The Hunt for Privacy Harms After Spokeo

Matthew S. DeLuca
Fordham University School of Law

Follow this and additional works at: https://ir.lawnet.fordham.edu/flr

Recommended Citation
Available at: https://ir.lawnet.fordham.edu/flr/vol86/iss5/4

This Note is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.
The Hunt for Privacy Harms After Spokeo

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

This note is available in Fordham Law Review: https://ir.lawnet.fordham.edu/flr/vol86/iss5/4
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.

INTRODUCTION.................................................................2440

I. PRIVACY AND STANDING: BRANDEISIAN BRAIN CHILDREN
   COLLIDE .................................................................2442
      A. What Is Standing? .................................2443
         1. Development of the Doctrine ......2443
         2. Injury in Fact .................................2445

* 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.
B. The Evolving Nature of Privacy Harms ........................................ 2446
   1. The Path of American Privacy Law ........................................ 2446
   2. The Growth of the Data Economy ........................................ 2449
   3. A “Kilimanjaro” for Privacy Plaintiffs? .............................. 2451
C. Judicial Skepticism of Privacy Harms ..................................... 2452
D. Spokeo and Its Holding ......................................................... 2454
   1. The Supreme Court’s Decision ............................................ 2455
   2. Disagreement over What Was at Stake in Spokeo .................. 2455
   3. Did Spokeo Change Anything? ........................................... 2456
II. COURTS SEARCH FOR PRIVACY HARMS AFTER SPOKEO .......... 2457
A. What Privacy Interests Are Courts Protecting? ......................... 2457
   1. Requiring More Than a Statutory Violation ......................... 2458
   2. Protection for Claims with Common Law Analogues ............... 2460
B. The Problems with Common Law Analogues .............................. 2463
C. Can Braithberg and Heglund Be Reconciled? ............................ 2464
III. TIME TO RETHINK THE NATURE OF PRIVACY INJURIES ............. 2465
A. Privacy Torts Are Ill Matched to New Harms ............................ 2466
   1. Spokeo Does Not Bind Courts to Privacy Torts .................... 2466
   2. Novel Conceptions of Privacy Injury Have Been Proposed ........ 2468
B. A Nexus of Privacy Interests Is Sufficient ............................... 2468
C. Supreme Court and Public Are Both Concerned with Privacy ...... 2470
CONCLUSION .................................................................................... 2470

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

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 \textit{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 \textit{Spokeo}.

---


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

\(^8\) \textit{Id.} at 1548–49.


\(^10\) Fifty-five percent of respondents to one survey said they decided not to make a purchase online because they were concerned about privacy. \textit{Companies That Fail to See Privacy as a Business Priority Risk Crossing the ‘Creepy Line’}, KPMG (Nov. 6, 2016), \url{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-SQIN]; see also \textit{Lee Rainie & Shiva Maniam, Americans Feel the Tensions Between Privacy and Security Concerns}, PWE RES. CTR. (Feb. 19, 2016), \url{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”\(^\text{11}\) 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”\(^\text{12}\)—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\(^\text{13}\)—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.\(^\text{14}\) 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\(^\text{15}\)—appear to have come into conflict.\(^\text{16}\) 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.\(^\text{17}\) 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.


\(^{14}\) See infra Part I.B.1.


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: (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. These three elements constitute an “irreducible constitutional minimum,” a “core component of standing.” 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. 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.

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. 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.” 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. 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.

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. 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.” The doctrine is justified as


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


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”).
31. 258 U.S. 126 (1922).
32. Id. at 127.
33. Id. at 129.
**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.* The petitioners in that case were in the business of selling data-processing services. 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.”

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.*

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. 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).
36. *Frothingham,* 262 U.S. at 479.
37. Id. at 486.
38. Id.
39. Id. at 488.
40. Id.
42. *Data Processing,* 397 U.S. at 151.
43. Id. at 152.
44. Fletcher, *supra* note 19, at 230.
Lujan v. Defenders of Wildlife46 tightened the requirements47 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 article54 that

“[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”).
58. Id. at 474 (Brandeis, J., dissenting).
60. RESTATEMENT (SECOND) OF TORTS §§ 652A–E (AM. LAW INST. 1977); Prosser, supra note 59, at 389.
it protects individual interests against government power, and so the Court has spoken out more forcefully for individual privacy in the context of Fourth Amendment rights. 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 and the right to be free from “unreasonable governmental prying.” 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.”

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. 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. 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 and allowing increased economic uses of information. 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. 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.

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.


78. Walker, supra note 75, at 88.


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. The expansion of credit-reporting agencies in the late nineteenth century struck some contemporary observers as an extremely worrisome form of public snooping. 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. Household-name companies like Google and Facebook, as well as smaller enterprises, hold vast troves of data, which power an economy premised on the collection of personal information. With those stores of data comes a risk of disclosure, whether as the result of a hack or other form of breach, as well as the possibility that a company or other entity may make use of the collected data in an unlawful manner.

Whether individuals use smartphone applications, go out to eat at popular restaurants, or wear certain activity-tracking devices, private persons, if they want to avail themselves of the promises of new technologies, often have little choice 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 or searches they conduct over the internet—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. 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. Today, individuals effectively pay for some of the world’s most popular online services by handing over information about themselves. The collection of data has gone beyond the accumulation of

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.”).
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. 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.

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

3. A “Kilimanjaro” for Privacy Plaintiffs?

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

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. But the necessity of a “concrete, living...
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

---

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.
107. Kaminski, supra note 6, at 416.
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).
acc cretive 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. Wood115 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.


117. Sprague, supra note 112, at 102.


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.
But Prosser alone cannot bear the blame for the judiciary’s skeptical approach to privacy concerns. 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.

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. Some privacy concerns have also long been seen as conflicting with First Amendment values. 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.

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.” 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.” This conceptualization supported, rather than undermined, First Amendment values by “protect[ing] individuals’ emotional and intellectual processes so that they can think for themselves.”

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.
123. Richards & Solove, supra note 119, at 1917.
125. See supra note 75 and accompanying text.
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. The much-anticipated case arose from claims brought by the plaintiff, Robins, under the FCRA. *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. Robins alleged that *Spokeo* maintained a report on him that contained numerous inaccuracies and that *Spokeo* thereby was in violation of FCRA.

Robins brought claims under the FCRA provisions that provide that consumer reporting agencies “follow reasonable procedures to assure maximum possible accuracy” of consumer reports and that

> any 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.

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.” 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.

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, 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.

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.

---

133. *Id.* at 1546.
134. *Id.*
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.”).
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.” 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.” In another brief, amici media companies argued that a strict injury-in-fact line would help ward off abusive class action suits.

3. Did Spokeo Change Anything?

One legal observer described the Court’s narrow holding in Spokeo as “somewhat of a disappointment.” At least some courts have not been convinced that Spokeo represents a substantial shift in the Supreme Court’s standing jurisprudence. 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. 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. Another district court summed up Spokeo as “offer[ing] useful guidance.” 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.

143. Id. at 6.
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. 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.

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.* and *Heglund v. Aitkin County* 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.” 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. 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.”

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 origins to understand the status of intangible harms. The Supreme Court denied the petition on January 22, 2018. See *Spokeo*, 2018 WL 3085282.


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

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


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.\textsuperscript{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.”\textsuperscript{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.”\textsuperscript{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 \textit{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.\textsuperscript{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.\textsuperscript{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.”\textsuperscript{163}

The Seventh Circuit reached a similar conclusion in \textit{Meyers v. Nicolet Restaurant of De Pere, LLC},\textsuperscript{164} where the court heard allegations under the Fair and Accurate Credit Transactions Act (FACTA).\textsuperscript{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.\textsuperscript{166} The Seventh Circuit reviewed the claims in light of the Court’s holding in \textit{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.\textsuperscript{167} The Seventh Circuit did not say that

\textsuperscript{158} \textit{Spokeo}, 136 S. Ct. at 1549.
\textsuperscript{159} \textit{Id}.
\textsuperscript{160} \textit{Id}.
\textsuperscript{161} 830 F.3d at 512.
\textsuperscript{162} \textit{Id}.
\textsuperscript{163} \textit{Id}.
\textsuperscript{164} 843 F.3d 724 (7th Cir. 2016).
\textsuperscript{165} \textit{Id}.
\textsuperscript{166} \textit{Id}.
\textsuperscript{167} \textit{Id}.
\textsuperscript{167} \textit{Id}.
\textsuperscript{167} \textit{Id}.
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.”

The Second Circuit similarly held that standing did not exist in a pair of FACTA cases, *Crupar-Weinmann v. Paris Baguette America, Inc.* and *Katz v. Donna Karan Co.* In *Paris Baguette*, the plaintiff brought suit after she received a receipt that displayed her credit card’s full expiration date; 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. 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. 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.

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.” 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.” 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. 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.

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.* 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.
173. *Paris Baguette*, 861 F.3d at 82.
174. *Katz*, 872 F.3d at 120.
177. *Id.* at 929–30.
178. *Id.* at 930.
179. 846 F.3d 909 (7th Cir. 2017).
standing, the court, as in Breitberg, went out of its way to say that “violation[s] of rights of privacy are actionable,” even if the plaintiff in this particular case could go no further.\textsuperscript{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.”\textsuperscript{181} Nor did Gubala say that he “fear[ed] that Time Warner would give away the information and it would be used to harm him.”\textsuperscript{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.”\textsuperscript{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.

\textit{a. Driver’s Privacy Protection Act Cases}

The Eighth Circuit’s denial of an invasion of a privacy interest in Breitberg sufficient to confer standing can be contrasted with its holdings in \textit{Shambour v. Carver County}\textsuperscript{184} and \textit{Heglund v. Aitkin County}\textsuperscript{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).\textsuperscript{186} The DPPA “restricts the use and distribution of personal information contained in motor-vehicle records.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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

\begin{footnotesize}
\begin{enumerate}
\item[\textsuperscript{180}] Id. at 912.
\item[\textsuperscript{181}] Id. at 910.
\item[\textsuperscript{182}] Id. at 913.
\item[\textsuperscript{183}] Id.
\item[\textsuperscript{184}] No. 16-1425, 2017 WL 4231114 (8th Cir. Sept. 25, 2017).
\item[\textsuperscript{185}] 871 F.3d 572 (8th Cir. 2017).
\item[\textsuperscript{186}] Shambour, 2017 WL 4231114, at *3; Heglund, 871 F.3d at 577; see also 18 U.S.C. § 2721 (2012).
\item[\textsuperscript{187}] Shambour, 2017 WL 4231114, at *1.
\item[\textsuperscript{188}] Heglund, 871 F.3d at 575.
\item[\textsuperscript{189}] Id. at 575–76.
\item[\textsuperscript{190}] Id. at 576.
\end{enumerate}
\end{footnotesize}
constitute an injury in fact.” 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.” 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.” 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.
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 proscribe[s] 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 harm206 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 Litigation208 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 visited210—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

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.”

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.”

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, 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” 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, or “a right of individual privacy.” These courts are not interpreting Spokeo to require them to draw a precise line from

215. Id. at 1341.

216. Id.


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.’”).


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

III. TIME TO RETHINK THE NATURE OF PRIVACY INJURIES

This Part suggests that \textit{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.\textsuperscript{230} The efficacy of agency and administrative enforcement of privacy statutes has been questioned,\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{234} Without the potential for private enforcement, privacy statutes run the risk of becoming congressional dead letters, “mere suggestions.”\textsuperscript{235} This Part proposes one way courts can prevent that outcome, while staying safely within the framework of \textit{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...
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 spaces237—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 century241 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 torts.

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 doctrine247—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 DPPA252 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

245. Solove, supra note 62, at 484.
246. See Abril, supra note 237, at 2.
247. See supra Part I.A.
recognized by the law. Eavesdropping was a crime at common law. Fourth Amendment jurisprudence and “the constitutional right to information privacy [and] evidentiary privileges” 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.” 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.” Professor Citron has argued that courts can look to the seventy years preceding Prosser’s work as a way to revitalize their privacy inquiries. 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.” Another commentator has suggested, drawing on fiduciary law, that courts could impose a duty to secure the information they obtain on “data confidants.” 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.

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” that famously motivated the Warren-Brandeis conception of privacy and that spurred the development of privacy law in America. Rather, plaintiffs suing under

253. Solove, supra note 62, at 492.
254. Id. at 478.
256. Calo, supra note 228, at 1131.
257. Citron, supra note 238, at 1832–34.
260. Solove & Citron, supra note 103, at 786.
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.
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).
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.