2017).

52. Don Corbett, *Virtual Espionage: Spyware and the Common Law Privacy Torts*, 36 U. BALT. L. REV. 1, 18–19 (2006).

53. Kyllo v. United States, 533 U.S. 27, 34 (2001) (asking "what limits there are upon this power of technology to shrink the realm of guaranteed privacy"); United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting) ("Electronic surveillance is the greatest leveler of human privacy ever known."); Lopez v. United States, 373 U.S. 427, 441 (1963) (Warren, C.J., concurring) ("[T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual.").

54. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (citing "[r]ecent inventions and business methods" as motivating a need for legal recognition of privacy concerns).

"[o]ut of a few scraps of precedent . . . invented a brand-new tort, invasion of privacy."[55] Brandeis would weave his developing vision of privacy into his opinions once on the Court.[56] For example, in his famous dissent in *Olmstead v. United States*,[57] a prohibition-era wire-tapping case, Brandeis forewarned of the invasions of privacy that could come with "[a]dvances in the psychic and related sciences [that] may bring means of exploring unexpressed beliefs, thoughts and emotions."[58]

Seventy years after Warren and Brandeis published their article, famed torts scholar William Prosser set out to map the spread of the right they identified and reviewed more than three hundred cases that had arisen in the intervening decades.[59] Prosser announced that the law of privacy was made up of four interests that could be invaded in four distinct ways: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light, and (4) appropriation of an individual's name or likeness.[60]

The law has never quite gone so far as to fully enforce what Warren and Brandeis referred to as "the right 'to be let alone.'"[61] Privacy law such as it exists in the United States today consists of a mix of federal and state statutes, along with common law torts.[62] Privacy statutes tend to be scattered and of limited scope.[63] The small handful of federal statutes targets a range of specific privacy concerns and includes the Fair Credit Reporting Act of 1970 (FCRA),[64] the Electronic Communications Privacy Act of 1986 (ECPA),[65] the Video Privacy Protection Act of 1988 (VPPA),[66] and the Telephone Consumer Protection Act of 1991 (TCPA).[67] Many states have either codified the privacy torts in statute or recognize them under common law.[68]

The law has long identified a tension between the desire to enforce a zone of personal privacy and other core principles of American law, including the First Amendment.[69] Privacy has nestled most comfortably into the law where

---

55. LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 548 (1973); *see also* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1345 (describing Justices Warren and Brandeis's handiwork as "light on hard precedent, but full of optimism").

56. Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1331 (2010).

57. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

58. *Id.* at 474 (Brandeis, J., dissenting).

59. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 388–89 (1960).

60. RESTATEMENT (SECOND) OF TORTS §§ 652A–E (AM. LAW INST. 1977); Prosser, *supra* note 59, at 389.

61. Warren & Brandeis, *supra* note 54, at 195.

62. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 483 (2006).

63. Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 881 (2003) (stating that statutes "address specific elements of fair information practices").

64. 15 U.S.C. § 1681 (2012).

65. 18 U.S.C. §§ 2510–2522 (2012).

66. 18 U.S.C. § 2710 (2012).

67. 47 U.S.C. § 227 (2012).

68. Matthew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 105 (2002).

69. *See* John A. Humbach, *Privacy and the Right of Free Expression*, 11 FIRST AMEND. L. REV. 16, 26–28 (2012); Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 132–33 (2000).

it protects individual interests against government power,[70] and so the Court has spoken out more forcefully for individual privacy in the context of Fourth Amendment rights.[71] There, the assertion of privacy rights has sat more agreeably alongside interests that Anglo-American law has thoroughly metabolized, such as the sanctity of the home[72] and the right to be free from "unreasonable governmental prying."[73] The Court has observed that "a person's *general* right to privacy . . . is, like the protection of his property and of his very life, left largely to the law of the individual States."[74]

The reluctance of the law to fully embrace privacy has been given expression by some scholars and jurists who argue that the costs of privacy are too high.[75] Privacy is seen, in many instances in which it is asserted, as little more than a desire that others not obtain information that one would rather others not possess.[76] Critics of asserted privacy rights contend that keeping privacy protections out of the law, or keeping such protections very narrowly tailored, has social benefits, including protecting broad freedom of expression[77] and allowing increased economic uses of information.[78] Indeed, one scholar has argued that the relative absence of American privacy laws may have been an important condition for the development of the commercial internet.[79] A counterpoint is provided by both the experience of European nations (which tend to have both an active internet and stricter privacy regulation) and independent research that indicates that the lack of privacy protections may make individuals reluctant to use the internet.[80]

---

70. "To Americans, the starting point for the understanding of the right to privacy is of course to be sought in the late eighteenth century, and especially in the Bill of Rights . . . ." James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1211–12 (2004). "In particular, 'privacy' begins with the Fourth Amendment: At its origin, the right to privacy is the right against unlawful searches and seizures." *Id.* at 1212.

71. *See* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 115–16 (2008).

72. Kyllo v. United States, 533 U.S. 27, 31 (2001).

73. Rakas v. Illinois, 439 U.S. 128, 166 (1978) (White, J., dissenting).

74. Katz v. United States, 389 U.S. 347, 350–51 (1967).

75. *See* BENJAMIN WITTES & JODIE C. LIU, THE PRIVACY PARADOX: THE PRIVACY BENEFITS OF PRIVACY THREATS 8 (2015), https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf [https://perma.cc/ERK9-XT2Y]; Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394 (1978); Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 88 (2001) ("[L]aws regulating privacy chill the creation of beneficial collective goods and erode social values.").

76. Grant Gross, *Judge: Give NSA Unlimited Access to Digital Data*, PCWORLD (Dec. 4, 2014, 1:46 PM), https://www.pcworld.com/article/2855776/judge-give-nsa-unlimited-access-to-digital-data.html [https://perma.cc/ZV5S-GSJB] (quoting Judge Posner as stating that "[m]uch of what passes for the name of privacy is really just trying to conceal the disreputable parts of your conduct").

77. *See* Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35, 51 (2002); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050–51 (2000).

78. Walker, *supra* note 75, at 88.

79. *See* Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 667 (2014) (describing "[t]he absence of privacy constraints" as "especially conducive to [i]nternet innovation").

80. *See* Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 434–35 (2014); Will Yakowicz, *Two-Thirds*

2. The Growth of the Data Economy

Information, even of imperfect quality, has long been valuable, even if it has not always been understood as a commodity.[81] The expansion of credit-reporting agencies in the late nineteenth century struck some contemporary observers as an extremely worrisome form of public snooping.[82] The development of the commercial internet made the collection and aggregation of information on a mass scale simpler and more lucrative. Today, personal data is gathered, mined, and marketed by companies large and small on a regular basis.[83] Household-name companies like Google and Facebook, as well as smaller enterprises,[84] hold vast troves of data, which power an economy premised on the collection of personal information.[85] With those stores of data comes a risk of disclosure, whether as the result of a hack or other form of breach,[86] as well as the possibility that a company or other entity may make use of the collected data in an unlawful manner.

---

of Customers Are Worried About Security While Shopping Online, INC. (Oct. 19, 2015), https://www.inc.com/will-yakowicz/survey-66-percent-customers-worried-id-theft-shopping-online.html [https://perma.cc/VS3U-XZ3W].

81. *See, e.g.*, HOMER, THE ODYSSEY 86 (Robert Fagles trans., Penguin Books 1996) (noting "rumor that carries news to men like nothing else").

82. *See, e.g.*, Sarah Jeong, *Credit Bureaus Were the NSA of the 19th Century*, ATLANTIC (Apr. 21, 2016), https://www.theatlantic.com/technology/archive/2016/04/mass-surveillance-was-invented-by-credit-bureaus/479226/ [https://perma.cc/MN4X-G2V5].

83. *See* Elizabeth Dwoskin & Craig Timberg, *Google Now Knows When Its Users Go to the Store and Buy Stuff*, WASH. POST (May 23, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/ [https://perma.cc/AN5Z-SRZF].

84. Michel Falcon, *You Can Collect Customer Data and Deliver a Better Experience Without Violating Privacy*, ENTREPRENEUR (July 31, 2017), https://www.entrepreneur.com/article/296270 [https://perma.cc/9S3K-AAWY]; Mike Montgomery, *Small Businesses Shouldn't Fear Big Data*, FORBES (May 7, 2015, 1:18 PM), https://www.forbes.com/sites/mikemontgomery/2015/05/07/small-businesses-shouldnt-fear-big-data/ [https://perma.cc/K5XB-4NBF]; Phil Simon, *Even Small Companies Can Tap Big Data If They Know Where to Look*, HARV. BUS. REV. (Dec. 16, 2013), https://hbr.org/2013/12/even-small-companies-can-tap-big-data-if-they-know-where-to-look [https://perma.cc/5YYB-FRS3].

85. *See* Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71, 71 (2016); Cate, *supra* note 50, at 888–89; Franks, *supra* note 51, at 454 ("Cell phone carriers, social media applications, and search engines now possess huge troves of user information."); Sheri B. Pan, Note, *Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze*, 30 HARV. J.L. & TECH., 239, 245 (2016) ("As more collection becomes constant, it is also increasingly imperceptible."); *see also In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 266 (3d Cir. 2016) (describing the "data-collecting infrastructure" of the internet that "hums along quietly in the background"); *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *1 (N.D. Cal. Dec. 3, 2013) (noting that Google's free products "turn a healthy profit . . . rely[ing] in substantial part on users' personal identification information"); Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016, 2:30 PM), http://www.newsweek.com/secretive-world-selling-data-about-you-464789 [https://perma.cc/F3A2-2ZCX].

86. *See* Selena Larson, *The Hacks That Left Us Exposed in 2017*, CNN (Dec. 20, 2017, 9:11 AM), http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html [https://perma.cc/KK8P-GGGS].

Whether individuals use smartphone applications,[87] go out to eat at popular restaurants,[88] or wear certain activity-tracking devices,[89] private persons, if they want to avail themselves of the promises of new technologies, often have little choice[90] but to hand over a variety of detailed information, such as their social security numbers and dates of birth, as well as potentially more intimate details—including their location[91] or searches they conduct over the internet[92]—to companies that may profit off that information.

With the growth of the commercial internet, companies realized a potential to gather more information for profitable use.[93] DoubleClick, for example, emerged in the late 1990s and became the internet's dominant advertising service by offering targeted ads based on profiles the company built of internet users.[94] Today, individuals effectively pay for some of the world's most popular online services by handing over information about themselves.[95] The collection of data has gone beyond the accumulation of

87. Kaveh Waddell, *When Apps Secretly Team Up to Steal Your Data*, ATLANTIC (Apr. 7, 2017), https://www.theatlantic.com/technology/archive/2017/04/when-apps-collude-to-steal-your-data/522177/ [https://perma.cc/7QN8-ZCQD].

88. Karen Stabiner, *To Survive in Tough Times, Restaurants Turn to Data Mining*, N.Y. TIMES (Aug. 25, 2017), https://www.nytimes.com/2017/08/25/dining/restaurant-software-analytics-data-mining.html [https://perma.cc/PPL7-8XDH].

89. Jenna McLaughlin, *How the Spies Learned to Stop Worrying and Love Fitbit*, FOREIGN POL'Y (Feb. 1, 2018, 12:38 PM), http://foreignpolicy.com/2018/02/01/how-the-spies-learned-to-stop-worrying-and-love-fitbit/ [https://perma.cc/8W6Q-4GSG].

90. The lack of meaningful choice to participate in an economic system that relies in large part on the disclosure of personal information was observed by one Supreme Court Justice four decades ago. United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting) ("[T]he disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account.").

91. Gil Aegerter, *License Plate Data Not Just for Cops: Private Companies Are Tracking Your Car*, NBC NEWS (July 19, 2013, 4:44 AM), https://www.nbcnews.com/news/other/license-plate-data-not-just-cops-private-companies-are-tracking-f6C10684677 [https://perma.cc/XK88-AL7C]; Jessica Leber, *How Wireless Carriers Are Monetizing Your Movements*, MIT TECH. REV. (Apr. 12, 2013), https://www.technologyreview.com/s/513016/how-wireless-carriers-are-monetizing-your-movements/ [https://perma.cc/Y5NG-RZ4Y].

92. Dan Gillmor, *As We Sweat Government Surveillance, Companies Like Google Collect Our Data*, GUARDIAN (Apr. 18, 2014, 12:31 PM), https://www.theguardian.com/commentisfree/2014/apr/18/corporations-google-should-not-sell-customer-data [https://perma.cc/ZDW4-AJ32]; Bruce Schneier, *'Stalker Economy' Here to Stay*, CNN (NOV. 26, 2013), http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/index.html [https://perma.cc/S4NB-BMBB].

93. "Personalization is the new religion of the information society, and the quant jocks of Big Data are its high priests." Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1923 (2013); *see also Getting to Know You*, ECONOMIST (Sept. 11, 2014), https://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party [https://perma.cc/9R42-5XM5].

94. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502 (S.D.N.Y. 2001).

95. *The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource [https://perma.cc/E4QT-728W]; *see also* Franks, *supra* note 51, at 454 ("Google and Facebook are not in fact free services, but rather platforms that essentially trade in users' private information."); Catherine Tremble, Note, *Wild Westworld: Section 230 of the CDA and Social Networks' Use of Machine-Learning Algorithms*, 86 FORDHAM L. REV. 825, 839 (2017).

details like names, addresses, and social security numbers; companies can pan through a flood of videos, photos, social media postings, location information, and other sources of data generated through the use of technology.[96] This constant flow of information, and the insights and revenues it can generate for businesses, has led to data being described as the "oil" of the modern economy.[97]

Recognizing this potential, businesses have for years identified their data stores as among their most prized assets.[98]

3. A "Kilimanjaro" for Privacy Plaintiffs?

While the expansion of this fecund data economy has met little legal or political resistance,[99] plaintiffs who have brought claims under a statute alleging privacy-right violations in federal court have sometimes faced an uphill battle.[100]

Standing doctrine has long been most comfortable with "tangible" injuries: the economic, physical, or other harms that the legal community of lawyers and judges can label and assess.[101] But the necessity of a "concrete, living

---

96. *Data Is Giving Rise to a New Economy*, ECONOMIST (May 6, 2017), https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy [https://perma.cc/JE9L-27AK].

97. *Id.*; *see also* Ben Tarnoff, *Silicon Valley Siphons Our Data Like Oil. But the Deepest Drilling Has Just Begun*, GUARDIAN (Aug. 23, 2017, 4:00 AM), https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook [https://perma.cc/A6W4-JFYA]; Ajay S. Banga, *A Global Economy Powered by Data*, WORLD ECON. F. (Jan. 27, 2016), https://www.weforum.org/agenda/2016/01/a-global-economy-powered-by-data [https://perma.cc/RP23-5MZ7] ("Just as steam powered much of the First Industrial Revolution, the free flow of data will be fundamental to powering what the World Economic Forum and others are calling the Fourth Industrial Revolution.").

98. Douglas Laney, *Infonomics: The Practice of Information Economics*, FORBES (May 22, 2012, 11:44 AM), https://www.forbes.com/sites/gartnergroup/2012/05/22/infonomics-the-practice-of-information-economics/#1d3608626ee4 [https://perma.cc/GY72-8NKY]; *see also* Alan Lewis & Dan McKone, *To Get More Value from Your Data, Sell It*, HARV. BUS. REV. (Oct. 21, 2016), https://hbr.org/2016/10/to-get-more-value-from-your-data-sell-it [https://perma.cc/GJ7H-M43F] ("Many companies guard their data as their crown jewels."); *The Rise of Data Capital*, MIT TECH. REV. 4 (Mar. 21, 2016), http://files.technologyreview.com/whitepapers/MIT_Oracle+Report-The_Rise_of_Data_Capital.pdf [https://perma.cc/BG6M-J8R5] ("Data capital is one of the most important assets of every online consumer service created in the past decade."). By contrast, technologist and security expert Bruce Schneier has argued in light of major data breaches that "data is a toxic asset and saving it is dangerous." Bruce Schneier, *Data Is a Toxic Asset, so Why Not Throw It Out?*, CNN (Mar. 1, 2016, 7:12 AM), http://www.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html [https://perma.cc/5R6Q-5NL8].

99. *See* Farhad Manjoo, *Can Washington Stop Big Tech Companies?: Don't Bet on It*, N.Y. TIMES (Oct. 25, 2017), https://www.nytimes.com/2017/10/25/technology/regulating-tech-companies.html [https://perma.cc/DT6Y-SAZV].

100. Wu, *supra* note 16, at 439; *see also In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *4 (N.D. Cal. Dec. 3, 2013) ("[E]ven though injury-in-fact may not generally be Mount Everest . . . in data privacy cases in the Northern District of California, the doctrine might still reasonably be described as Kilimanjaro.").

101. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete."); Coleman v. Miller, 307 U.S. 433, 460

contest between adversaries"[102] has not prevented standing doctrine from recognizing intangible harms as valid for Article III purposes.

While the intangibility of alleged privacy harms may often count against them, some commentators have noted, by way of comparison, the way intangible harms—implicated in torts such as loss of consortium or breach of confidence—are routinely recognized by the courts.[103] One prominent past recognition of standing for an intangible injury was in *FEC v. Akins*,[104] in which the Court said that the denial of information to which the plaintiffs were entitled under the Federal Election Campaign Act (FECA) constituted injury in fact.[105] And the Court in *Spokeo* cited free speech and free exercise cases to support its reaffirmation of the principle that intangible injuries can be sufficiently concrete.[106]

At the same time, the bar for privacy harms appears to be elevated.[107] One scholar has perceived a shift away from asking "whether the plaintiff before the court [is] the right plaintiff" to asking whether "the harm caused by the defendant is the right kind of harm."[108] The move toward questioning the cognizability of some alleged privacy harms was occurring in the lower courts before *Spokeo*.[109]

C. Judicial Skepticism of Privacy Harms

Courts before *Spokeo* were already weighing the many ways in which plaintiffs allege data-related privacy harms.[110] For example, there currently exists a circuit split that developed before *Spokeo* on whether a plaintiff can allege as a cognizable injury in fact the increased future risk of identity theft after a data breach.[111] In reviewing the development of privacy as a legal concern in the United States, commentators have noted the way in which the

---

(1939) (Frankfurter, J., concurring) (describing the "expert feel of lawyers" in assessing what constitutes a case or a controversy); *see also* Hein v. Freedom from Religion Found., Inc., 551 U.S. 587, 619 (2007) (Scalia, J., concurring) (discussing "Wallet Injury" as opposed to "Psychic Injury").

102. *Coleman*, 307 U.S. at 460.

103. "[I]n other areas of the law, conceptions of harm have evolved to recognize injury that is hard to see or measure. This is true for pain and suffering, loss of consortium, and other matters that are not easily translated into monetary terms." Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 756 (2018); *see also* Wu, *supra* note 16, at 439.

104. 524 U.S. 11 (1998).

105. Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 638 (1999).

106. *Spokeo*, 136 S. Ct. at 1549 (citing Pleasant Grove City v. Summum, 555 U.S. 460 (2009); Church of Lukumi Babalu Aye, Inc. v. Hialeah, 508 U.S. 520 (1993)).

107. Kaminski, *supra* note 6, at 416.

108. Wu, *supra* note 16, at 439.

109. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011); Wu, *supra* note 16, at 447.

110. Solove & Citron, *supra* note 103, at 744 (observing that for some judges "recognizing data-breach harms is akin to attempting to tap dance on quicksand, with the safest approach being to retreat to the safety of the most traditional notions of harm").

111. *Compare* Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (concluding that the plaintiffs had not established standing), *with* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696–97 (7th Cir. 2015) (holding that standing had been properly established regarding future risk of identity theft).

accretive processes that have contributed to privacy law have often been catalyzed by radical upsets in technology and society.[112]

At the same time, while noting this hesitancy in the legal community, it is wrong to suggest that American judges, or the citizenry for that matter, are indifferent to privacy concerns.[113] It may be that the judiciary's reluctance to jump to recognizing privacy harms is, at least in part, bound up in the way in which privacy wended its way into American law in the first place.

The word "privacy" appears nowhere in the Constitution.[114] Causes of action against, for example, eavesdropping (alongside extrajudicial self-remedies, such as dueling) provided some protection in preconstitutional America for what may be understood today as privacy interests. The famous 1763 case *Wilkes v. Wood*[115] captured the colonial imagination as a paradigmatic instance of unlawful government intrusion.[116] Since then, one scholar has summed up some of the privacy interests embedded in the Constitution as including, among others, protections for personal religious practices, private property, and some economic activity.[117] The Court has recognized that the Constitution provides protections for personal privacy against intrusion by the government.[118]

The privacy torts as they are recognized today are another matter. Neil Richards and Daniel Solove have pointed to the pivotal role that Prosser played in systematizing and raising the status of the privacy torts as a prime factor in privacy law's relative nonresponsiveness to social change over the decades since Prosser's article.[119] While Prosser's review of hundreds of cases implicating privacy, which led to his sorting them into four cognizable privacy torts, played a hugely influential role in gaining legitimacy for privacy as a distinct legal interest,[120] it also may have sapped the "generative and creative energy sparked by the Warren and Brandeis article," leaving privacy to calcify in the face of the technological changes of recent

112. "The key to understanding legal privacy as it has developed over 100 years of American life . . . is to understand that its meaning is heavily driven by the events of history." Gormley, *supra* note 55, at 1340. "The most distinctive characteristic of privacy—which can be gleaned from a hundred-year examination of the cases—is its heavy sensitivity to historical triggers." *Id.* at 1439; *see also* Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 89 (2008); Julia M. MacAllister, Note, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2462 (2017).

113. *See* Whitman, *supra* note 70, at 1158 ("It is simply false to say that privacy doesn't matter to Americans.").

114. Reidenberg, *supra* note 63, at 879.

115. (1763) 98 Eng. Rep. 489 (CP).

116. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 772 (1994); Sprague, *supra* note 112, at 94.

117. Sprague, *supra* note 112, at 102.

118. Katz v. United States, 389 U.S. 347, 350 (1967).

119. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1889 (2010). Prosser may have been keen on bolstering what he saw as more promising fledgling torts, such as intentional infliction of emotional distress, and Richards and Solove observe that Prosser seems to have been concerned that these might be "swallowed up by privacy." *Id.* at 1908–09.

120. *Id.* at 1888.

decades.[121] But Prosser alone cannot bear the blame for the judiciary's skeptical approach to privacy concerns.[122] His privacy torts have cast their long shadow because courts, Richards and Solove argue, enthusiastically embraced Prosser's categories and "stopped engaging in the dynamic creative activity" that had accompanied earlier judicial exploration of alleged privacy harms.[123]

But judges have also found ways to view privacy harms that are more in keeping with traditional notions of what an injury should look like. So, for example, some courts have felt comfortable reaching for a decrease in a smartphone's battery charge as an adequate injury when a plaintiff alleged that a party's data-collection activities caused their phone battery to drain more rapidly.[124]

Some privacy concerns have also long been seen as conflicting with First Amendment values.[125] If enthusiasts say data are the oil of the information economy, then the free exchange of facts and opinions is the oil of a vibrant democratic republic.[126]

Richards argues that, even for Brandeis, the organization of the tort law of privacy seems to have been a secondary concern over the course of Brandeis's wide-ranging career—less important than what the Justice saw as the socially salubrious "duty of publicity."[127] Richards suggests that, as his thought matured, Brandeis himself grew to favor a conception of privacy founded on the Constitution and not on tort—a form of "intellectual privacy."[128] This conceptualization supported, rather than undermined, First Amendment values by "protect[ing] individuals' emotional and intellectual processes so that they can think for themselves."[129]

D. Spokeo *and Its Holding*

Part I.D.1 outlines the key portions of the Supreme Court's *Spokeo* decision. Part I.D.2 provides background on what the parties to the case and amici curiae saw at stake in *Spokeo*. Last, Part I.D.3 asks what, if any, change *Spokeo* brought about in federal standing doctrine.

---

121. *Id.* at 1890–91.

122. Rodney A. Smolla, *Accounting for the Slow Growth of American Privacy Law*, 27 NOVA L. REV. 289, 289–90 (2002); Robert M. Connallon, Comment, *An Integrative Alternative for America's Privacy Torts*, 38 GOLDEN GATE U. L. REV. 71, 82–83 (2007).

123. Richards & Solove, *supra* note 119, at 1917.

124. *In re* Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013); Goodman v. HTC Am., Inc., No. C11-1793MJP, 2012 WL 2412070, at *5 (W.D. Wash. June 26, 2012).

125. *See supra* note 75 and accompanying text.

126. *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 663 (1994); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 266 (1964).

127. Richards, *supra* note 56, at 1310–11.

128. *Id.* at 1343.

129. *Id.* at 1342.

1. The Supreme Court's Decision

The Supreme Court decided *Spokeo* in May 2016.[130] The much-anticipated[131] case arose from claims brought by the plaintiff, Robins, under the FCRA.[132] Spokeo runs a website that can be used to generate reports on individuals by gathering information including age, address, and data on more personal matters, including income.[133] Robins alleged that Spokeo maintained a report on him that contained numerous inaccuracies and that Spokeo thereby was in violation of FCRA.[134]

Robins brought claims under the FCRA provisions that provide that consumer reporting agencies "follow reasonable procedures to assure maximum possible accuracy" of consumer reports[135] 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.[136]

The Supreme Court did not directly address the question "[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."[137] The Court instead held that the Ninth Circuit erred by finding standing based on Robins's alleged particularized injury and by failing to consider whether the injury was also concrete.[138]

2. Disagreement over What Was at Stake in *Spokeo*

Amicus briefs filed in *Spokeo* by privacy groups and members of private industry took different views on the nature of the data-driven activity at issue in the case. Privacy advocates, as well as the U.S. Solicitor General,[139] argued that the FCRA's private right of action played an important role in regulating the uses companies make of the data that they collect.[140]

Industry voices, on the other hand, foresaw a rush of "no-injury class action lawsuits" that "could threaten nearly every aspect of the U.S.

130. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016).
131. Editorial, *Justices Should Let an Online Privacy Case Proceed*, N.Y. TIMES (Oct. 31, 2015), https://www.nytimes.com/2015/11/01/opinion/sunday/justices-should-let-a-online-privacy-case-proceed.html [https://perma.cc/85TS-6C8P].
132. *Spokeo*, 136 S. Ct. at 1544.
133. *Id.* at 1546.
134. *Id.*
135. 15 U.S.C. § 1681e(b) (2012).
136. *Spokeo*, 136 S. Ct. at 1545 (quoting 15 U.S.C. § 1681n(a)).
137. Petition for a Writ of Certiorari at i, *Spokeo*, 136 S. Ct. 1540 (No. 13-1339).
138. *Spokeo*, 136 S. Ct. at 1549.
139. Brief for the United States as Amicus Curiae Supporting Respondent at 27, *Spokeo*, 136 S. Ct. 1540 (No. 13-1339) ("That interest is particularly salient given the modern proliferation of large databases and the ease and rapidity of Internet transmissions.").
140. Brief for Amici Curiae Center for Democracy & Technology et al. in Support of Respondent at 15, *Spokeo*, 136 S. Ct. 1540 (No. 13-1339).

economy."[141] Google, Yahoo!, Twitter, LinkedIn, and Netflix were among the technology companies that signed on to a brief in which they argued that their businesses were "uniquely vulnerable to the untoward consequences of the Ninth Circuit's misreading of Article III."[142] The amici noted that their "successful innovations and use of easily replicated computer processes allow billions of people to benefit from the valuable services and products they provide, usually at little or no cost to consumers."[143] In another brief, amici media companies argued that a strict injury-in-fact line would help ward off abusive class action suits.[144]

3. Did *Spokeo* Change Anything?

One legal observer described the Court's narrow holding in *Spokeo* as "somewhat of a disappointment."[145] At least some courts have not been convinced that *Spokeo* represents a substantial shift in the Supreme Court's standing jurisprudence.[146] One circuit assessed *Spokeo*'s influence as casting a renewed focus for courts on examining subject matter jurisdiction when it appears that a plaintiff may be alleging merely a bare procedural violation of a statute.[147] One district court has described *Spokeo* as laying out a "blueprint" for assessing the concreteness of an alleged injury but said that the Supreme Court's opinion merely had recited standard conceptions of the injury-in-fact requirement.[148] Another district court summed up *Spokeo* as "offer[ing] useful guidance."[149] These differing conceptions about precisely what *Spokeo* means, and whether or not it develops pre-existing law, appear to be *Spokeo*'s most significant short-term legacies.[150]

---

141. Brief of Amicus Curiae Consumer Data Industry Association in Support of Petitioner at 3–4, *Spokeo*, 136 S. Ct. 1540 (No. 13-1339).

142. Brief for Amici Curiae eBay Inc. et al. in Support of Petitioner at 5, *Spokeo*, 136 S. Ct. 1540 (No. 13-1339).

143. *Id.* at 6.

144. Brief for Amici Curiae Time Inc. and Seven Media Organizations in Support of Petitioner at 24, *Spokeo*, 136 S. Ct. 1540 (No. 13-1339).

145. Amy Howe, Opinion, *Case on Standing and Concrete Harm Returns to the Ninth Circuit, at Least for Now*, SCOTUSBLOG (May 16, 2016, 6:45 PM), http://www.scotusblog.com/2016/05/opinion-analysis-case-on-standing-and-concrete-harm-returns-to-the-ninth-circuit-at-least-for-now/ [https://perma.cc/3KLJ-6Y34].

146. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 637–38 (3d Cir. 2017) ("[W]e do not believe that the Court so intended to change the traditional standard for the establishment of standing."); Thomas v. FTS USA, LLC, 193 F. Supp. 3d 623, 629 (E.D. Va. 2016) ("*Spokeo* did not change the basic requirements of standing."); *see also* Michael G. McLellan, *Finding a Leg to Stand on:* Spokeo, Inc. v. Robins *and Statutory Standing in Consumer Litigation*, 31 ANTITRUST 49, 49–50 (2017).

147. Katz v. Donna Karan Co., 872 F.3d 114, 118 (2d Cir. 2017).

148. Aranda v. Caribbean Cruise Line, Inc., 202 F. Supp. 3d 850, 855 (N.D. Ill. 2016).

149. Ruk v. Crown Asset Mgmt., LLC, No. 1:16-CV-3444-LMM-JSA, 2017 WL 3085282, at *3 (N.D. Ga. Mar. 22, 2017).

150. In December 2017, after the Ninth Circuit again ruled in favor of Robins's standing, Spokeo filed a second petition for a writ of certiorari in the Supreme Court. Petition for Writ of Certiorari, Spokeo, Inc. v. Robins, No. 17-806, 2018 WL 3085282 (Jan. 22, 2018). The petitioners wrote that "hundreds of lower courts [had] adopted conflicting interpretations" of the Court's standard expressed in *Spokeo* and asked the Court to address "widespread

II. COURTS SEARCH FOR PRIVACY HARMS AFTER *SPOKEO*

While the case was only decided in 2016, one result of *Spokeo* now seems assured: it introduced fresh layers of confusion in an area of the law—privacy claims—that was already rife with uncertainty.[151] A string of cases decided in both the circuit courts of appeals and the federal district courts since *Spokeo* have addressed standing challenges that arose after plaintiffs brought claims pursuant to a statute that implicated a privacy concern.[152]

Part II details significant cases that have been decided since *Spokeo* and examines the way in which they follow the Supreme Court's suggestions to test the concreteness of intangible injuries. Part II.A looks at the privacy interests courts have and have not recognized as legitimate for standing purposes. Part II.B then explores some of the subtleties that can arise in courts' comparisons to analogous harms. Finally, Part II.C uses the Eighth Circuit's decisions in *Braitberg v. Charter Communications, Inc.*[153] and *Heglund v. Aitkin County*[154] to investigate the different ways courts may frame seemingly similar injuries to different results in the standing analysis.

A. What Privacy Interests Are Courts Protecting?

In *Spokeo*, the Supreme Court held that Robins could not prevail on the basis of a "bare procedural violation."[155] The Court went on to say that "not all inaccuracies cause harm or present any material risk of harm" and gave the example of an inaccurate zip code to illustrate a harmless privacy violation.[156] The Court concluded that "[i]t is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[157]

The Supreme Court stated that "both history and the judgment of Congress play important roles" and instructed lower courts to look to both of these

---

confusion" about the status of intangible harms. *Id.* at i, 14. The Supreme Court denied the petition on January 22, 2018. *Spokeo*, 2018 WL 3085282.

151. *See* William Baude, *Standing in the Shadow of Congress*, 2016 SUP. CT. REV. 197, 216; Lauren E. Willis, Spokeo *Misspeaks*, 50 LOY. L.A. L. REV. (forthcoming 2018) (manuscript at 103); Megan Dowty, Note, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 696 (2017).

152. One review of cases that cited to *Spokeo* in holding on standing found that the majority of the cases clumped around the FCRA, the TCPA, and the Fair Debt Collection Practices Act (FDCPA). Tyler Kasperek Somes, *Assessing* Spokeo, Inc. v. Robins: *The Future of Statutory Damage Class Actions in the Consumer Protection Arena*, 20 J. CONSUMER & COM. L. 122, 125 (2017).

153. 836 F.3d 925 (8th Cir. 2016).

154. 871 F.3d 572 (8th Cir. 2017).

155. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016).

156. *Id.*

157. *Id.* This "zip code" example has been cited repeatedly by lower courts in the course of denying standing. *See, e.g.*, *Braitberg*, 836 F.3d at 930; Hancock v. Urban Outfitters, Inc., 830 F.3d 511, 514 (D.C. Cir. 2016) (stating that "the Supreme Court advised . . . [that] disclosure of an incorrect zip code is not a concrete Article III injury"); Cruper-Weinmann v. Paris Baguette Am., Inc., 235 F. Supp. 3d 570, 574 (S.D.N.Y. 2017). One scholar contests the example's premise and argues that an inaccurate zip code can indeed be the source of substantial harms in a data-driven world. *See* Wu, *supra* note 16, at 459.

sources of guidance when faced with alleged intangible injuries.[158] Harkening back to the case-or-controversy requirement, the Court noted, "[I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[159] It continued, "Congress is well positioned to identify intangible harms that meet minimum Article III requirements" and so "its judgment is also instructive and important."[160]

Part II.A.1 lays out cases where the courts have denied standing and have held that the plaintiff failed to allege a sufficient injury. Part II.A.2 then presents cases where courts have found standing, at least in part, by analogizing the plaintiff's alleged injury to one that has been historically recognized by the courts, usually in the common law, and frequently to one of the privacy torts.

1. Requiring More Than a Statutory Violation

Lower courts have followed *Spokeo*'s instructions in cases in which they have found that the plaintiffs had not suffered any concrete harm, despite the alleged violation of a statute as to that individual plaintiff. In one such case, the Court of Appeals for the District of Columbia found that plaintiffs had not adequately established standing for alleged violations of Washington D.C.'s Use of Consumer Identification Information Act and its Consumer Protection Procedures Act.[161] The two plaintiffs had made purchases at local clothing stores and, while at the register, were each asked for their zip codes, a request that they alleged violated statutory protections against requiring address information to complete their transactions.[162] The court denied standing and noted that neither of the plaintiffs alleged any harm, such as invasion of privacy or emotional injury, beyond the "naked assertion that a zip code was requested and recorded."[163]

The Seventh Circuit reached a similar conclusion in *Meyers v. Nicolet Restaurant of De Pere, LLC*,[164] where the court heard allegations under the Fair and Accurate Credit Transactions Act (FACTA).[165] The plaintiff, Meyers, received a receipt after dining at the defendant-restaurant that did not have the credit card expiration date properly truncated as required by law.[166] The Seventh Circuit reviewed the claims in light of the Court's holding in *Spokeo*, stated that the inclusion of the full expiration led to no "appreciable risk of harm," and concluded that Meyers's alleged injuries were insufficient to confer standing.[167] The Seventh Circuit did not say that

158. *Spokeo*, 136 S. Ct. at 1549.
159. *Id.*
160. *Id.*
161. *Hancock*, 830 F.3d at 512.
162. *Id.*
163. *Id.* at 513–14.
164. 843 F.3d 724 (7th Cir. 2016).
165. *Id.* at 725.
166. *Id.*
167. *Id.* at 727.

such a violation of FACTA could never satisfy the injury-in-fact requirement but stated that the plaintiff's allegations were "completely divorced from any potential real-world harm."[168]

The Second Circuit similarly held that standing did not exist in a pair of FACTA cases, *Crupar-Weinmann v. Paris Baguette America, Inc.*[169] and *Katz v. Donna Karan Co.*[170] In *Paris Baguette*, the plaintiff brought suit after she received a receipt that displayed her credit card's full expiration date;[171] in *Katz*, decided three months after *Paris Baguette*, the plaintiff alleged that he received a receipt that improperly displayed the first six digits of his credit card number.[172] In *Paris Baguette*, the Second Circuit said that it was joining the Seventh Circuit's result in *Meyers* and held that printing "an expiration date on an otherwise properly redacted receipt" does not satisfy the injury-in-fact requirement.[173] In *Katz*, the court held that the court below had not erred in finding that the alleged FACTA violation did "not increase the risk of real harm" and so was not sufficient to establish standing.[174]

Outside the FACTA context, the Seventh and Eighth Circuits have arrived at similar results in two cases that implicated claims under the Cable Communications Policy Act (CCPA), which provides that a "cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access [by the subscriber] or pursuant to a court order."[175] In the Eighth Circuit case, plaintiff and class representative Braitberg alleged that defendant Charter Communications's failure to destroy customers' personally identifiable information after they had canceled their subscriptions was a "direct invasion of [customers'] federally protected privacy rights."[176] Plaintiffs contended that this violation of a statutory right alone was enough to qualify as an injury in fact, but the Eighth Circuit found that argument unconvincing and instead stated that *Spokeo* had "superseded" two earlier circuit decisions that seemed to support Braitberg's position.[177] The court denied standing on the ground that Braitberg had "identifie[d] no material risk of harm" from Charter Communications's retention of the data and further commented that the common law recognized no harm emerging from the company retaining information it had obtained lawfully.[178]

The Seventh Circuit borrowed from *Braitberg* and its own precedent in *Meyers* in denying standing for a putative class action that also alleged CCPA violations in *Gubala v. Time Warner Cable, Inc.*[179] Despite denying

168. *Id.* at 729.
169. 861 F.3d 76 (2d Cir. 2017).
170. 872 F.3d 114 (2d Cir. 2017).
171. *Paris Baguette*, 861 F.3d at 78.
172. *Katz*, 872 F.3d at 116.
173. *Paris Baguette*, 861 F.3d at 82.
174. *Katz*, 872 F.3d at 120.
175. 47 U.S.C. § 551(e) (2012).
176. Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 927 (8th Cir. 2016).
177. *Id.* at 929–30.
178. *Id.* at 930.
179. 846 F.3d 909 (7th Cir. 2017).

standing, the court, as in *Braitberg*, went out of its way to say that "[v]iolations of rights of privacy are actionable," even if the plaintiff in this particular case could go no further.[180] The plaintiff in *Gubala* had not alleged that Time Warner had "ever given away or leaked or lost any of his personal information or intends to give it away or is at risk of having the information stolen from it."[181] Nor did Gubala say that he "fear[ed] that Time Warner w[ould] give away the information and it w[ould] be used to harm him."[182] Presumably, if the plaintiff had asserted any or some combination of these privacy interests, the court might at least have been more willing to let him proceed. But, the court said, "he hasn't said *any* of that."[183]

2. Protection for Claims with Common Law Analogues

In cases where courts have been able to identify a privacy interest, or an intersection of privacy interests, that have historically been recognized by the courts, the courts have found sufficient injury for standing purposes.

a. Driver's Privacy Protection Act Cases

The Eighth Circuit's denial of an invasion of a privacy interest in *Braitberg* sufficient to confer standing can be contrasted with its holdings in *Shambour v. Carver County*[184] and *Heglund v. Aitkin County*,[185] cases decided nearly three weeks apart and in which standing was found for plaintiffs who alleged violations of the Driver's Privacy Protection Act (DPPA).[186] The DPPA "restricts the use and distribution of personal information contained in motor-vehicle records."[187]

In *Heglund*, the husband-and-wife-plaintiffs alleged that their information in Minnesota's driver's license database had been improperly accessed by police officers.[188] The couple requested an audit of access to their information because they feared harassment from Jennifer Heglund's ex-husband, who was a Minnesota state trooper.[189] The audit revealed that her information had been accessed 446 times over a ten-year period and that her current husband's records had been accessed thirty-four times between 2006 and 2013.[190] The defendants, challenging the plaintiffs' standing, argued that Jennifer Heglund's "professed anxiety from knowing that [an officer] improperly accessed her personal information is not sufficiently concrete to

180. *Id.* at 912.
181. *Id.* at 910.
182. *Id.* at 913.
183. *Id.*
184. No. 16-1425, 2017 WL 4231114 (8th Cir. Sept. 25, 2017).
185. 871 F.3d 572 (8th Cir. 2017).
186. *Shambour*, 2017 WL 4231114, at *3; *Heglund*, 871 F.3d at 577; *see also* 18 U.S.C. § 2721 (2012).
187. *Shambour*, 2017 WL 4231114, at *1.
188. *Heglund*, 871 F.3d at 575.
189. *Id.* at 575–76.
190. *Id.* at 576.

constitute an injury in fact."[191] The court disagreed. It explicitly distinguished *Braitberg* and found that "[a]n individual's control of information concerning her person—the privacy interest the Heglunds claim here—was a cognizable interest at common law."[192] The *Heglund* court explained this different outcome by drawing a line between the privacy interest it identified as legitimate here, and "the lack of comparable tradition of suits for retaining information lawfully obtained" that seemed to form the basis for the plaintiff's claim in *Braitberg*.[193]

In *Shambour*, the second of these two Eighth Circuit DPPA cases, the plaintiff alleged that her driver's records had been accessed fifty-nine times over an eight-year period.[194] A former law enforcement officer, Shambour alleged that "her appearance [had] 'changed noticeably' since her time as an officer" and "hypothesized that individuals viewed her record out of romantic attraction or curiosity about the changes in her appearance."[195] Finding that the plaintiff's claims could not be distinguished from those in *Heglund*, the court held that she had standing for her DPPA claims.[196]

b. Fair Credit Reporting Act Cases

Two cases examining standing for FCRA claims serve to further demonstrate the privacy interests courts have identified and explain that the invasion of these interests constitutes an injury under a *Spokeo* analysis.

The FCRA cases present two apparently dissimilar fact patterns—the first involves allegedly stolen laptops, and the second concerns *Spokeo* on remand from the Supreme Court. In *In re Horizon Healthcare Services Inc. Data Breach Litigation*,[197] the Third Circuit weighed standing for plaintiffs who alleged, after the theft of two laptops holding sensitive personal information, that defendant Horizon had provided inadequate protection for their personal information.[198] There, the court found that Congress had, through the FCRA, "create[d] a remedy for the unauthorized transfer of personal information."[199] The court stated that, "with privacy torts, improper dissemination of information" can rise to the level of a cognizable injury.[200] Although Horizon's actions would not in themselves necessarily generate a cause of action under common law,[201] the court noted that Congress had, in FCRA, "established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself."[202]

---

191. *Id.* at 577.
192. *Id.*
193. *Id.* at 578.
194. *Shambour*, 2017 WL 4231114, at *1.
195. *Id.*
196. *Id.* at *2.
197. 846 F.3d 625 (3d Cir. 2017).
198. *Id.* at 629.
199. *Id.*
200. *Id.* at 638–39.
201. "No common law tort proscribes the release of truthful information that is not harmful to one's reputation or otherwise offensive." *Id.* at 639.
202. *Id.*

Analyzing Robins's claims on remand (and citing *In re Horizon*), the Ninth Circuit similarly emphasized that the pairing between a harm defined by Congress in statute and one long recognized in the courts does not have to be an exact match.[203] "Even if there are differences between FCRA's cause of action and those recognized at common law, the relevant point is that Congress has chosen to protect against a harm that is at least closely similar *in kind* to others that have traditionally served as the basis for lawsuit."[204] In Robins's case, the Ninth Circuit said that "[c]ourts have long entertained causes of action to vindicate intangible harms caused by certain untruthful disclosures about individuals"[205] and that in FCRA Congress had applied that principle to a perceived risk of harm[206] that could arise in the context of credit reporting.[207]

c. Video Privacy Protection Act Cases

Finally, the Third and Eleventh Circuits have discerned a close relationship between traditional causes of action and VPPA claims in *In re Nickelodeon Consumer Privacy Litigation*[208] and *Perry v. Cable News Network, Inc.*[209] The Third Circuit in *In re Nickelodeon*—a consolidated class action that alleged that Google and Viacom unlawfully collected data from the plaintiffs, children under age thirteen, including the videos they watched and websites they visited[210]—held that *Spokeo* did nothing to deny the plaintiffs standing and that the alleged harm included a "*de facto* injury, *i.e.*, the unlawful disclosure of legally protected information."[211] The court did not pair the alleged harm with a specific common law analogue but instead seemingly blended the congressional and historical inquiries. It stated, "Congress has long provided plaintiffs with the right to seek redress for unauthorized disclosures of information that, in Congress's judgment, ought to remain private."[212]

The Eleventh Circuit took greater pains to point out the nearness of the VPPA claims alleged to a common law harm in *Perry*.[213] The plaintiff in this case brought suit under the VPPA alleging that, after he downloaded the CNN app to his phone in 2013, the app collected information on his viewing activity without his knowledge and unlawfully disclosed his personally identifiable information.[214] The Eleventh Circuit analogized to the elements

203. Robins v. Spokeo, Inc., 867 F.3d 1108, 1115 (9th Cir. 2017).
204. *Id.*
205. *Id.*
206. For example, in introducing the FCRA, lawmakers recounted the story of a man who was never able to obtain credit even after he had been exonerated of a crime. 115 CONG. REC. 2411–12 (1969).
207. *Robins*, 867 F.3d at 1115.
208. 827 F.3d 262 (3d Cir. 2016).
209. 854 F.3d 1336 (11th Cir. 2017).
210. *In re Nickelodeon*, 827 F.3d at 267.
211. *Id.* at 274.
212. *Id.*
213. *Perry*, 854 F.3d at 1340–41.
214. *Id.* at 1338–39.

of the tort of intrusion upon seclusion and further noted that "Supreme Court precedent has recognized in the privacy context that an individual has an interest in preventing *disclosure* of personal information."[215] The court held that Perry had "satisfied the concreteness requirement of Article III standing, [by] alleg[ing] a violation of the VPPA for a wrongful disclosure."[216]

B. The Problems with Common Law Analogues

Because of the Supreme Court's instruction in *Spokeo* that lower courts should consider both the "judgment of Congress" and any "close relationship" to a harm historically recognized in the law,[217] courts have scrutinized how closely an alleged harm resembles one recognized at common law or otherwise in the English and American legal traditions. One potential problem with this closeness analysis is that it leaves to individual judges the framing of the alleged harm and the question of whether it has the "feel"[218] of a traditionally recognized harm. And so, in the cases since *Spokeo*, courts can be seen engaging in this closeness inquiry with varying degrees of precision, sometimes naming specific privacy torts, other common law causes of action like libel,[219] or "a right of individual privacy."[220] These courts are not interpreting *Spokeo* to require them to draw a precise line from

215. *Id.* at 1341.

216. *Id.*

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

218. Coleman v. Miller, 307 U.S. 433, 460 (1939) (Frankfurter, J., concurring) ("Judicial power could come into play only in matters that . . . arose in ways that to the expert feel of lawyers constituted 'Cases' or 'Controversies.'").

219. Hatch v. Demayo, No. 1:16CV925, 2017 WL 4357447, at *4 (M.D.N.C. Sept. 29, 2017) ("Specifically, Plaintiffs' allegation bears a close relationship to the interest protected by the invasion of privacy torts, namely, leading a secluded and private life."); Garey v. Farrin, No. 1:16CV542, 2017 WL 4357445, at *5 (M.D.N.C. Sept. 29, 2017) ("Plaintiffs' alleged harms are closely related to the invasion of privacy, which has long provided a basis for recovery at common law."); Phillips v. Trans Union, LLC, No. 3:16-CV-00088, 2017 WL 3911018, at *1 (W.D. Va. Sept. 6, 2017) (stating that the plaintiff's "alleged injury is analogous to common law causes of action (like defamation and libel)"); *In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1216 (C.D. Cal. 2017) ("Plaintiffs' VPPA claims are even more deeply rooted in the common law."); Gambles v. Sterling Infosystems, Inc., 234 F. Supp. 3d 510, 523 (S.D.N.Y. 2017) ("These echo the sorts of allegations on which tort claims were permitted to proceed at common law . . . ."); Whitaker v. Appriss, Inc., 229 F. Supp. 3d 809, 812 (N.D. Ind. 2017) ("Rights protected in statutes like the [Drivers Privacy Protection Act] are natural outgrowths of the privacy-based torts of the common law."); Matera v. Google Inc., No. 15-CV-04062-LHK, 2016 WL 5339806, at *10 (N.D. Cal. Sept. 23, 2016) ("[V]iolations of the Wiretap Act and [Children's Internet Protection Act] are similar to common law invasion of privacy in both their substantive prohibitions and their purpose."); Witt v. Corelogic Saferent, LLC, No. 3:15-cv-386, 2016 WL 4424955, at *12 (E.D. Va. Aug. 18, 2016) ("The common law has long recognized a right to personal privacy . . . ."); Mey v. Got Warranty, Inc., 193 F. Supp. 3d 641, 645 (N.D. W. Va. 2016) ("The invasion of privacy claim that is most analogous here is intrusion upon seclusion."); Thomas v. FTS USA, LLC, 193 F. Supp. 3d 623, 636 (E.D. Va. 2016) ("[I]t has long been the case that an unauthorized dissemination of one's personal information . . . constitutes a concrete injury . . . .").

220. Ruk v. Crown Asset Mgmt., LLC, No. 1:16-CV-3444-LMM-JSA, 2017 WL 3085282, at *5 (N.D. Ga. Mar. 22, 2017) ("[O]ur common law traditionally recognizes a right of individual privacy, which is legally protected by the courts in certain circumstances.").

a privacy harm Congress has identified to one that has a long history in the courts. One district court has stated that defendants seeking to challenge plaintiffs' standing should not misinterpret *Spokeo* as requiring that the privacy interest protected by statute be precisely the same as one protected by a common law privacy harm for if that was necessary, there would be little use for the statute.[221]

C. Can Braitberg *and* Heglund *Be Reconciled?*

A comparison of *Braitberg* and *Heglund* sheds light on some of the concerns courts bring to bear when applying *Spokeo* to an alleged privacy injury. Perhaps most significantly, these two cases—in which different statutes were at issue—also demonstrate how the way in which the parties and court frame the potential common law analogue can influence the outcome of the standing analysis.

Both the DPPA and the CCPA contain provisions aimed at ensuring that the information in question is used only for the purpose for which it was collected, absent consent for a new use.[222] In *Braitberg*, the CCPA imposed what the plaintiff alleged was "a duty to destroy personally identifiable information" and, the plaintiff alleged, the defendant violated this duty "by retaining certain information longer than the company should have kept it."[223] The alleged injury in *Heglund* was that the repeated improper access of the plaintiffs' records had "invad[ed] Jennifer's privacy."[224] In both cases, the plaintiffs took action before filing suit to ascertain whether there had been some allegedly unlawful treatment of their information—that it had been improperly retained or wrongfully accessed.[225]

But the circuit's opinions diverged when they sought a common law analogue. The *Braitberg* court determined that "retention of information lawfully obtained . . . without further disclosure" has not traditionally been recognized in American courts, while the *Heglund* court stated that "[a]n individual's control of information concerning her person . . . was a cognizable interest at common law."[226]

There are other concerns that have traditionally formed important subcurrents in privacy discourse that, if not explicitly relied upon in the *Heglund* court's rationale, nevertheless merit mention in the opinion, including that the alleged wrongful access implicated law enforcement personnel and that the plaintiff "professed anxiety" about the suspected access.[227] While the court does not say that these facts in the case led to its identification of a privacy harm and concrete injury, both the sense of an

221. *Whitaker*, 229 F. Supp. 3d at 813.
222. Solove, *supra* note 62, at 520–21.
223. Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 930 (8th Cir. 2016).
224. Heglund v. Aitkin County, 871 F.3d 572, 578 (8th Cir. 2017).
225. *Heglund*, 871 F.3d at 576; *Braitberg*, 836 F.3d at 927.
226. *Heglund*, 871 F.3d at 577; *Braitberg*, 836 F.3d at 930.
227. *Heglund*, 871 F.3d at 576–77.

emotional harm[228] and the potential abuse of government authority to violate a protected privacy interest[229] have historically been important perimeter markers for privacy harms.

III. TIME TO RETHINK THE NATURE OF PRIVACY INJURIES

This Part suggests that *Spokeo*'s instruction that courts should look to whether an alleged intangible injury bears close comparison to a traditionally recognized harm has opened an unanticipated opportunity to reinvigorate discussion in the federal judiciary about the nature of privacy harms.[230] The efficacy of agency and administrative enforcement of privacy statutes has been questioned,[231] and the courts, adjudicating suits brought by private individuals, may prove to be an important force in regulating privacy infringements caused by information technology.[232] If courts do not embrace this role and instead do more to limit private causes of action in federal privacy statutes through the vehicle of standing, they will further defang the few protections individuals have in the data economy.[233] As matters now stand, companies with vast stores of data often face little in the way of substantive repercussions when those data are breached.[234] Without the potential for private enforcement, privacy statutes run the risk of becoming congressional dead letters, "mere suggestions."[235] This Part proposes one way courts can prevent that outcome, while staying safely within the framework of *Spokeo*.

Part III.A argues—drawing from a substantial body of scholarship developed by Daniel Solove, Ryan Calo, Danielle Citron, Neil Richards, and others—that Prosser's four privacy torts are, on their own, inadequate to

228. Warren & Brandeis, *supra* note 54, at 213; *see also* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1145 (2011).

229. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

230. This Note takes no position on whether a plaintiff should have to show more than a statutory violation; that is, it does not seek to answer the question of "statutory standing." This Note rather proceeds on the observable fact that lower courts are searching for analogues for alleged privacy injuries and offers suggestions for courts pursuing that inquiry.

231. Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 26–31 (2008); Austin H. Krist, Note, *Large-Scale Enforcement of the Fair Credit Reporting Act and the Role of State Attorneys General*, 115 COLUM. L. REV. 2311, 2324 (2015).

232. *See, e.g.*, Lawrence Hurley, *U.S. Supreme Court to Settle Major Cellphone Privacy Case*, REUTERS (June 5, 2017, 9:48 AM), https://www.reuters.com/article/us-usa-court-mobilephone/u-s-supreme-court-to-settle-major-cellphone-privacy-case-idUSKBN18W1RY [https://perma.cc/T88D-UFAG]; Jill Priluck, *How Courts Avoid Ruling on Issues of Privacy*, SLATE (Apr. 11, 2017, 5:38 PM), http://www.slate.com/articles/technology/future_tense/2017/04/how_courts_avoid_ruling_on_issues_of_technology_and_privacy.html [https://perma.cc/R5BF-EYYD].

233. One scholar has already observed that "the trend in federal privacy statutes has been to undercut the interests of individuals in protecting privacy rights." De Armond, *supra* note 231, at 45.

234. *See* Robert Hackett, *How Much Do Data Breaches Cost Big Companies?: Shockingly Little*, FORTUNE (Mar. 27, 2015), http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/ [https://perma.cc/4TMR-S437].

235. De Armond, *supra* note 231, at 35.

provide legal redress for harms generated by the data economy. Part III.B then encourages courts to employ a nexus approach to assess the concreteness of privacy harms, an approach that satisfies *Spokeo* while at the same time unchaining courts from the overworked privacy torts. Finally, Part III.C emphasizes the extent to which privacy harms arising from new technology have been topics of considerable concern both to the public and the Supreme Court in recent years.

A. Privacy Torts Are Ill Matched to New Harms

Scholars have remarked that the privacy torts that sprang from Warren and Brandeis's collaboration, and that were systematized by Prosser, are poorly suited to the challenges presented by changing forms of technology.[236] One scholar has noted how the torts are often defined partly by reference to protected spaces[237]—for example, intrusion upon seclusion—but this approach runs up against its limits where technology has blurred traditional legal boundaries. Professor Citron has urged courts to "take cues from privacy tort law's intellectual history to ensure its continued vitality."[238] She urges courts to do this by revisiting the emphasis Warren and Brandeis put on the right of privacy as protecting an individual's "inviolate personality."[239] Professor Sarah Ludington has proposed a novel tort for the misuse of personal information that takes guidance from both the existing privacy torts and privacy legislation.[240] The judicial reluctance to continue the development of the privacy torts over the past century[241] has only served to exacerbate the need for new consideration of what privacy harms the law should recognize.

Part III.A.1 argues that, while the privacy torts may be useful to courts looking to identify sufficiently concrete privacy injuries for standing purposes, *Spokeo* does not limit their search to the four privacy torts. Part III.A.2 lays out some more recent conceptualizations of privacy injury proposed by scholars.

1. *Spokeo* Does Not Bind Courts to Privacy Torts

The Supreme Court's instruction in *Spokeo* to consider whether an alleged intangible harm bears a relation to one traditionally recognized by the courts does not require the courts to hew so closely to the four traditional privacy

236. Samantha Barbas, *Saving Privacy from History*, 61 DEPAUL L. REV. 973, 973 (2012) (noting that "tort privacy is especially inadequate to address the needs of the twenty-first century"); Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 145 (2006); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 155 (2007).

237. Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 17–18 (2007).

238. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1852 (2010).

239. *Id.*

240. Ludington, *supra* note 236, at 146.

241. *See supra* Part I.C.

torts when considering the concreteness of an injury asserted under a statute implicating a privacy interest. In other words, that the plaintiff asserts a harm to a privacy interest does not mean the harm must itself bear a close relationship to a traditional privacy tort. Both the Ninth and Third Circuits have emphasized that *Spokeo* does not require an exact match.[242] One district court, in a decision cited by several others,[243] has further emphasized that *Spokeo*'s concreteness analysis does not require that the harm with which a closeness is identified be "of any particular jurisdiction" and further stated that the analogous harm does not need to be one that, if alleged independently, would give rise to a viable tort claim.[244]

This degree of discretion courts can employ in searching out analogues for alleged privacy harms seems particularly appropriate, as determinations concerning what interests deserve privacy protection are always normative and culturally conditioned.[245] Privacy is contextual.[246] Courts should look beyond the privacy torts to other privacy-related interests historically protected by the courts to allow plaintiffs to pass the standing bar drawn by *Spokeo*, both out of deference to separation-of-powers principles—which undergird standing as a doctrine[247]—and to give vitality to privacy claims.

This would serve separation-of-powers principles because it would help the courts give meaningful effect to the statutes Congress has enacted. The decision by Congress to include a private right of action when a privacy concern is at stake represents a purposeful and reasoned decision by the legislature. Neither the Gramm-Leach-Bliley Act (GLBA) nor the Health Insurance Portability and Accountability Act (HIPAA), both of which implicate privacy concerns, contains an explicit private right of action.[248] Courts, including the Supreme Court, reviewing the legislative histories of statutes such as the FCRA,[249] the VPPA,[250] the TCPA,[251] and the DPPA[252] have found that Congress, as the nation's deliberative and legislative body, was responding to specific privacy concerns and intended to regulate certain privacy-infringing behavior.

Furthermore, undue adherence to Prosser's privacy torts leads to an incomplete picture of the range of privacy harms that have historically been

242. Robins v. Spokeo, Inc., 867 F.3d 1108, 1115 (9th Cir. 2017); Susinno v. Work Out World, Inc., 862 F.3d 346, 351 (3d Cir. 2017).

243. *See* Engebretson v. Aitkin County, No. 14-1435 ADM/FLN, 2016 WL 5400363, at *4 (D. Minn. Sept. 26, 2016); Krekelberg v. Anoka County, No. 13-3562 (DWF/TNL), 2016 WL 4443156, at *3 (D. Minn. Aug. 19, 2016).

244. Potocnik v. Carlson, No. 13-CV-2093 (PJS/HB), 2016 WL 3919950, at *3 (D. Minn. July 15, 2016).

245. Solove, *supra* note 62, at 484.

246. *See* Abril, *supra* note 237, at 2.

247. *See supra* Part I.A.

248. Menton v. Experian Corp., No. 02 Civ. 4687(NRB), 2003 WL 21692820, at *3 (S.D.N.Y. July 21, 2003); Joshua D.W. Collins, Note, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 201 (2007).

249. *See* Safeco Ins. Co. of Am. v. Burr, 551 U.S. 47, 52 (2007).

250. *See* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1252–53 (11th Cir. 2015).

251. *See* L.A. Lakers, Inc. v. Fed. Ins. Co., 869 F.3d 795, 799 (9th Cir. 2017).

252. *See* Reno v. Condon, 528 U.S. 141, 143–44 (2000).

recognized by the law. Eavesdropping was a crime at common law.[253] Fourth Amendment jurisprudence and "the constitutional right to information privacy [and] evidentiary privileges"[254] all fall under the umbrella of privacy law. The protection of privacy afforded by anonymous speech has long been an important part of American public life and has been described by the Court as "a shield from the tyranny of the majority."[255] Holding the courts to the four privacy torts in their search for analogues misrepresents the privacy concerns sown broadly across the landscape of American law.

2. Novel Conceptions of Privacy Injury Have Been Proposed

While courts have been slow since Prosser to delineate new privacy wrongs, scholars have engaged in robust discussion of what constitutes an injury to privacy and what forms of privacy harm should be legally cognizable. Instead of being amorphous and merely motivated by an "ick" factor, one professor has described privacy harms as "unique injur[ies] with specific boundaries and characteristics."[256] Professor Citron has argued that courts can look to the seventy years preceding Prosser's work as a way to revitalize their privacy inquiries.[257] Richards has argued for rights of "intellectual privacy" that are founded on the First Amendment and that protect "our reading, our communications, and our expressive dealings with others."[258] Another commentator has suggested, drawing on fiduciary law, that courts could impose a duty to secure the information they obtain on "data confidants."[259] Writing together, Solove and Citron have noted that, in the context of harms resulting from data breaches, courts are presented with opportunities to read precedents "flexibly and creatively"—but seldom seize that chance.[260]

The intellectual groundwork laid by these scholars stands ready to assist courts prepared to investigate more deeply new forms of privacy harm that arise from the widespread collection and retention of data.

B. A Nexus of Privacy Interests Is Sufficient

Few of the plaintiffs in the cases discussed in this Note appear to have asserted anything so broad as the "right to be let alone"[261] that famously motivated the Warren-Brandeis conception of privacy and that spurred the development of privacy law in America.[262] Rather, plaintiffs suing under

253. Solove, *supra* note 62, at 492.
254. *Id.* at 478.
255. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); *see also* Joel R. Reidenberg, *The Transparent Citizen*, 47 LOY. U. CHI. L.J. 437, 439 (2015).
256. Calo, *supra* note 228, at 1131.
257. Citron, *supra* note 238, at 1832–34.
258. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 408 (2008).
259. Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 628 (2018).
260. Solove & Citron, *supra* note 103, at 786.
261. Warren & Brandeis, *supra* note 54, at 193.
262. Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 623–25 (2002).

privacy statutes seem to act on the basis of a more narrow principle: that when society, through Congress, has circumscribed certain interactions as subject to privacy protections, individuals should be able to sue for redress when they personally suffer infringements of those interests. This Part proposes a way that federal courts, working within the framework laid out by *Spokeo*, can conceptualize those alleged injuries in the context of standing.

In order to grant plaintiffs the benefit of the few existing privacy protections in statute, courts employing *Spokeo*'s standing analysis for the concreteness of intangible harms should apply a nexus approach that looks beyond the privacy torts in assessing whether plaintiffs have adequately established injury in fact. They should look for significant overlapping privacy concerns that have historically been recognized by the courts. Instead of seeking a perfect tort analogue to an alleged privacy injury and dismissing for lack of standing if no perfect analogue exists, lower courts should find that such a nexus of implicated privacy interests is sufficient to give concreteness to the alleged injury.

The cases in Part II illustrate how, to some extent, this is already what courts are doing when they find privacy harms.[263] But because of the potential for confusion and uncertainty that surrounds privacy, the insufficiency of the privacy torts, and the potential for privacy-adverse judges to frame a privacy interest so as to not recognize a common law analogue,[264] the courts should shift to an approach that finds that a nexus of privacy interests is sufficient. Such a nexus may be formed by the intersection of the varied privacy-related interests long recognized by the law, including the involvement of law enforcement in the alleged injury, emotional distress, or other conjunctions of privacy-implicated concerns that in and of themselves would not give rise to a cause of action.

This approach would help courts recognize privacy harms as Warren and Brandeis, and the opinions they drew on, found such harms—unnamed but nevertheless present.[265] An approach that recognizes a nexus of privacy concerns as sufficient to establish concreteness for purposes of injury in fact would also go further toward respecting the separation-of-powers principles that serve as the constitutional underpinnings for the standing doctrine.[266] To restrict Congress to the identification only of harms that look like older harms would be an improper judicial interference with the legislative power vested in Article I of the Constitution, quite apart from the practical difficulties sure to result from strictly restraining federal courts to the harms that would have been familiar to their judicial ancestors in "the courts at Westminster."[267]

This nexus approach, which finds a new privacy interest where several traditional privacy concerns overlap, especially when the area within that nexus has been elevated by a statute, best respects the interests both of

263. *Supra* Part II.
264. *Supra* Part I.C.
265. *See* RESTATEMENT (SECOND) OF TORTS § 652A cmt. (a) (AM. LAW INST. 1977); *see also supra* Part I.B.1.
266. *Supra* note 46 and accompanying text.
267. Coleman v. Miller, 307 U.S. 433, 460 (1939) (Frankfurter, J., concurring).

privacy law and of the constitutional, separation-of-powers justifications for standing. It allows courts to identify injuries similar to those with which their competency is long settled, while simultaneously not hampering Congress's power to respond to new forms of harm.

C. Supreme Court and Public Are Both Concerned with Privacy

Privacy harms are a growing area of legal concern that courts should not ignore. As the Ninth Circuit recently observed, "[t]he modern information age has shined a spotlight on information privacy."[268] Outside of the legal arena, Pierre Omidyar, a prominent technology billionaire who founded eBay, wrote in the *Washington Post* that he fears that, "[f]or all the ways this technology brings us together, the monetization and manipulation of information is swiftly tearing us apart."[269] The United States saw 1091 data breaches in 2016, a 40 percent increase over the previous year.[270]

The Supreme Court has recognized the manner in which changes in technology can result in new forms of harm to privacy interests.[271] In 2011, in the course of striking down a Vermont law that restricted the sale of prescriber data to pharmaceutical marketers, the Court in *Sorrell v. IMS Health Inc.*[272] said that the "capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure."[273] Little has been done since to address that threat to privacy.

CONCLUSION

The Supreme Court's holding in *Spokeo* added new difficulty to the already considerable challenges privacy plaintiffs face. As businesses built on the commodification of personal information expand, the privacy torts, long starved for judicial attention, have proven ill equipped to the regulation of this widespread economic activity, with its attendant potential for harms. Should the federal courts, through the vehicle of standing, remove themselves from the adjudication of novel privacy harms, even when redress for such harms has been provided for by Congress, there will be little incentive for companies to avoid such harms, and private individuals will be left without a remedy.

The approach proposed by this Note accords with the Court's instructions in *Spokeo* for testing the concreteness of intangible harms and would allow

---

268. Syed v. M-I, LLC, 853 F.3d 492, 495 (9th Cir. 2017).

269. Pierre Omidyar, Opinion, *Pierre Omidyar: 6 Ways Social Media Has Become a Direct Threat to Democracy*, WASH. POST (Oct. 9, 2017), https://www.washingtonpost.com/news/theworldpost/wp/2017/10/09/pierre-omidyar-6-ways-social-media-has-become-a-direct-threat-to-democracy/?utm_term=.7252f92a6207 [https://perma.cc/7U6R-BKT6].

270. *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CTR. (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html [https://perma.cc/CS2Y-ZPGT].

271. *Supra* Part I.B.1.

272. 131 S. Ct. 2653 (2011).

273. *Id.* at 2672.

plaintiffs to pursue the remedies Congress has afforded them in privacy statutes. This approach properly respects the separation-of-powers rationale that the Supreme Court has said rests at the core of standing, and it helps ensure that courts retain their important role as protectors of private individuals' rights in a shifting economic landscape by giving force and meaning to the privacy protections Congress has enacted.