Washington Law Review

Volume 95 | Number 3

10-1-2020

Data Protection in Disarray

Thomas D. Haley
University of Virginia School of Law, thaley@law.virginia.edu

DATA PROTECTION IN DISARRAY

Thomas D. Haley*

Abstract: Businesses routinely lose or misuse individuals' private information, with results that can be devastating. Federal courts often leave those individuals without legal recourse by dismissing their lawsuits for lack of standing, even though plaintiffs in these cases provide stronger showings of harm than courts usually require. Using an original data set, this Article shows how standing analysis in these cases has gone awry and argues that the standing inquiry in today's data-protection cases harms both public policy and standing doctrine.

This Article makes three contributions to literatures in federal courts and privacy. First, it shows that current federal court practice too often allows data collectors to cause harm without penalty. Data collectors—from theme parks and grocery stores to Equifax and Google—routinely collect private information improperly and inadequately protect the data they collect. This Article unpacks the various ways federal courts get standing wrong in the lawsuits that follow, such as by focusing on the particular scraps of information collected or lost via data breach to find plaintiffs have not suffered an "injury in fact." Second, this Article draws on an original data set of 217 federal data-protection decisions to demonstrate systemic pressures that lead federal courts to misapply standing doctrine in data-protection litigation. Existing scholarship focuses on analyzing a handful of leading appellate cases and therefore misses the full scope of federal courts' seeming hostility toward data-protection lawsuits. Third, by bringing to light systemic issues that have not been considered in this context, this Article proposes changes to federal courts' approach to standing in these cases that will help align the incentives and costs of data collection and help to develop a robust body of federal law on issues of data protection.

* Research Assistant Professor, University of Virginia School of Law. For helpful comments and conversations, I am grateful to Andrew Gilden, Cathy Hwang, Matthew Tokson, and Justin Weinstein-Tull and to workshop participants at Stanford Law School and the University of Richmond School of Law. Thanks also to Matthew O'Connor for excellent research assistance and the editors of *Washington Law Review* for their outstanding editing. This paper is supported in part by the Albert and Elaine Borchard Fund for Faculty Excellence.

INTRODUCTION

Six Flags theme parks require fingerprint scans from children.[1] Both Facebook and Google run facial recognition on user-uploaded photos to identify the subjects of other photos.[2] History shows that none of these companies can be counted on to keep that data private; neither can the federal courts be counted on to hear the lawsuits that follow. This Article shows how standing doctrine—an important but under-explored factor in data-protection litigation—prevents plaintiffs from prevailing in lawsuits,

1. Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, 129 N.E.3d 1197 (sustaining lawsuit arising under the Illinois Biometric Information Privacy Act ("BIPA")).

2. Patel v. Facebook Inc., 290 F. Supp. 3d 948 (N.D. Cal. 2018) (sustaining lawsuit alleging this practice violated BIPA); Rivera v. Google, Inc., 366 F. Supp. 3d 998 (N.D. Ill. 2018) (dismissing for lack of standing lawsuit alleging similar claims).

leaving them unprotected and federal laws unenforced. To do so, this Article draws on empirical analysis of hundreds of hand-collected federal decisions on standing.

Every day, businesses collect reams of individuals' personal data. Businesses use biometric identifiers like fingerprints and retinal scans ubiquitously for tasks as mundane as time tracking.[3] But in both collection and brokerage, businesses routinely violate laws meant to protect individuals' privacy. Six Flags, for example, requires season passholders to give up their fingerprints to park security and to scan their fingerprints each time they visit the park. While this data collection may help protect the theme park's crown jewels[4] from wily teenagers sharing a single season pass, Six Flags' actions also violate Illinois' Biometric Information Privacy Act.[5] Other businesses also routinely disregard federal statutes. Numerous cable companies have violated the Cable Communications Policy Act's (CCPA) data destruction requirements by illegally keeping former customers' records for years after termination of the customer relationship.[6]

Yet federal judges have been strangely hesitant to open the courthouse doors to plaintiffs in these cases. Even where defendants have clearly acted illegally, federal courts routinely dismiss data-protection lawsuits for lack of standing.[7] Drawing on analysis of a hand-collected dataset of over 200 federal data protection cases, this Article shows that factors including overreliance on inapplicable precedent and drift from the purposes of standing doctrine drive these decisions. The Article then proposes solutions for those problems.

To gain access to federal court, a plaintiff must establish that they have Article III standing by satisfying a three-part test that, in theory, applies equally to all types of cases.[8] In the United States Supreme Court's current

---

3. *See, e.g.*, McGinnis v. U.S. Cold Storage, Inc., 382 F. Supp. 3d 813 (N.D. Ill. 2019) (dismissing for lack of standing lawsuit arising from fingerprint time-tracking).

4. *See, e.g.*, *Raging Bull*, SIX FLAGS GREAT AM., https://www.sixflags.com/greatamerica/attractions/raging-bull [https://perma.cc/E9E2-B5YL] (asking "Do You Have What It Takes to Tame the Bull?"); *Giant Drop*, SIX FLAGS GREAT AM., https://www.sixflags.com/greatamerica/attractions/giant-drop [https://perma.cc/H545-LXD5] (allegedly "Taking Screams to New Heights").

5. *See* 740 ILL. COMP. STAT. 14/15(b) (2019) (setting forth restrictions on collection of biometric information).

6. *See, e.g.*, Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017) (dismissing CCPA lawsuit for lack of standing); Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925 (8th Cir. 2016) (same).

7. *See Gubala*, 846 F.3d 909; *Braitberg*, 836 F.3d 925.

8. *See, e.g.*, Allen v. Wright, 468 U.S. 737, 750 (1984) (holding that "Article III of the Constitution confines the federal courts to adjudicating actual 'cases' and 'controversies.' . . . The Art[icle] III

conception, the crux of that inquiry is whether a plaintiff has suffered an "injury in fact" at the hands of the defendant; that is, a harm that is sufficiently "concrete" and "particularized."[9] Modern standing doctrine has primarily developed in the context of hot-button issues, including environmental protection,[10] religious schooling,[11] same-sex marriage,[12] and government surveillance.[13] This heritage proves an unsteady foundation for recent developments in data-protection litigation, where the ethereal nature of data and the possibility of harm that might flow from its loss lead the courts to additional philosophical questions. If an employee clocks in and out with her fingerprint but does not receive statutorily mandated information about retention of that fingerprint, is she harmed? If Uber lets a hacker steal a driver's name, license number, bank account number, and bank routing number, may the driver sue before the hacker uses the driver's identity?[14] As a result, courts applying the same Supreme Court precedent in the data-protection context have reached

---

doctrine that requires a litigant to have 'standing' to invoke the power of a federal court is perhaps the most important" doctrine of justiciability).

9. *See, e.g.*, Spokeo, Inc. v. Robins, __ U.S. __, 136 S. Ct. 1540, 1548 (2016) (vacating and remanding lawsuit under the Fair Credit Reporting Act for additional analysis of the concreteness of plaintiff's alleged harm).

10. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992) (dismissing for lack of standing lawsuit under citizen-suit provision of the Endangered Species Act).

11. *See* Ariz. Christian Sch. Tuition Org. v. Winn, 563 U.S. 125 (2011) (dismissing for lack of standing lawsuit challenging state's provision of tax credit to taxpayers contributing money to religious schools).

12. *See* Hollingsworth v. Perry, 570 U.S. 693 (2013) (holding private parties seeking to defend constitutionality of California's Proposition 8 lacked standing to do so where state declined to defend the proposition).

13. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (dismissing for lack of standing lawsuit by attorneys, human rights workers, and other organizations challenging widespread surveillance under the Foreign Intelligence Surveillance Act). Richard Fallon argues that the Supreme Court's standing jurisprudence is inconsistently applied and depends on factors including the justices' political views. *See* Richard H. Fallon, Jr., *The Fragmentation of Standing*, 93 TEX. L. REV. 1061, 1096 (2015) (noting that "[w]ith the Roberts Court, as with predecessor Courts, it is possible to distinguish judicial conservatives from liberals and to characterize some standing rulings as having either a liberal or a conservative valence"). Such concerns are not new—Gene Nichol, for example, deemed the inconsistency of standing jurisprudence "radically unsatisfying." Gene R. Nichol, Jr., *Standing for Privilege: The Failure of Injury Analysis*, 82 B.U. L. REV. 301, 304 (2002) (arguing that standing analysis "systematically favors the powerful over the powerless").

14. Put another way, Seth Kreimer has likened disagreement over the sufficiency of informational injuries to early skepticism about the theory of quantum mechanics. *See* Seth F. Kreimer, *"Spooky Action at a Distance": Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 751–52 (2016) (arguing that informational injuries "fatally undermine an account of Article III that insists on 'direct,' 'tangible,' and 'palpable' injuries to physical or economic interests as the ticket of admission to the federal courthouse, and profoundly alter notions of 'particularized' and 'imminent' injury").

results that are divergent, if not irreconcilable.

Normatively, whether isolated instances of improper data collection or data loss should suffice for standing is a contested issue. Many scholars have argued, emphatically, yes, with contentions ranging from broad theories of probabilistic standing to specific examples of courts treating privacy harms with unwarranted exceptionalism.[15] But many federal courts seem to disagree. Judicial reticence to recognize harm in data-protection litigation contributes to rampant, judicially approved, consequence-free lawbreaking by businesses, which continue to improperly collect, store, trade, and lose valuable private information. Along the way, at every level of the federal judicial system, courts have departed from prevailing formulations of standing doctrine, subverted the justifications for the doctrine's existence, and engaged freely in speculation about the nature and extent of data-protection harms.[16]

This Article bridges the gap between theory and reality in explaining federal courts' reluctance to entertain data-protection lawsuits. Part I shows that federal courts have departed from traditional conceptions of standing doctrine and its underlying purposes in data-protection litigation, to the detriment of individual litigants and the judicial system. While the scholarly literature advocates the normative position that the courts have gone astray, it is limited by its reliance on a handful of leading cases that

---

15. In general, for example, Jonathan Nash has argued for taking a present-value approach to probabilistic standing. *See* Jonathan Remy Nash, *Standing's Expected Value*, 111 MICH. L. REV. 1283 (2013) (proposing expected-value analysis as basis for assessing injury-in-fact and redressability prongs of standing inquiry). Andrew Hessick has similarly argued against requiring a high risk of harm to establish standing as unsupported by Article III. *See* F. Andrew Hessick, *Probabilistic Standing*, 106 NW. U. L. REV. 55, 58 (2012) ("Article III does not impose a minimum risk-requirement."). In the specific context of data protection, Danielle Citron and Daniel Solove argue that increased risk of identity theft and anxiety about the consequences of data breach resemble a variety of harms in other contexts that have been held enough to satisfy Article III. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 744 (2018) ("[A]nxiety and risk, together and alone, deserve recognition as compensable harms."). Julie Cohen challenges the incoherent distinctions between data-protection cases and other types of litigation, as well as those between lawsuits arising from data breaches versus data gathering. *See* Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 548 (2017) (noting that, in contrast to the urgency with which data breaches are treated, "there are no vested interests in creating a comparable sense of emergency about processes that underlie a multibillion-dollar industry"). Felix Wu explores the ways in which privacy litigation has changed courts' approach to standing at the most fundamental levels. *See* Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 439 (2017) ("Whereas older standing cases focused on whether the plaintiff before the court was the right plaintiff, the newer privacy-based cases are focused on, or making assumptions about, whether or not the harm caused by the defendant is the right kind of harm.").

16. Indeed, Wu argues that the federal courts are engaged in usurpation of the legislative branch's powers in the realm of data protection. *See* Wu, *supra* note 15, at 458.

leaves the extent of the problem unclear. Part II reveals how serious the problem of standing in data-protection litigation has become and, in doing so, provides empirical support for existing critiques of federal courts' handling of these cases. Drawing on analysis of over 200 federal decisions on standing in data-protection cases,[17] this Part identifies potential drivers of the courts' curious decision-making. Among other conclusions, this analysis shows that courts rely too heavily on the Supreme Court's 2013 decision in *Clapper v. Amnesty International USA*[18] and appear to analyze standing from the wrong starting point. Finally, Part III discusses the theoretical and practical implications of correcting these errors. Theoretically, it argues that standing doctrine requires a more nuanced approach than the mechanical application of the one-size-fits-all test currently employed by courts. Practically, it explores ways to put the courts back on course and the benefits that would flow from allowing more data-protection lawsuits to advance to determination on the merits.

I. THE LIMITS OF MODERN STANDING DOCTRINE IN DATA-PROTECTION CASES

Standing doctrine arises from the United States Constitution. Article III provides that "[t]he judicial Power shall extend to" certain, enumerated types of "Cases" and "Controversies."[19] When there is no Case or Controversy, the judicial power does not exist, and the court must dismiss the case. From this straightforward foundation rises an area of law of paramount importance—and complexity.[20]

In later Parts, this Article shows how doctrinal drift from the purposes of standing doctrine occurred in data-protection cases and why it is vitally important to refocus the doctrine. This Part sets the stage. Section I.A. provides a brief overview of the state of standing doctrine in data-protection litigation. Section I.B. highlights how standing doctrine has failed to adapt to these cases—and particularly the types of harms underlying them.

---

17. This dataset represents a substantially complete set of data-protection standing cases decided after the Supreme Court's influential decision in *Clapper*.

18. 568 U.S. 398 (2013).

19. U.S. CONST. art. III, § 2.

20. The Framers declined to define either "Case" or "Controversy" or to leave much recorded discussion on what they meant. As Chief Justice Warren put it, "those two words have an iceberg quality, containing beneath their surface simplicity submerged complexities which go to the very heart of our constitutional form of government." Flast v. Cohen, 392 U.S. 83, 93–94 (1968) (holding that taxpayers had standing to seek injunction against government spending on materials for use in religious schools).

A. Standing in Data-Protection Litigation

Standing is a threshold, jurisdictional requirement in any federal case. To cross that threshold, a plaintiff must satisfy a three-part test. They must show first, that they suffered an injury-in-fact; second, that the injury is traceable to the defendant; and third, that the injury is redressable by a favorable decision.[21] For all that the courts emphasize the constitutional nature of standing doctrine, in fact, the Constitution does not refer to standing. Rather, the doctrine is purely a judge-made interpretation of Article III's "Cases" and "Controversies" provision. The doctrine's amorphous character has led to inconsistent results that underscore the difficulties in its application.[22]

1. The Purposes of Standing Doctrine

Judges developed standing doctrine in service of two primary goals: maintaining the separation of powers and ensuring that cases are adversarial in nature.[23]

First, standing prevents the judiciary from encroaching on the responsibilities of the legislative and executive branches. Where a plaintiff has suffered no injury, or their injury is not traceable to the conduct of the defendant, suspicion arises that the plaintiff may be using the judicial system to address a political grievance—a grievance that

---

21. This is a slight simplification of the test prescribed by the Supreme Court. *See, e.g.*, Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992) ("Over the years, our cases have established that the irreducible constitutional minimum of standing contains three elements. First, the plaintiff must have suffered an 'injury in fact'—an invasion of a legally protected interest which is (a) concrete and particularized and (b) 'actual or imminent, not "conjectural" or "hypothetical."' Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be 'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.' Third, it must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'" (citations omitted)).

22. Thus, Chief Justice Warren acknowledged that "[p]art of the difficulty in giving precise meaning and form to the concept of justiciability stems from the uncertain historical antecedents of the case-and-controversy doctrine." *Flast*, 392 U.S. at 95–96.

23. *See, e.g.*, Ann Woolhandler & Caleb Nelson, *Does History Defeat Standing Doctrine?*, 102 MICH. L. REV. 689, 694 (2004) ("The question of which parties may properly come to court to vindicate these different kinds of legal rights is central to the issue of standing. In trying to address that question, American courts have traditionally drawn partly upon general principles of jurisprudence and partly upon distinctively American ideas about popular sovereignty, limited government, and the separation of powers."); *see also* Hessick, *supra* note 15, at 56 ("Courts cannot decide legal questions in the abstract based on hypothetical disputes. As the Supreme Court has told us, the case-or-controversy requirement of Article III limits the federal judiciary to resolving legal questions only in the context of redressing or preventing an 'actual' or threatened injury resulting from violations of the law.").

should be addressed by the elected branches of government.[24] This justification has clear appeal. *Fairchild v. Hughes*[25] is a paradigmatic case. In that case, plaintiff Charles Fairchild, a New York businessman, sued to restrain the government from enforcing the Nineteenth Amendment, which prohibits the government from denying citizens the right to vote on the basis of sex.[26] Fairchild's theory of the case was strained, to put it charitably. He argued that the Secretary of State was on the verge of proclaiming the Nineteenth Amendment valid.[27] This, in turn, meant that the Attorney General could soon be called upon to enforce it.[28] Fairchild alleged there were questions about the validity of the process of the Amendment's passage through state legislatures.[29] Thus, if the Secretary of State and Attorney General did what he predicted, they would mislead state election officials into permitting women to vote, thereby "prevent[ing] ascertainment of the wishes of the legally qualified voters."[30] The Supreme Court denied standing, recognizing this as a politically-motivated and convoluted attempt by a private litigant to coerce the judiciary into stepping outside its role in the constitutional structure.[31]

Second, standing is necessary for the functioning of the adversarial system employed by the federal courts. That system relies primarily on opposing parties with enough at stake in the dispute to ensure that all relevant evidence, law, and argument on any given issue is put before the judge.[32] This "adversarial system" justification for standing doctrine is at least as appealing as the separation of powers. It is easy to see that legal

---

24. *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013) (noting that "[t]he law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches"). Justice Powell characterized standing as necessary to prevent the use of the judicial system for "amorphous general supervision of the operations of government." United States v. Richardson, 418 U.S. 166, 192 (1974) (Powell, J., concurring) (opining that expanding the judicial power to taxpayer suits would work to the detriment of the federal judicial system).

25. 258 U.S. 126 (1922).

26. U.S. CONST. amend. XIX ("The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any state on account of sex.").

27. *Fairchild*, 258 U.S. at 127–28.

28. *Id.*

29. *Id.* at 127.

30. *Id.* at 128.

31. *Id.* at 129.

32. *See, e.g.*, United States v. Fruehauf, 365 U.S. 146, 157 (1961) (extolling the "clear concreteness provided when a question emerges precisely framed and necessary for decision from a clash of adversary argument exploring every aspect of a multifaceted situation embracing conflicting and demanding interests").

precedent created on an issue being argued by parties who lacked sufficient incentive to put on their best case may be flawed.[33] By closing the courthouse doors in these instances, standing doctrine helps to preserve the benefits of an adversarial, common-law judicial system.

However, neither of these justifications applies to all types of cases. Lawsuits between private parties typically implicate the adversarial justification but have little to do with the separation of powers. *Johnson v. United Air Lines, Inc.*,[34] a recent district court case, provides an example. *Johnson* arose from United's requirement that Johnson, a baggage handler, use his fingerprints to clock in and out of work.[35] United, in violation of a statute, did not disclose its data-retention practices or obtain consent from Johnson and his coworkers to collect their biometric information.[36] This dispute does not raise any separation-of-powers concerns. It is for the courts to adjudicate whether a defendant has violated law and in doing so harmed a plaintiff. But questions might linger whether plaintiffs have enough at stake in such a case to put forth meaningful argument and evidence. In *Johnson*, plaintiff alleged only that he and his colleagues were deprived of notice and disclosure mandated by a statute.[37] Whether that gave him enough of a stake in the dispute to put forth a serious case is less clear than, for instance, a claim that defective equipment caused a suitcase to fall on him.

Despite the lack of overlap in the leading justifications for standing doctrine, the Supreme Court mandates a one-size-fits-all inquiry. It is no surprise, then, that the federal courts have struggled to consistently apply the test. That lack of consistency manifests in the courts' varied treatment of cases depending on the context in which they arise.[38] The burgeoning area of data-protection litigation is a prime example.

2. Confounding Strains of Data-Protection Litigation

Various factors in data-protection litigation further complicate the standing inquiry. Imagine a typical data breach: hackers have stolen data from millions of consumers stored by, say, an online retailer. But what types of data? How much? What can the hackers reasonably be expected

33. Examples of federal courts doing exactly that in data-protection litigation are discussed in section II.B.

34. No. 17 C 08858, 2018 WL 3636556 (N.D. Ill. July 31, 2018).

35. *Id.* at *1.

36. *Id.*

37. *Id.* at *3.

38. *See, e.g.*, Fallon, *supra* note 13, at 1071–80 (analyzing divergent standing analysis in cases arising in contexts such as the Establishment Clause, the Equal Protection Clause, and national security).

to do with the data? Have affected consumers seen signs of identity theft? If so, are they attributable to this hack, or any number of other hacks over the years?

Still more confounding factors arise in cases where companies have improperly collected data but have not lost it. Cable companies, for instance, routinely retain personal information of former customers. The CCPA forbids this practice, but the customer has no reason to believe anybody other than the cable company has access to the information. Is the bare statutory violation enough of a harm to establish standing?

Decisions on standing have turned on the answers to these questions, and the outcomes are not consistent. This Article identifies three leading categories of confounding factors present in data-protection litigation: the probabilistic harm strain, the intangible harm strain, and the temporal strain.

a. The Probabilistic Harm Strain

A common question in data-protection litigation is one of probabilities. Plaintiffs in these cases are worse off than they would have been had data collectors better secured their data, or not retained it beyond the period authorized by statute. But it is hard for judges—or anyone—to estimate precisely how much harm plaintiffs will suffer. A hacker might use stolen information to bring one plaintiff to absolute financial ruin; another plaintiff's information might never be used. The cable company might lose improperly retained information, subjecting the plaintiff to that same roll of the dice; but then, the company might never lose the data.

Because probabilistic standing is at the heart of much data-protection litigation, *Clapper*, a case arising out of post-9/11 government surveillance, looms large over the analysis.[39] There, respondents sued to enjoin NSA surveillance conducted under the Foreign Intelligence Surveillance Act of 1978.[40] Amendments to that Act permitted the NSA to surveil a target without demonstrating probable cause that the target "is a foreign power or agent of a foreign power" and without specifying "the nature and location of each of the particular facilities or places at which

39. Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013). Other scholars pin much of the blame for judicial mishandling of privacy cases on the *Clapper* decision. *See, e.g.*, Solove & Citron, *supra* note 15, at 741 (noting that "[i]n decision after decision, courts have relied on *Clapper* to dismiss data-breach cases"); *see also id.* at 744 (noting that "*Clapper* and *Spokeo* have led to confusion about how harms involving personal data should be conceptualized"). That contention finds substantial empirical support. *See infra* section II.A.

40. *Clapper*, 568 U.S. at 406–07.

the electronic surveillance will occur."[41] Respondents challenged the constitutionality of this statutory scheme. To support standing, they alleged "that there is an objectively reasonable likelihood that their communications will be acquired" by NSA surveillance and "that the risk of surveillance . . . is so substantial that they have been forced to take costly and burdensome measures to protect the confidentiality of their international communications."[42]

The Supreme Court, invoking the separation-of-powers justification,[43] rejected respondents' arguments. With respect to respondents' claimed future harm—the "objectively reasonable likelihood" of communications interception—the Court held that for a future harm to be "concrete" enough to support standing, it must be "certainly impending."[44] Writing for the majority, Justice Alito characterized respondents' argument as a five-step chain of causation, which he deemed "their highly speculative fear."[45] In contrast, the dissent proceeded from the adversarial justification[46] in contending that respondents established a sufficient probability of future harm to justify standing.

In Part II, this Article analyzes hundreds of data-protection cases decided after *Clapper* to show, among other things, that *Clapper* has become a core piece of the courts' reasoning in data-protection litigation. Numerous leading circuit court opinions in data-protection cases have discussed *Clapper*, usually extensively, in assessing standing.[47] In the

41. *Id.* at 404.

42. *Id.* at 407.

43. *Id.* at 408 ("The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches.").

44. *Id.* at 409–10 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 565 (1992)).

45. *Id.* at 410 ("[R]espondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the [Foreign Intelligence Surveillance Court] will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.").

46. Standing "helps to ensure that the legal questions presented to the federal courts will not take the form of abstract intellectual problems resolved in the 'rarified atmosphere of a debating society' but instead those questions will be presented 'in a concrete factual context conducive to a realistic appreciation of the consequences of judicial action.'" *Id.* at 423 (Breyer, J., dissenting) (citations omitted) (quoting Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 472 (1982)).

47. *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017); Beck v. McDonald, 848 F.3d 262, 267–68 (4th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016); *In re* SuperValu, Inc., 870 F.3d 763, 769 (8th Cir. 2017); Remijas v. Neiman Marcus Grp.,

federal judicial system as a whole, of the 209 data-protection cases studied for this Article, 49% cited *Clapper*—and that number rises to 69% of decisions finding that plaintiffs lacked standing.[48]

But *Clapper* is the wrong foundation for conducting a standing inquiry in data-protection litigation for several reasons.[49] Most substantially, it is a poor fit in that separation-of-powers concerns predominate: the case involves a claim against the government based on an allegedly unconstitutional statutory scheme[50] and directly implicates issues of national security.[51] In contrast, most data-protection cases involve private, non-governmental parties in disputes unrelated to such lofty issues.

Clapper is not the only source of confusion. As a general rule, federal decisions on standing in data-protection litigation are not a model of clarity. The confusion goes all the way to the top, with the Supreme Court's decision in *Spokeo, Inc. v. Robins*.[52] There, Thomas Robins sought to bring a class-action lawsuit against the "people search engine" Spokeo for alleged violation of the Fair Credit Reporting Act (FCRA).[53] According to the complaint, Spokeo gathered and disseminated information about Robins such as that he was married with children, had a graduate degree, and was employed at a high-paying job.[54] Unhappily for Robins, none of that was true.[55] Robins alleged that Spokeo's inaccurate reporting violated the FCRA's requirement that entities like Spokeo ensure the accuracy of their reporting, entitling Robins to an award of statutory damages.[56]

LLC, 794 F.3d 688, 692 (7th Cir. 2015).

48. More detailed empirical analysis of *Clapper*'s impact on data-protection cases is set forth in Part II.

49. Among them the fact that Justice Alito's casual dismissal of respondents' fears quickly proved to be so very wrong. *See, e.g.*, Jameel Jaffer & Patrick C. Toomey, *How the Government Misled the Supreme Court on Warrantless Wiretapping*, THE NATION (Dec. 18, 2013), https://www.thenation.com/article/archive/how-government-misled-supreme-court-warrantless-wiretapping/ [https://perma.cc/GK3K-WE98] (discussing Edward Snowden's revelations about NSA wiretapping).

50. *See Clapper*, 568 U.S. at 408 ("In keeping with the purpose of [standing] doctrine, 'our standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional.'").

51. *See id.* at 409 ("[W]e have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs.").

52. __ U.S. __, 136 S. Ct. 1540 (2016).

53. *Id.* at 1544.

54. *Id.* at 1546.

55. *Id.*

56. *Id.* at 1545 (noting the FCRA requires that "consumer reporting agencies . . . 'follow reasonable

Robins's difficulty arose from the fact that he asserted only a "technical" violation of the FCRA—in other words, Spokeo violated a statute, but it was not clear that Robins was harmed by the violation. For the District Court, that was not enough to confer standing.[57] The Ninth Circuit disagreed,[58] and many commentators believed the Supreme Court's subsequent grant of certiorari would lead to a decision clarifying standing issues in data-protection litigation.[59]

The Supreme Court did not oblige. After reiterating the importance of standing doctrine to ensuring the separation of powers,[60] the Court punted on the fundamental issue by splitting the "concrete and particularized" element of the injury-in-fact test, holding that the Ninth Circuit did not properly analyze the "concreteness" of Robins's harm, and remanded for further consideration.[61] As a result, *Spokeo* stands for little more than a reaffirmation that intangible harms *can be* sufficiently concrete to confer standing—but provides no guidance on how to assess concreteness.

b. The Intangible Harm Strain

Perhaps the only point of agreement among the circuit courts is that actual evidence of identity theft closely following a data breach is actionable.[62] But the more typical case involves harms that are much less tangible—breach or improper collection has occurred, but identity theft has not yet been observed. Several circuits have denied standing in these

---

procedures to assure maximum possible accuracy of' consumer reports," and subjects "'any person who willfully fails to comply with any requirement [of the FCRA] with respect to any individual' . . . [to] 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").

57. Robins v. Spokeo, Inc., No. CV10–05306 ODW, 2011 WL 597867, at *1–2 (C.D. Cal. Jan. 27, 2011) (finding allegations of possible future harm insufficient for standing).

58. Robins v. Spokeo, Inc., 742 F.3d 409, 413–14 (9th Cir. 2014) (holding plaintiff's allegations of violation of statutory rights under the FCRA sufficed for standing).

59. *See, e.g.*, Daniel Townsend, *Who Should Define Injuries for Article III Standing?*, 68 STAN. L. REV. ONLINE 76, 77 (2015) (stating that "the Supreme Court is not in the business of simple error correction, and *Spokeo* would not have garnered so much attention—including over thirty amicus briefs—if it presented only a question that was easily resolved by preexisting standing doctrine").

60. *Spokeo*, 136 S. Ct. at 1546–47 ("The Constitution confers limited authority on each branch of the Federal Government. . . . In order to remain faithful to this tripartite structure, the power of the Federal Judiciary may not be permitted to intrude upon the powers given to the other branches. . . . [Standing] doctrine developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood.").

61. *Id.* at 1548–50 (elucidating a distinction between "concrete" and "particularized" for purposes of standing analysis).

62. *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017) ("Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury.").

types of cases. For example, the Fourth Circuit denied standing in *Beck v. McDonald*,[63] where two data breaches at a medical center resulted in the loss of the plaintiffs' personal information including names, social security numbers, birth dates, physical descriptors, and medical diagnoses.[64] The Fourth Circuit pointed to the absence of allegations that the compromised information had been used to plaintiffs' detriment in the intervening years in denying standing. Similarly, the Eighth Circuit denied standing to all plaintiffs save one in *In re SuperValu, Inc.*,[65] in which hackers breached the payment-card system of a grocery chain.[66] The only plaintiff who squeaked through the standing inquiry was the one who alleged a fraudulent charge appeared on his payment card.[67] The court looked to the fact that no social security numbers, birth dates, or driver's license numbers were alleged to have been stolen, and found that without that information it would be unlikely that the data thief could open new accounts using plaintiffs' identities.[68]

The Seventh Circuit's decision in *Remijas v. Neiman Marcus Group LLC*[69] stands as the polar opposite to *Beck* in the data-breach context. Where *Beck* found no standing even though bad actors purloined highly sensitive information including social security numbers, *Remijas* found standing even though plaintiffs alleged only the theft of credit card numbers, not social security numbers or birth dates. *Beck* relied on a constellation of highly specific and often dubious arguments against finding standing, such as distinguishing other cases on the grounds that they involved allegations that "the data thief intentionally targeted the personal information compromised in the data breaches."[70] *Remijas* offers a more straightforward approach that seems more apt for what is supposed to be a threshold, non-merits inquiry, finding it plausible to infer that hackers who obtained the private information of plaintiffs intended to use

63. 848 F.3d 262 (4th Cir. 2017).

64. *Id.* at 267 (finding plaintiffs lacked standing to sue based on risk of harm following data breach that compromised personally identifying information and health information).

65. 870 F.3d 763, 766 (8th Cir. 2017).

66. *Id.* (finding plaintiffs lacked standing to sue based on risk of harm following data breach that compromised payment card information).

67. *Id.* at 772.

68. *Id.* at 770.

69. 794 F.3d 688 (7th Cir. 2015).

70. Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017). *Beck* is not the first appellate decision to indulge in curious arguments about a data thief's motivations. In *Reilly v. Ceridian Corp.*, the Third Circuit denied standing in part on the grounds that "[h]ere, there is no evidence that the intrusion was intentional or malicious." 664 F.3d 38, 44 (3d Cir. 2011).

that information, to plaintiffs' detriment.[71]

Indeed, *Beck* notwithstanding, courts have been more apt to find standing when more information is allegedly lost. For instance, in two recent cases,[72] data breaches led to loss of information including names, birth dates, and social security numbers, among other types of information. Both courts found the threat of harm sufficient to confer standing.[73] Moreover, the Sixth Circuit echoed *Remijas*, finding it plausible to infer a substantial risk of harm from hackers obtaining the personal information of plaintiffs and declining to penalize plaintiffs for filing suit before actually suffering identity theft.[74]

Cases involving wrongful collection rather than data breach present distinct issues. The Supreme Court's failure to offer meaningful guidance in *Spokeo* is of particular importance in these cases. In one influential case, *Gubala v. Time Warner Cable, Inc.*,[75] the plaintiff learned that Time Warner Cable continued to keep private information about him, including his date of birth, social security number, address, phone numbers, and credit card information some eight years after he cancelled his cable subscription. The plaintiff alleged that this constituted a straightforward violation of the CCPA, which required Time Warner to destroy all that information once it no longer had a customer relationship with Gubala.[76] But the Seventh Circuit found that Time Warner's unauthorized retention of plaintiff's information did not actually harm plaintiff.[77]

---

71. *See Remijas*, 794 F.3d at 693 ("At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

72. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 622–23 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386–87 (6th Cir. 2016) (finding plaintiffs had standing to sue based on risk of future harm following data breach that compromised personal information).

73. *See Attias*, 865 F.3d at 622–23; *Galaria*, 663 F. App'x at 386–87.

74. *Galaria*, 663 F. App'x at 388 ("There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. . . . Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security.").

75. 846 F.3d 909 (7th Cir. 2017) (finding plaintiff lacked standing to sue based on defendant's unlawful retention of personal information beyond time mandated for destruction).

76. *Id.* at 910. Specifically, the statute "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 to such information." *Id.*

77. *Id.* at 913.

c. The Temporal Strain

Further complicating matters is the fact that many data-protection cases do not involve observed identity theft, and for good reason. As the Seventh Circuit noted in *Remijas*, the longer a plaintiff waits for identity theft to occur before bringing suit, the more likely a defendant is to be able to argue that an intervening data breach caused the harm.[78] Plaintiffs stuck choosing between suing shortly after a data breach (alleging only an increased risk of identity theft) or years down the line when fraudulent charges have appeared (possibly as a result of any number of other intervening data breaches) have generally chosen the former course. In doing so, they often trade a merits problem for a threshold one. Judicial demands for allegations of actual identity theft force plaintiffs into a lose-lose situation.

B. Recurring Errors

That the federal courts get standing in data-protection litigation wrong cannot, of course, be taken for granted. Scholars have raised many issues with the courts' reasoning in leading cases—for example, shifting the locus of the standing inquiry, myopically viewing asserted harms, and miscalculating risk. Pulling together these strains of criticism, broader discussion of standing doctrine, and analysis of the case law, this Article shows that courts routinely err in these cases in two critical ways. First, courts wrongly focus on the nature of the harm rather than the party asserting the harm. Second, courts flub their assessment of the harm itself.

1. Harm-Centered Standing

The three-part standing test's purpose and effect were, from its inception and for decades, focused on ensuring that the correct *plaintiff* brought a given claim.[79] Cases since *Clapper*, however, have pivoted away from focusing on the party asserting a harm and toward an inquiry into the sufficiency of the harm itself, injecting further confusion in data-

78. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Requiring the plaintiffs 'to wait for the threatened harm to materialize in order to sue' would create a different problem: 'the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not "fairly traceable" to the defendant's data breach.'" (citations omitted)).

79. *See, e.g.*, Flast v. Cohen, 392 U.S. 83, 99–100 (1968) (holding that "when standing is placed in issue in a case, the question is whether the person whose standing is challenged is a proper party to request an adjudication of a particular issue and not whether the issue itself is justiciable"); *see also* Wu, *supra* note 15, at 440–44 (collecting cases).

protection cases. As Felix Wu has convincingly demonstrated, data-protection cases are driving this shift, with consequences that cascade outside the realm of data-protection litigation.[80]

The Supreme Court's historic focus on party rather than harm is evident from the early modern standing cases. *Flast v. Cohen*,[81] for example, recognized that "[t]he fundamental aspect of standing is that it focuses on the party seeking to get his complaint before a federal court and not on the issues he wishes to have adjudicated."[82] In his survey of major standing cases, Wu demonstrates that the focus on party prevailed at least until *Clapper*.[83] But lower court cases following *Clapper*, and arguably the Supreme Court itself in *Spokeo*, focused the inquiry on whether privacy harms are "harm" for purposes of standing.

The Seventh Circuit's standing dismissal in *Gubala* is the paradigmatic case. There, the court held that the aggrieved cable customer could "no more sue than someone who, though he has never subscribed and means never to subscribe to a cable company, nevertheless is outraged by the thought that Time Warner and perhaps other cable companies are violating a federal statute with apparent impunity."[84] In other words, the court held expressly that, for standing purposes, the identity of the plaintiff is irrelevant, or at most secondary to the question of whether there has been a proper harm. That holding could not be farther from the rule followed by the Supreme Court for decades that standing is about the parties, not the issues. It is also difficult to situate within either of the primary justifications for standing. The separation of powers is not enhanced by focusing on harm rather than party; if anything, the opposite is true—the *Gubala* court's hypothetical concerned citizen, like the plaintiff in *Fairchild*, sets up the quintessential separation-of-powers standing dismissal. Likewise, the concerned citizen has little, if any, stake in the outcome of such a dispute compared to an affected former customer. *Gubala*, therefore, cannot be said to proceed from the adversarial justification either.[85]

---

80. Wu, *supra* note 15, at 446–57 (tracing development of standing jurisprudence).

81. 392 U.S. 83 (1968).

82. *Id.* at 99.

83. *See* Wu, *supra* note 15, at 442–46 (discussing, inter alia, *City of Los Angeles v. Lyons*, *Lujan v. Defenders of Wildlife*, and *Summers v. Earth Island Institute*).

84. Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 911–12 (7th Cir. 2017).

85. Highlighting how unmoored the *Gubala* decision is from earlier conceptions of standing, Wu notes that the Seventh Circuit "effectively treated as insignificant the fact that the plaintiffs in the case were suing on the basis of *their* information having been retained and not someone else's information—precisely the sort of fact that was of crucial significance in cases like *Lujan*." Wu, *supra* note 15, at 456 (emphasis in original).

A harm-focused approach also contributes to the fragmentation of standing, to use the term coined by Richard Fallon.[86] Fallon describes a tendency in the Supreme Court's standing decisions toward complex, confusing, and irreconcilable distinctions between various types of cases, all purportedly decided pursuant to the same three-part test for standing. His examples primarily involve public rights and actors: challenges to government conduct, such as cases arising under the Establishment Clause, Equal Protection Clause, national security, challenges to agency procedures, cases brought by governmental actors and entities, and probability-based challenges to government conduct.[87] The harm-focused approach emerging in data-protection litigation gives rise to similar fragmentation in disputes between private parties asserting private rights, such as the typical data-breach case of a privacy claim against a private enterprise.

As Fallon recognizes, a complex doctrine of standing is not necessarily a bad thing.[88] As discussed above, the best justification for standing doctrine varies from case to case; intuitively, the question of whether a given plaintiff may sue to stop large-scale government surveillance raises entirely different issues than whether a plaintiff may sue to make a cable company delete retained customer information. But hiding such complexity behind a one-size-fits-all test and repeated invocations of vague, high-minded concepts like the separation of powers serves no one.[89] Confusion is the inevitable result of this approach, as is "suspicion of naked, result-oriented manipulation."[90]

Worse still, as Wu argues, shifting focus to the sufficiency of an alleged harm usurps the role of the legislative branch,[91] directly contrary to the justification for standing doctrine invoked in most recent Supreme Court standing jurisprudence.[92] Particularly where, as in *Gubala*, a plaintiff sues

---

86. *See* Fallon, *supra* note 13, at 1070 ("By 'fragmentation,' I mean the division of standing law into multiple compartments, most of which may be intelligible in themselves, but that reflect more conceptual and normative diversity than unity.").

87. *See id.* at 1070–92 (collecting examples of divergent approaches to the standing inquiry).

88. *See id.* at 1092 ("In principle, doctrinal complexity . . . could promote valid purposes, even if it made knowledge of the law harder to attain. Nearly all rules are over or underinclusive when measured against their background justifications. Without wholly eliminating over and underinclusivity, a more complex system of rules might, under some circumstances, produce better outcomes than a simpler, more elegant doctrinal structure.").

89. *See, e.g.*, *id.* at 1116 ("In the domain of standing law, we should recognize simplicity and elegance as illusions.").

90. *Id.* at 1094.

91. *See* Wu, *supra* note 15, at 451 (arguing that dismissal of federal statutory claims on standing grounds "shifts the locus of control over the development of the law").

92. *See, e.g.*, Spokeo, Inc. v. Robins, __ U.S. __, 136 S. Ct. 1540, 1547 (2016) ("[By] limit[ing]

under a federal statute, a rule rejecting standing for violation of the statute prevents both enforcement of the statute and development of precedential interpretation of that statute. For Wu, this represents constitutionalizing a deregulatory agenda.[93]

While there is reason to believe that the current state of affairs is not so dire,[94] the implications of this change in focus are tremendous. Developing a robust body of law inviting judges to find a plaintiff has no standing based on a threshold, supposedly non-merits assessment of her injury necessarily invites judges to indulge their own beliefs and biases. For instance, in the context of constitutional litigation, it is already apparent that Supreme Court case law develops largely from the views of the justices on the rights in question.[95] It would be in the public interest to make that kind of outcome more difficult to reach; a focus on asserted harms makes it far easier. Such activity is also observable in data-protection litigation, where judicial skepticism has the potential to wreak havoc on privacy law.[96]

2. The Sufficiency of Harm

Shifting to a harm-based standing inquiry might raise less concern if the courts could be counted on to assess harms consistently and accurately. At least in the data-protection context, they have not done so. Scores of cases dismissing data-protection lawsuits for perceived lack of harm misunderstand the risks in question, fail to treat probabilistic injuries seriously, and ignore the non-monetary harms that flow from data-

---

the category of litigants empowered to maintain a lawsuit in federal court to seek redress for a legal wrong . . . '[t]he law of Article III standing . . . serves to prevent the judicial process from being used to usurp the powers of the political branches' and confines the federal courts to a properly judicial role." (citations omitted)).

93. *See id.* at 460 ("Standing becomes a means by which politically desirable regulation is struck down by the courts. Whatever the merits of a deregulatory agenda, that agenda should be established, if at all, through the political process.").

94. *See infra* section II.A.3 (showing that federal statutory claims fare reasonably well against standing challenges in data-protection litigation).

95. *See* Fallon, *supra* note 13, at 1095–96 ("[T]he Justices' substantive constitutional views inevitably drive standing decisions in a number of important areas."); *see also* Nichol, *supra* note 13, at 304 ("As elite judges summarily determine which interests are worthy of legal cognizance, they unsurprisingly embrace concerns that strike closest to home, sustaining 'harms' that mirror the experiences and predilections of their own lives.").

96. *See* Wu, *supra* note 15, at 450. Wu argues that by throwing out cases for lack of standing where courts have doubts about the existence of a cognizable harm, "courts are not only adopting a particular perspective on the nature and value of privacy, they are shifting the law on standing to one that allows courts to dismiss claims on the basis of their views on the nature and value of the asserted harms. That shift will have effects far beyond the privacy cases that precipitated it." *Id.*

protection violations. In doing so, they eschew reasoning that has rendered the standing inquiry an afterthought in numerous other contexts.

a. Underestimating the Risk of Identity Theft

Two considerations have taken on an almost talismanic nature for federal courts assessing the risk of identity theft following a data breach: what specific information is at issue, and whether plaintiffs have already seen signs of identity theft. As to the latter, courts generally find that allegations of actual identity theft suffice for standing.[97] But where a plaintiff's identity has not yet been stolen, the specific information involved often decides the case.

Many courts have demanded that substantial amounts of personally identifiable information (PII) be taken to present a substantial risk of harm. Take *SuperValu*, for example. SuperValu, which operated chains of grocery and liquor stores, suffered a data breach affecting its cash register system at over 200 stores.[98] The company allegedly employed poor security practices, including the use of default passwords, despite the valuable and sensitive information stored on its servers.[99] The hack compromised customer information including names, credit card numbers, three-digit verification codes, and PINs. But the Eighth Circuit found that plaintiffs did not allege a sufficient injury-in-fact, citing the lack of personally identifiable information in the compromised data.[100] In the court's view, the information taken would not enable the hackers to open new accounts in plaintiffs' names, and therefore plaintiffs failed to plead a substantial risk of harm.[101]

Focusing on PII does have intuitive appeal. An allegation that a

---

97. *See, e.g.*, *In re* SuperValu, Inc., 870 F.3d 763, 772 (8th Cir. 2017) ("[P]laintiff Holmes alleges a present injury in fact to support his standing. He alleges that he suffered a fraudulent charge on the credit card he previously used to make a purchase at one of defendants' stores affected by the data breaches.").

98. *See, e.g.*, Nicole Perlroth, *Supervalu Discloses a Data Breach*, N.Y. TIMES (Aug. 15, 2014), https://www.nytimes.com/2014/08/16/technology/food-retailer-discloses-a-data-breach.html [https://perma.cc/8ZVW-L8QL] (reporting that breach affected 180 SuperValu stores and 29 franchised stores).

99. *See SuperValu*, 870 F.3d at 766.

100. *See id.* at 770 ("Initially, we note that the allegedly stolen Card Information does not include any personally identifying information, such as social security numbers, birth dates, or driver's license numbers.").

101. *Id.* ("[P]ursuant to the factual evidence relied on in the complaint, there is little to no risk that anyone will use the Card Information stolen in these data breaches to open unauthorized accounts in the plaintiffs' names, which is 'the type of identity theft generally considered to have a more harmful direct effect on consumers.'" (citations omitted)).

defendant has allowed bad actors to obtain PII suggests that the plaintiff is at high risk of identity theft—the bad actor has all the information they need to obtain credit in the plaintiff's name or otherwise impersonate the plaintiff.

But it is not true, as cases like *SuperValu* hold, that loss of less or different information means a plaintiff is not at risk. Information does not exist in a vacuum. Researchers have for decades demonstrated that supposedly non-identifying information can be aggregated, analyzed, and reidentified. Paul Schwartz and Daniel Solove, for instance, discuss the example of AOL's 2006 release of twenty million search queries that AOL had fully anonymized—users were described only by a number.[102] Researchers nevertheless were able to identify the person behind the number in many cases simply by collating searches.[103] Paul Ohm provides another bracing example: "How many other people in the United States share your specific combination of ZIP code, birth date (including year), and sex? According to a landmark study, for 87 percent of the American population, the answer is zero; these three pieces of information uniquely identify each of them."[104] One recent study found that reidentification becomes possible given only a few attributes, and that access to fifteen demographic attributes would uniquely identify 99.98% of individuals.[105]

To focus on the completeness of PII lost in a data breach is therefore too narrow, and, indeed, it is emblematic of what Schwartz and Solove have called "the PII problem,"[106] as it overemphasizes particular types and groupings of information. Again, *SuperValu* proves instructive. Even considering the lost information in isolation, the court's finding seems intuitively odd. But it is even harder to reconcile when combined with the fact that modern data thieves often have access to other troves of information including names, social security numbers, and dates of birth.

---

102. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1841 (2011) (discussing examples of users identified from "fully anonymized" search queries).

103. *Id.*

104. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1705 (2010) (arguing that reidentification "sound[s] the death knell for the idea that we protect privacy when we remove PII from our databases").

105. Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, NATURE COMMC'NS, July 23, 2019, at 5 (noting that "[o]ur results, first, show that few attributes are often sufficient to re-identify with high confidence individuals in heavily incomplete datasets and, second, reject the claim that sampling or releasing partial datasets, e.g., from one hospital network or a single online service, provide plausible deniability").

106. Schwartz & Solove, *supra* note 102 (arguing for a new theoretical approach to PII accounting for the malleability of information).

Aggregation of that data with the information lost in the SuperValu breach gives the thieves everything they need to perpetrate identity theft on a massive scale. The risk to the plaintiffs in any given data breach is thus much higher than is stated by those courts that narrowly focus their inquiry into harm.

b. Economic Harm and Probabilistic Injuries

Speculative and inaccurate judicial estimation of the risk of harm is particularly galling because there is no textual or logical basis for such a practice.[107] The Supreme Court's standing jurisprudence clearly establishes that the bar for monetary loss to constitute injury-in-fact is incredibly low, if it exists at all.[108] Yet courts still demand increasingly higher risk of harm in order to find standing based on a possible future injury.

It is therefore troubling that the federal courts do not meaningfully engage the concept of expected value in assessing the existence of an Article III harm in data-protection litigation. Expected value is an economic concept used widely in law, economics, psychology and other fields to neatly estimate the value of a future harm by multiplying the size of the harm by the probability that it will occur.[109] Others have discussed how expected value might be used in lawsuits to assess harm. Jonathan Nash notes, for example, that mortality risks of 1 in 100,000 would suffice for a showing of injury in fact.[110] While the consequences that flow from a privacy harm may not typically include death, and the probability that they will occur is not susceptible to easy calculation, even a rudimentary calculation of expected value would seem to establish the existence of a harm in a typical data-protection case.[111] For example, a 2014 study by

---

107. *See* Hessick, *supra* note 15, at 65 (noting that "Article III does not distinguish between low risks of harm and high risks of harm"); *see also id.* at 67 (arguing that "[w]hat this means is that all claims based on risk of injury present an actual case or controversy, no matter how small the risk. So long as (1) the challenged activity increases the plaintiff's risk of suffering harm and (2) a judicial order could stop the challenged activity, thereby removing the increased risk of harm, courts should have Article III jurisdiction to hear the claim").

108. *See, e.g.*, Czyzewski v. Jevic Holding Corp., __ U.S. __, 137 S. Ct. 973, 983 (2017) (noting that "[f]or standing purposes, a loss of even a small amount of money is ordinarily an 'injury'"); McGowan v. Maryland, 366 U.S. 420, 430–31 (1961) (finding plaintiffs who were fined five dollars each had standing); *see also* Carpenters Indus. Council v. Zinke, 854 F.3d 1, 5 (D.C. Cir. 2017) (holding that "[a] dollar of economic harm is still an injury-in-fact for standing purposes").

109. *See, e.g.*, Nash, *supra* note 15, at 1306 (proposing an expected-value test for standing where any positive expected value would suffice and defining an expected value test as "multiplying the magnitude of the harm by its probability").

110. *Id.*

111. Although those courts that have engaged in something approximating such an inquiry have

the Department of Justice found that the average loss for a victim of identity theft amounted to $1,343.[112] Even a 1/1000 risk of identity theft in the wake of a data breach would establish an expected loss of more than one dollar, the actual loss of which courts in other contexts have held sufficient for standing purposes.[113]

Furthermore, as Nash argues, the risk of harm creates present economic effects;[114] that is, risks of harm inflict present injuries separate from the expected value of that future harm. The paradigmatic example is the existence of insurance—individuals and businesses alike pay relatively small amounts in the present to cover themselves from incurring larger costs in the event of future harm.[115] In the data-protection context, news of a data breach might lead an affected customer to purchase credit monitoring, or to undertake the time-consuming and costly process of changing any affected information such as her social security number or credit card information.[116] These are real, present economic harms that result from data breaches. That a single dollar of economic harm suffices for injury-in-fact in other contexts reveals troubling exceptionalism in data-protection litigation.

c. Non-Economic Harm

In any event, injury-in-fact is not limited to economic harm. The Supreme Court has long held that non-economic interests may support standing, specifically identifying aesthetic, conservational, recreational, and spiritual interests as potentially supporting standing.[117] Data-

---

not done the inquiry credit. See, for example, the *Beck* Court's determination that a 33% chance that affected plaintiffs would suffer identity theft meant that it was more likely than not that a given plaintiff would *not* be harmed, thus precluding standing. *See* Beck v. McDonald, 848 F.3d 262, 275–76 (4th Cir. 2017).

112. *See* Cody Gredler, *The Real Cost of Identity Theft*, CSID (Sept. 9, 2016), https://www.csid.com/2016/09/real-cost-identity-theft/ [https://perma.cc/C5DM-G8FE].

113. *See Carpenters Indus. Council*, 854 F.3d at 5.

114. Nash, *supra* note 15, at 1325.

115. *Id.* at 1326 ("Indeed, individuals often act to substitute current economic cost for future risk. Consider the institution of insurance: people who insure against risks pay current dollars as the insurance premium. In return, they will be reimbursed for (at least most of) the costs of the future harm insured against.").

116. Federal courts have explicitly refused to take such costs into account in determining whether plaintiffs have suffered harm, deeming these injuries "self-imposed." *Beck*, 848 F.3d at 276–77 (collecting cases).

117. *See* Ass'n of Data Processing Serv. Orgs., Inc. v. Camp, 397 U.S. 150, 154 (1970); *see also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 562–63 (1992) ("Of course, the desire to use or observe an animal species, even for purely esthetic purposes, is undeniably a cognizable interest for purposes of standing.").

protection litigation implicates a variety of non-economic harms that courts have been hesitant to embrace.

The obvious non-economic harms flowing from a data breach are increased risk of identity theft and anxiety about the fallout of the data breach. Citron and Solove persuasively argue that these are real harms that ought to suffice for standing purposes,[118] as they have sufficed in other contexts. Increased risk of future harm, for example, has been found compensable in the medical malpractice and environmental law contexts.[119] That these types of harms suffice in those contexts is unsurprising given the strongest underlying purpose of standing doctrine in private-rights cases: ensuring that the litigants have sufficient interest and adversity to frame the issues in dispute. So, too, in the data-protection context. A plaintiff whose information has been stolen incurs increased risk of identity theft and possibly present costs to ameliorate the risk. Such a plaintiff has a clear interest in obtaining redress. The defendant has a concomitant interest in avoiding liability.

The larger harm, however, is anxiety. It is hard to envision a credit-monitoring solution so robust that a person whose information has been stolen need never think about identity theft again, to say nothing of data breaches that involve the loss of intimate or embarrassing information.[120] Surveys of data-breach victims confirm this intuition. For example, one survey of victims of the 2017 Equifax data breach found that nearly 90% of respondents "experienced adverse feelings or emotions," and 81% of that group reported feeling anxiety as a result of the breach.[121]

It should be beyond dispute that this anxiety is a cognizable harm. Courts rejecting it in data-protection cases run counter to recognition of anxiety as sufficient harm in other cases. Ryan Calo notes the quintessential example of the "tort of assault—where the harm is the emotion of fear . . . ."[122] Citron and Solove catalog other torts premised on pure emotional distress, including alienation of affection, breach of confidentiality, intentional and negligent infliction of emotional distress,

---

118. *See, e.g.*, Solove & Citron, *supra* note 15, at 744–45 ("Risk and anxiety are injuries in the here and now.").

119. *Id.* at 761–62 (discussing contexts in which courts have found future harm compensable).

120. *See id.* at 764–65 (discussing fallout from data breach at a website used to arrange adulterous relationships, including the suicides of multiple individuals affected).

121. IDENTITY THEFT RES. CTR., EQUIFAX ONE YEAR LATER: AFTERMATH REPORT 2018, at 1, 4 (2018), https://www.idtheftcenter.org/wp-content/uploads/2018/08/ITRC_Equifax-Breach-Aftermath-Report-2018-2.pdf [https://perma.cc/K9HQ-2SNS] (reporting that victims of identity theft experience emotions such as "fear regarding their personal financial security or feeling a sense of helplessness").

122. Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 363 (2014).

and the privacy torts themselves.[123] It is no longer controversial that these torts are redressable in court. Yet courts do not take analogous injuries in data-protection cases seriously, often preferring instead to concoct distinctions with no basis in logic or precedent.[124]

To the extent courts have dismissed anxiety stemming from privacy harms as too difficult to calculate, they again depart from settled rules in other contexts. Julie Cohen notes the backflips that courts are willing to perform in order to quantify damages in intellectual-property lawsuits.[125] And in any event, whether the harm is difficult to calculate goes to the issue of remedies, not standing.

Standing is vital in ensuring the constitutional role and proper functioning of the federal judiciary. Tying together various strains of scholarship helps to identify examples of federal courts drifting from the history and purpose of the doctrine in data-protection litigation. However, the focus on a relative handful of Supreme Court and appellate cases leaves unclear the extent of the potential problem. That narrow focus also makes it more difficult to identify potential causes and solutions. Part II takes the next step by surveying a broader landscape of standing challenges in data-protection cases in an effort to understand how widespread the problem has become and determine *why* the courts have drifted.

II. EXPLORING ERROR

Existing literature makes several important contributions in identifying errors and discrepancies in leading data-protection cases. But these piecemeal analyses cannot reveal whether there are systemic pressures behind the errors, and therefore are limited in what solutions they can propose.

This Part shows that systemic problems drive erroneous decisions on standing in data-protection litigation. Through analysis of hand-collected and hand-coded data derived from 217 decisions in these types of cases, this Part identifies a variety of factors leading to the aberrant decisions on standing in data-protection litigation discussed in Part I. While some of

123. Solove & Citron, *supra* note 15, at 768–73 (discussing development of legal redress for anxiety).

124. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 45–46 (3d Cir. 2011) (distinguishing medical malpractice and toxic tort cases from data breach because "there is no quantifiable risk of damage in the future" and those cases "hinge[] on human health concerns").

125. *See* Cohen, *supra* note 15, at 542 (noting, inter alia, that in copyright and patent infringement cases, courts "assign damages based on hypothesized reasonable licensing fees for imagined transactions"; "posit menus of licensing rates for nascent or nonexistent markets"; and "determine the profits attributable to infringing activity by means of arithmetically convenient fictions").

these explanations—such as path dependence—are relatively innocuous, others lend support to the view that federal courts are engaged in inappropriate policy- and preference-based decision-making.

Section II.A describes the methodology employed to assemble and code the data set underlying this Part. Section II.B presents empirical findings from the 217 cases included in the data set and the most direct explanations for erroneous decisions that arise from the data, including overreliance on *Clapper* and failure to proceed from the appropriate justification for standing. Section II.C discusses other potential explanations that find support in the case law and in existing scholarship across a number of fields, most worrying among them evidence of preference-based decisions.

A. Methodology

1. Selection of Cases

To assemble the data set analyzed in this Article, I conducted multiple searches of the Westlaw database of all federal cases decided between February 26, 2013, (the date on which the Supreme Court issued its decision in *Clapper*) and the end of 2019. Cases were identified via two search strings, designed to be fairly overinclusive: 1) op((data /p privacy) & standing); and 2) op((data /p breach) & standing).[126] In total, these searches returned 2,056 results.[127] I then manually reviewed each case to determine if the decision dealt with a challenge to standing to assert a data-protection claim—that is, a claim involving alleged wrongful collection or disclosure of private information.[128] Of the 2,056 cases reviewed, 217 fit those criteria.[129] I conducted substantially all of the analysis on a subset of 209 cases after discarding eight cases in which courts reached mixed results on standing.

---

126. Thus, search one would return all federal cases that included the words "data" and "privacy" in the same paragraph, and that also included the word "standing" anywhere in the opinion. The "op" operator restricts the search to the text of the opinion itself, thus excluding Westlaw's proprietary editorial "Headnotes."

127. The total number of results is reached by conducting one omnibus search that captures the results from both searches.

128. While I construed data-protection claims broadly, I excluded certain types of claims that fell just beyond the scope of wrongful collection or disclosure of private information, although nominally asserting privacy claims. The most frequent type of claim excluded at this edge was for unsolicited telephone calls to plaintiffs in violation of the Telephone Consumer Protection Act. *See* Hale v. Creditors Relief LLC, No. 17-2447, 2018 WL 2539080 (D.N.J. June 4, 2018).

129. The most frequent types of false positives in the search results include motions to suppress evidence in criminal proceedings and decisions in all types of cases using the rhetorical phrase "standing alone." *See* Doe v. Compact Info. Sys., Inc., No. 3:13-CV-5013-M, 2015 WL 11022761, at *5 (N.D. Tex. Jan. 26, 2015).

2. Case Coding

I reviewed all cases fitting the selection criteria and hand-coded each on a variety of issues, including:

Court;
Judge;
Decision date;
Claims asserted;
Whether the case involved a data breach;
Formulation of standing doctrine;
Standing outcome;
Merits outcome, if present;
Citation to *Clapper*; and
Citation to *Spokeo*.[130]

Across all 217 cases, I identified eighty-three distinct types of claims asserted—for example, negligence, violation of New York's General Business Law, violation of the federal Stored Communications Act, and violation of the right to privacy under the California Constitution. I then assigned each type of claim to one of fourteen second-level categories—for example, negligence is a non-privacy tort and violation of the Stored Communications Act is a federal wiretap claim. Finally, I assigned each type of claim to one of five high-level categories based on its second-level category—for example, grouping together all common-law claims and all federal statutory claims.

3. Description of the Data Set

The data set includes decisions from fifty-eight different federal courts, authored by 148 different judges.[131] In total, district court opinions account for 177 decisions in the data set, with the remaining thirty-two coming from the courts of appeals. The number of cases decided in each year analyzed varies significantly:

130. As a check on coding accuracy, a research assistant independently coded a subset of sixty-three cases on these same issues. I measured coding reliability using Cohen's kappa, finding a high degree of similarity in coding across the key measures of standing outcome ($\kappa = 0.936$), citation to *Clapper* ($\kappa = 0.935$), and presence of a data breach ($\kappa = 1$), as well as on the prevalent formulations of standing doctrine, "case or controversy" ($\kappa = 0.904$) and absence of stated formulation ($\kappa = 0.967$).

131. This figure excludes the five per curiam appellate decisions included in the dataset.

Table 1:
Breakdown of Cases by Year

Year	Number of Cases
2013	14
2014	16
2015	24
2016	37
2017	45
2018	40
2019	33

4. Limitations of the Data Set

While the data set is reasonably comprehensive, it is not without limitations. As a starting point, it is limited to decisions present in the Westlaw database, which may not include every decision from every federal court. Analysis of the decisions of appellate courts may be skewed by exogenous selection effects, namely, that a district court's denial of a motion to dismiss for lack of standing is not immediately appealable. Similarly, analysis of particular district courts may be skewed by plaintiffs' forum-shopping behavior—certain early circuit court opinions may have incentivized plaintiffs to bring claims in district courts governed by relatively friendly circuit decisions.

B. Findings

At least in the context of data-protection litigation, the federal courts appear to have lost sight of the purpose of standing doctrine. That conclusion is supported by multiple findings that emerge from the data. Most significant among those findings is that the courts rely too heavily on *Clapper* and tend to find no standing when relying on *Clapper*. Other trends apparent in the data include the courts' marked tendency not to expressly discuss the purpose of the standing inquiry, disparate results depending on the type of claim asserted, and substantial jurisdictional variations in the adjudication of standing challenges.

1. Citation to Clapper *Correlates with Denial of Standing*

Clapper has little to do with data protection by private entities—NSA communications interception at a massive scale in the name of national security implicates a host of concerns that do not arise when private

entities obtain or lose control of private information. That has not stopped it from becoming the go-to Supreme Court precedent for lower courts grappling with challenges to standing in data-protection litigation. Indeed, nearly all the major appellate cases discussed in this Article engage extensively with *Clapper*.[132] In doing so, the courts of appeals ingrained the idea that *Clapper*'s harsh assessment of future harms in the standing inquiry should be applied wholesale in data-protection litigation. District courts followed suit, regularly relying on *Clapper* in discussing data-protection standing, and particularly when denying standing.

The data on this point bear emphasis. Of 209 standing decisions in data-protection litigation issued after *Clapper*, 103 (49.3%) cite *Clapper*. Of those 103 cases, sixty-six (64%) find the plaintiffs lack standing. In 2016, the peak year for *Clapper* citations, sixteen out of twenty-four (67%) decisions citing *Clapper* denied standing.[133] Regression analysis confirms the presence of a negative correlation between citation to *Clapper* and findings on standing.[134] The effect is much more pronounced in the district courts, with 69% of district court decisions citing *Clapper* finding plaintiffs lack standing, compared to only 37.5% of appellate decisions citing *Clapper*.[135]

---

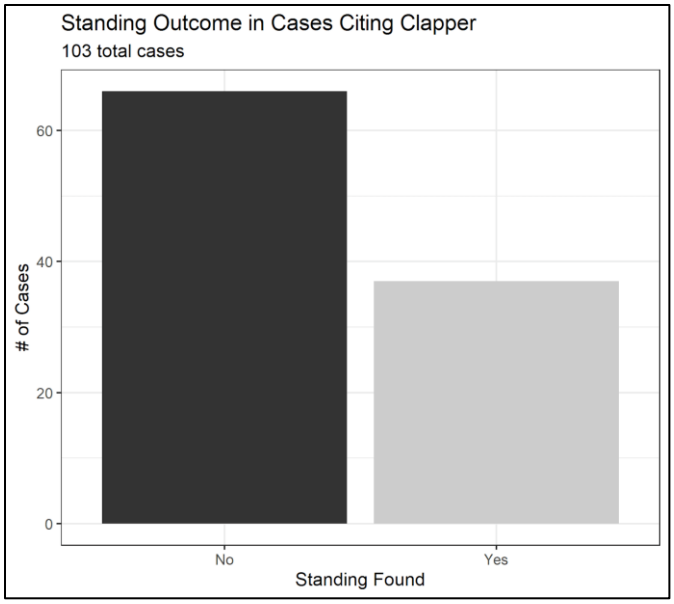
132. *See* Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); *In re* SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015). Only *Gubala* and *Reilly* do not discuss *Clapper*, and the latter by virtue of the fact that it predates *Clapper*. Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

133. 2015 proved to be the most challenging year for plaintiffs confronted with *Clapper*-citing courts: 82% of the seventeen decisions that year denied standing. By way of comparison, 86% of decisions not citing *Clapper* that year found standing.

134. When evaluated as the sole predictor of standing, citation to *Clapper* is significantly negatively correlated with standing ($p < .001$). When evaluated alongside a large group of other predictors (whether a case involves a data breach, standing formulation, and intermediate-category claim type), the negative correlation remains significant ($p < .001$).

135. Although appellate courts, like district courts, found standing less frequently when citing *Clapper*, the relationship is not statistically significant.

Figure 1:
Standing Outcome in Cases Citing *Clapper*



Many courts explicitly, but wrongly, contend that *Clapper* must be applied in data-protection cases. The Fourth Circuit in *Beck*, for example, declared that "*Clapper*'s discussion of when a threatened injury constitutes an Article III injury-in-fact is controlling here"[136]—but that is not correct. To the contrary, there is every reason to treat *Clapper* as at most persuasive in a data-protection case between private parties, given its unique context of a constitutional challenge to a statutory scheme enacted in the name of national security.[137] Courts have substantial leeway in determining what, exactly, constitutes binding precedent in a given case.[138] Recalling the purposes of standing doctrine illuminates the

136. *Beck*, 848 F.3d at 272.

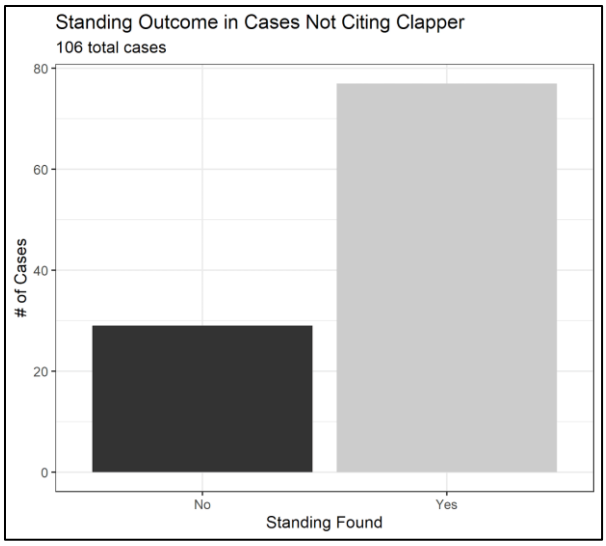
137. In one thorough examination of *Clapper*'s relevance, Judge Koh rejected the notion "that *Clapper* represents the sea change that [defendant] suggests." *In re* Adobe Sys., Inc. Priv. Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014). Judge Koh reached that conclusion by observing that "*Clapper* did not change the law governing Article III standing. The Supreme Court did not overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact, causation, and redressability. . . . Moreover, *Clapper*'s discussion of standing arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result." *Id.* at 1213–14 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013)).

138. *See* Oona A. Hathaway, *Path Dependence in the Law: The Course and Pattern of Legal*

problem. The Supreme Court's reasoning in *Clapper* proceeds from the separation-of-powers rationale for standing. That rationale has no application in data-protection cases like *Beck*. Only by ignoring that discrepancy or its import can a court proclaim that *Clapper* directly controls.

The data also show the existence of another path. The overall citation rate for *Clapper*, while high (49%), does not suggest that the courts uniformly believe it necessary to apply in data-protection cases. And just as citations to *Clapper* correlate with findings of no standing, of the 106 cases studied that do not cite *Clapper*, 72.6% find standing exists.[139] Simply put, nothing about *Clapper* requires federal courts to dismiss data-protection cases for lack of standing, but too often the courts have chosen the wrong path.[140]

Figure 2:
Standing Outcome in Cases Not Citing *Clapper*



Change in a Common Law System, 86 IOWA L. REV. 101, 123–24 (2001) ("What constitutes precedent in a particular case is a flexible concept that is subject to interpretation, especially when considering cases that are not directly on point. In practice, courts may interpret a prior decision in such a way that it does not appear to be controlling, even though a strong argument might be made that it is relevant and controlling precedent. Courts may also do the opposite, citing a preceding case as controlling or persuasive precedent when that case is arguably not relevant to the issue at hand. Furthermore, courts may intentionally emphasize some facts and deemphasize others to make a case appear controlling or not, depending on the desired result." (footnotes omitted)).

139. Here again, the appellate courts were more solicitous, finding standing in 87.5% of cases not citing *Clapper*, compared to only 70% of district court cases.

140. That said, the data give some reason to hope for improvement: citations to *Clapper* in data-protection cases have declined since 2016.

2. Failure to Consider the Purpose of Standing Doctrine

Another factor potentially leading to standing dismissals in data-protection litigation is the failure of courts to grapple with the appropriate justification for standing doctrine as they conduct the inquiry. In his concurrence in *Spokeo*, Justice Thomas acknowledged that the standing inquiry should be different depending on whether public or private rights are at issue in the case.[141] In particular, he recognized that the separation of powers is not implicated when plaintiffs allege a violation of private rights, and that in private-rights cases a plaintiff "need not allege actual harm beyond the invasion of that private right."[142] Data-protection lawsuits are private-rights actions and should typically survive standing challenges.

Nonetheless, the data suggest that federal courts are not employing this approach, which helps account for why only 55% of the cases studied survived challenges to standing. Analysis of how federal courts justify application of standing doctrine in these cases yields troubling results. By far the most common justification relied on by the courts in these decisions is mere invocation of Article III's reference to "Cases" or "Controversies."[143] That clause of Article III is the textual hook for standing doctrine's existence but provides no guidance about the purpose of the doctrine. Yet 118 of the 209 (56%) cases studied invoked "Cases" or "Controversies" as justification for standing doctrine's existence, without any further analysis or discussion of standing's purpose. Worse, the second-most common justification found in the cases was the absence of justification: in eighty-five cases (41%), the court merely stated and applied the three-part test for standing.

Courts are not, of course, required to recite the justification for every doctrine they apply. That said, it is striking that in 187 out of 209 (89%) cases studied, courts effectively declined to expressly engage with the justifications for a case-ending, constitutional doctrine as they applied it.[144] Equally striking, the justification with the most relevance to data-protection litigation—the necessity of adversarial presentation of the

---

141. Spokeo, Inc. v. Robins, __ U.S. __, 136 S. Ct. 1540, 1550–54 (2015) (Thomas, J., concurring) (analyzing the public/private rights distinction in standing doctrine).

142. *Id.* at 1553.

143. *See, e.g.*, *In re* LinkedIn User Priv. Litig., 932 F. Supp. 2d 1089, 1092 (N.D. Cal. 2013) ("An Article III federal court must ask whether a plaintiff has suffered sufficient injury to satisfy the 'case or controversy' requirement of Article III of the U.S. Constitution.").

144. Sixteen of the 118 cases citing "Cases" or "Controversies" as a justification for standing doctrine also discuss another justification and are thus excluded from this statement.

issues—appears in only four cases (1.9%).[145]

3. Inconsistent Treatment of Different Types of Claims

The data also reveal discrepancies in standing outcome depending on the types of claim asserted. Standing is, supposedly, a non-merits inquiry. The specific formulation of a plaintiff's claim is not a factor in the three-part test. Indeed, courts have developed a distinct doctrine of statutory standing that addresses whether a plaintiff with Article III standing nevertheless falls outside the zone of interest a statute is meant to address.[146]

Yet the data show a substantial difference in standing determinations based on the type of claim being asserted and the source of the injury in question. Claims involving data breaches offer a striking example. Of the 209 cases with definitive rulings on standing analyzed, ninety-four arose from a data breach. Courts found that these data breach plaintiffs had standing in only 47% of cases, compared to an overall standing rate of 61% in non-data-breach cases. This discrepancy is, unsurprisingly, magnified by the *Clapper* effect. Of the eighty data-breach decisions, seventy-two cite *Clapper*, and only 37.5% of those cases find standing.

145. Although such a small sample size is not statistically significant, it is interesting to note that courts found standing existed in three (75%) of these cases. All four of these decisions came from district courts. *See* Opperman v. Path, Inc., 87 F. Supp. 3d 1018, 1057 (N.D. Cal. 2014) (finding standing); Ruk v. Crown Asset Mgmt., LLC, No. 16-CV-3444-LMM, 2017 WL 3085282, at *1 (N.D. Ga. Mar. 22, 2017) (finding standing); Oneal v. First Tenn. Bank, No. 17-CV-3-SKL, 2018 WL 1352519, at *10 (E.D. Tenn. Mar. 15, 2018) (dismissing for lack of standing); Gordon v. Chipotle Mexican Grill, Inc., 344 F. Supp. 3d 1231, 1239 (D. Colo. 2018) (finding standing).

146. *See, e.g.*, Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 128 & n.4 (2014) (noting that the inquiry whether a plaintiff "falls within the class of plaintiffs whom Congress has authorized to sue" is sometimes called "statutory standing" and is "treated . . . as effectively jurisdictional").

Figure 3:
Cases Arising from Data Breaches

Similar discrepancies emerge when looking at the types of claims asserted. At a high level of generality, three categories of claims are most common in data-protection cases: state statutory (136 cases), common law (126 cases), and federal statutory (94 cases).[147] Even at this level of generality, there are stark differences. State statutory claims fared the worst—courts found standing in only 54% of cases asserting causes of action based on state statutes. The common law fared slightly better, with courts finding standing in 56% of cases asserting a common-law cause of action. Plaintiffs asserting claims based on federal statutes fared best, with courts finding standing in 63% of cases.[148]

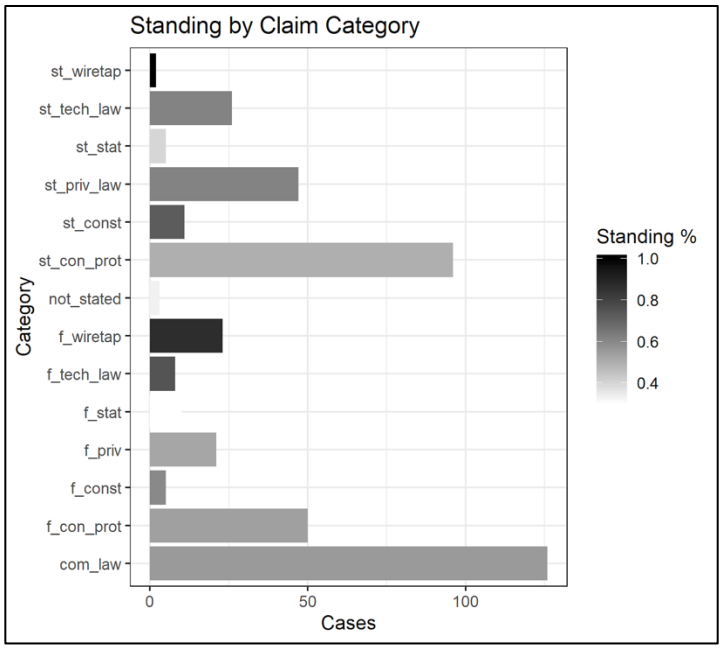
These high-level discrepancies can be explained to some extent by more granular examination of the claims asserted. For example, plaintiffs

147. Remaining high-level categories of claims were rarely asserted: state constitutional (eleven cases) and federal constitutional (five cases). In three cases, the nature of plaintiffs' claims was not apparent from the opinion.

148. Regression analysis confirms a positive correlation between presence of a federal statutory claim and a finding of standing ($p < .05$). No statistically significant correlation was found with respect to state statutory or common law claims.

asserting federal wiretap claims were very successful: courts found standing in 87% of cases asserting violations of the Wiretap Act or the Stored Communications Act.[149] But only two cases in the entire data set involved assertion of a state-law wiretap claim.[150]

Figure 4:
Standing by Claim Category



Plaintiffs suing under privacy statutes did not fare as well, further supporting the notion that judges are skeptical about privacy harms. Only 62% of cases involving claims under state privacy statutes were permitted to proceed, well ahead of the 52% of federal privacy claims in which courts found standing.

Of note, the most prevalent category of statutory claims was also the least successful: consumer protection. Just 50% of the ninety-six decisions involving state-law consumer protection claims found standing; for federal consumer protection claims, that number creeps up only to 54% in

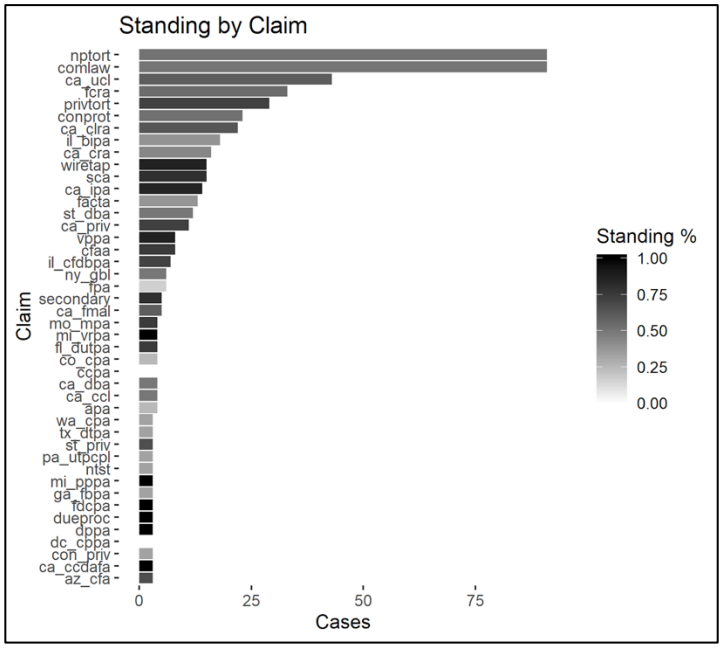
149. Here, too, regression analysis confirms a positive correlation between presence of a federal wiretap claim and a finding of standing ($p < .05$).

150. *See In re* Google Inc., No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sep. 26, 2013); Opperman v. Path, Inc., 87 F. Supp. 3d 1018 (N.D. Cal. 2014).

fifty cases.[151]

More detailed examination reveals interesting variation. The most common type of consumer protection claim—violation of California's Unfair Competition Law (UCL), an act with strict statutory standing requirements—fared relatively well: courts found standing existed in 60% of the forty-three cases asserting UCL claims.[152] The most common federal consumer protection claim—violation of the Fair Credit Reporting Act—was less successful, with courts finding standing in 55% of thirty-three cases. The biggest loser among federal consumer protection claims were claims under the Fair and Accurate Credit Transactions Act (FACTA)—only 38% of the thirteen cases asserting such claims survived a standing challenge.

Figure 5:
Standing by Claim



151. A negative correlation between presence of a state consumer-protection claim and finding of standing exists in the data ($p < .05$).

152. This level of success may be attributable at least in part due to the courts hearing the claims: thirty-five of the forty-three cases asserting UCL claims were heard in California's district courts, and one was heard in the Ninth Circuit.

Finally, three major types of common-law claims appear in the cases: privacy torts, non-privacy torts (typically negligence), and other claims (such as breach of contract). Privacy tort claims were both most successful and least-often asserted: 72% of the twenty-nine cases asserting privacy torts were permitted to go forward.[153] The other categories fell below the overall standing rate of 54% in all cases analyzed (52% for non-privacy torts and 51% for other common-law claims).

This empirical analysis supports many of the ideas advanced in Part I. Low standing rates in data breach cases suggest that federal courts are unduly skeptical of the risk of harm flowing from data breaches, particularly in the aftermath of *Clapper*. The courts' skepticism would also account for the relatively low rate of standing in non-privacy tort cases. Judicial skepticism about harm also appears to be borne out by the relatively low rates of standing in cases asserting statutory privacy and consumer protection claims. It is telling, for instance, that courts dismissed a large majority of FACTA claims for lack of standing. Among other things, FACTA instructs retailers not to print more than the last five digits of a person's credit or debit card number on a receipt.[154] For reasons passing understanding, many retailers appear to be in breach of that requirement.[155] Congress explicitly adjudged that printing more than the last five digits of a card number presented a risk to consumers, and enacted FACTA "with the intended purpose of helping to combat identity theft."[156] Yet most federal courts to confront the issue have substituted their own view of harm for Congress's, finding allegations of FACTA violations insufficiently "concrete" or "imminent" to support standing.[157]

Conversely, where plaintiffs sue under statutes, and particularly federal statutes, that more strongly imply culpable behavior by defendants, courts find standing more often—federal wiretap and Computer Fraud and Abuse Act (CFAA) claims stand as by far the most successful.[158] These types of framing differences should, in theory, have no impact on the standing analysis. That they do confirms judicial misapplication of the doctrine.

---

153. Privacy tort claims in non-data-breach cases were particularly successful, with a standing rate of 88%. In data-breach cases, privacy torts fared less well, but still better than data-breach cases not involving privacy tort claims (54% vs. 47%).

154. *See* 15 U.S.C. § 1681c(g)(1).

155. *See, e.g.*, Taylor v. Fred's, Inc., 285 F. Supp. 3d 1247, 1254 (N.D. Ala. 2018) ("[The plaintiff] . . . received a receipt that 'displayed the first six digits and the last four digits of [their] debit card.'").

156. *Id.* (quoting Wood v. J Choo USA, Inc., 201 F. Supp. 3d 1332, 1334 (S.D. Fla. 2016)).

157. *See id.* at 1258–71.

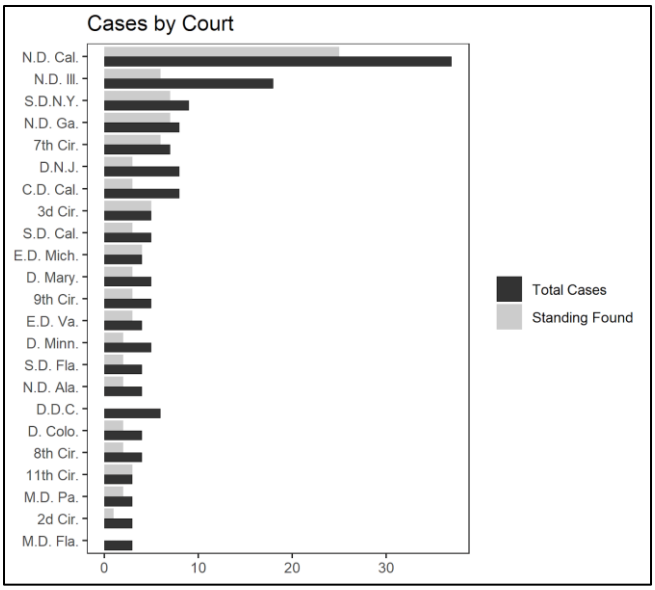
158. Only two of the cases analyzed asserted state law wiretap claims, but it is interesting to note that courts found standing in both.

4. Jurisdictional Variations

If uniform application of the law is a goal of the federal judicial system, data-protection cases show the courts falling well short. The data reveal substantial variation in approach and adjudication at the district level.

Given that data-protection cases typically involve technology companies and online services, it is unsurprising that the Northern District of California is the leading venue for data-protection cases, issuing thirty-seven decisions on standing in such cases since *Clapper*. The court has also proven reasonably plaintiff-friendly, finding standing in twenty-five of those thirty-seven cases (68%).[159] The second most frequent venue, the Northern District of Illinois, has been much less solicitous, finding standing in only six of eighteen cases (33%) analyzed. Reliance on *Clapper* is a significant point of distinction between these districts: the California court cited *Clapper* in only twelve of the thirty-seven (32%) data-protection cases analyzed, while the Illinois court cited it in eleven out of eighteen (61%).

Figure 6:
Cases by Court



159. The large number of cases in the Northern District of California yields the only two judges issuing five or more opinions on standing in data-protection cases. Judge Koh leads the way with nine decisions; in light of her thorough analysis of *Clapper* in *In re Adobe Systems*, it is no surprise that she found standing existed in eight (89%) of these cases. Judge Davila, by contrast, found standing in only two of seven (29%) of the cases he decided.

No other courts appear nearly so frequently in the data, but interesting trends emerge from the handful of repeat players. For example, among courts issuing five or more decisions on standing in data-protection cases since *Clapper*, most tend strongly in one direction or another on the question of standing. On the one end, in addition to the Northern District of California, both the Northern District of Georgia and Southern District of New York have been friendlier to plaintiffs, finding standing in seven of eight and nine cases, respectively, while the Seventh Circuit found standing in six of seven cases and the Third Circuit found standing in all five cases it decided. At the other end, the District of Columbia outdid the Northern District of Illinois, finding standing in none of the six cases it decided.[160] This tendency perhaps exemplifies the role of path dependence in individual courts.

C. Contributing Causes

The data show that a number of factors—*Clapper*, justification for standing, etc.—are directly correlated with federal courts dismissing data protection cases at the standing stage. In addition to the direct correlations found in the data, this Article demonstrates numerous potential contributing factors that find support in the data, case law, and other scholarship. Leading factors include path dependence, the policy preferences of judges, and simple ignorance.

1. Path Dependence

The above data analysis strongly suggests harmful path dependence is at work in data-protection cases. At its most basic level, path dependence is the notion that earlier decisions constrain future decisions.[161] Path dependence is a defining feature of a common-law system: previous decisions of the higher courts are binding on future decisions of the lower courts. Past decisions, even when not binding, are given persuasive effect in present cases. And stare decisis counsels that courts should stick to the path if reasonably possible.

The system has built-in drawbacks, among them that the first decisions on a given issue are disproportionately impactful and that it therefore

160. A handful of courts deciding five or more cases were more varied in determining standing: the Central District of California and the District of New Jersey (both, three of eight), the District of Minnesota (two of five), and the Southern District of California and the Ninth Circuit (both, three of five).

161. Hathaway, *supra* note 138, at 103–04 (defining path dependence as the idea that "an outcome or decision is shaped in specific and systematic ways by the historical path leading to it").

incentivizes races to the courthouse.[162] These issues may well be at play in the data-protection context. In data-protection litigation, some of those early choices raise serious concerns, effectively poisoning subsequent development in the doctrine. The direct and largely unquestioned adoption of *Clapper* in the data-protection context is a ready example. Another fascinating example is found in a line of cases in the Northern District of Illinois involving Illinois' Biometric Information Privacy Act (BIPA) that emerges from a troublingly non-adversarial context.

BIPA is a (for now) unique statute. As explained by the Illinois Supreme Court, BIPA

> imposes numerous restrictions on how private entities collect, retain, disclose and destroy biometric identifiers, including retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry, or biometric information. Under the Act, any person "aggrieved" by a violation of its provisions "shall have a right of action against an offending party" and "may recover for each violation" the greater of liquidated damages or actual damages, reasonable attorney fees and costs, and any other relief, including an injunction, that the court deems appropriate.[163]

In recent years, it has apparently become commonplace for employers to use fingerprinting systems for time-tracking: rather than clocking in and out with a punch card, ID, or the like, employees use their fingerprints. Many of these employers have not heeded BIPA's notice and disclosure requirements, leading to a wave of putative class-action lawsuits. Such lawsuits have led to a series of decisions from the Northern District of Illinois on standing, including, chronologically, the *McCollough v. Smarte Carte, Inc.*,[164] *Howe v. Speedway LLC*,[165] *Dixon v. Washington & Jane Smith Community—Beverly*,[166] *Goings v. UGN, Inc.*,[167] *Aguilar v. Rexnord LLC*,[168] *Johnson v. United Air Lines, Inc.*,[169] *Miller v. Southwestern Airlines Co.*,[170] *McGinnis v. United States Cold Storage,*

---

162. *Id.* at 105 (noting that "courts' early resolutions of legal issues can become locked-in and resistant to change" and that "the order in which cases arrive in the courts can significantly affect the specific legal doctrine that ultimately results").

163. Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, 129 N.E.3d 1197, 1199–200.

164. No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).

165. No. 17-cv-07303, 2018 WL 2445541 (N.D. Ill. May 31, 2018).

166. No. 17 C 8033, 2018 WL 2445292 (N.D. Ill. May 31, 2018).

167. No. 17-cv-9340, 2018 WL 2966970 (N.D. Ill. June 13, 2018).

168. No. 17 CV 9019, 2018 WL 3239715 (N.D. Ill. July 3, 2018).

169. No. 17 C 08858, 2018 WL 3636556 (N.D. Ill. July 31, 2018).

170. No. 18 C 86, 2018 WL 4030590 (N.D. Ill. Aug. 23, 2018).

Inc.,[171] and *Colon v. Dynacast, LLC* cases.[172]

Over the course of these nine cases, the judges of the Northern District reached a loose rule for whether these allegations support standing: where, as in *Dixon* and *Miller*, the plaintiffs alleged that the employers disclosed fingerprint scans to third parties (usually payroll vendors), the plaintiffs alleged a sufficiently concrete injury for Article III purposes. In the remaining cases, which featured no allegations of disclosure, the courts declined to find standing. One of the later cases in the line, *McGinnis*, neatly summarizes the point: "All other courts in this District that have considered whether a person suffers a concrete injury from the *known* collection and retention of a fingerprint, *without disclosure* to a third-party, have answered the question no."[173]

Whether this distinction is correct[174] is of secondary importance to how it was reached. At first blush, this is an ordinary series of cases in one district raising similar issues, with judges appropriately taking cues from each other's reasoning in rendering their decisions. But under the surface lies a crucial problem: nearly all these cases were decided in the absence of real argument by the parties.

The problem lies in the posture of the majority of these cases: *Howe*, *Dixon*, *Goings*, *Aguilar*, *Johnson*, *Miller*, and *Colon* were all originally filed in *state* court, then removed to federal court by defendants. In most of them, the defendants then sought a merits dismissal under Rule 12(b)(6) on the basis that the plaintiffs were not "aggrieved" by the violations of BIPA alleged—a statutory-standing argument that plainly implicates whether the plaintiffs had Article III standing. *Howe*, the first of these cases to confront the conundrum, summarized the issues as follows:

> Procedurally, Howe finds himself in an awkward position. To succeed in his lawsuit, he must establish that he is a "person aggrieved" who has statutory standing to assert a cause of action under BIPA. However, if he has a cognizable injury under BIPA, then it follows that he also has constitutional standing and must proceed in a disfavored forum. Therefore, in an effort to achieve

171. 382 F. Supp. 3d 813 (N.D. Ill. 2019).

172. No. 19-cv-4561, 2019 WL 5536834 (N.D. Ill. Oct. 17, 2019).

173. *McGinnis*, 382 F. Supp. 3d at 819 (first citing *Johnson*, 2018 WL 3636556; then citing *Aguilar*, 2018 WL 3239715; then citing *Goings*, 2018 WL 2966970; then citing *Howe*, 2018 WL 2445541; and then citing *McCollough*, 2016 WL 4077108).

174. Under the analysis in Part I, the presence or absence of disclosure to a third party appears to be a distinction without a difference. The statutory violation is complete without such disclosure, and the courts' reasoning as to why this "bare procedural violation" does not suffice is premised on, and suffers the same defects as, the Seventh Circuit's decision in *Gubala*.

> remand without fatally undermining his claims, Howe declines to take a position on constitutional standing and argues that it is Defendants' burden to establish such standing. . . . To avoid remand, Defendants find themselves having to establish that Howe has suffered a sufficient injury for purposes of Article III standing even as their motion to dismiss vigorously contests the adequacy of his injury for purposes of statutory standing.[175]

In other words, this posture is a disaster, particularly for a determination of standing. As discussed above, the most powerful justification for the doctrine's application in data-protection litigation is to ensure the existence of an adversarial context in which all pertinent issues of fact and law can be brought before the court. Yet even without that vital clash of argument, the judges of the Northern District were compelled to rule on standing, because standing is a jurisdictional prerequisite and a federal court must always ensure it has jurisdiction, even if it requires raising issues of subject-matter jurisdiction on its own motion and resolving them with or without assistance from the parties.[176]

Even assuming the most impartial and thorough approach by these judges, they reached decisions in these cases in exactly the manner the common-law judicial system and the doctrine of standing are meant to avoid. Worse, the problem is compounding. *Howe* and *Dixon* were decided on the same day.[177] *Goings* came next and relied on *Howe* and *Dixon* in assessing standing.[178] *Aguilar*, in turn, relied on all three,[179] then *Johnson* incorporated *Aguilar*, and so on.[180] This is an example of what Hathaway calls "increasing returns path dependence," in which "once a court makes an initial decision, it is less costly to continue down that same

---

175. *Howe*, 2018 WL 2445541, at *3–4.

176. *See, e.g.*, *Dixon*, 2018 WL 2445292, at *4 (noting that the court has an "independent obligation to ensure that it has subject matter jurisdiction").

177. *Howe* and *Dixon* were each decided on May 31, 2018. *Howe* dismissed the action for lack of standing despite noting that "[d]efendants undoubtedly violated BIPA if they failed to provide Howe disclosures and obtain his written authorization prior to collecting and storing his fingerprints and did not create or make publicly available a biometric data retention and destruction policy." *Howe*, 2018 WL 2445541, at *7. *Dixon*, on the other hand, declined to dismiss on standing grounds. *Dixon*, 2018 WL 2445292, at *10.

178. *Goings*, 2018 WL 2966970, at *2 (citing the foregoing in stating that "[t]his case joins the growing ranks of BIPA actions filed in this district and elsewhere in which courts have adjudicated the sufficiency of the complaint against challenges brought under Rules 12(b)(1) and/or 12(b)(6)").

179. Aguilar v. Rexnord LLC, No. 17 CV 9019, 2018 WL 3239715, *3 (N.D. Ill. July 3, 2018) (agreeing with the analysis in the foregoing in assessing "the question [of standing] in the context of an employer's biometric clocking system").

180. Johnson v. United Air Lines, Inc., No. 17 C 08858, 2018 WL 3636556, *3 (N.D. Ill. July 31, 2018) (citing the foregoing in support of holding that the plaintiff lacked standing).

path than it is to change to a different path."[181]

The ultimate negative impact of following this tainted path can be seen in *Rivera v. Google, Inc.*,[182] another BIPA case decided in the Northern District of Illinois. Unlike the line of cases discussed above, *Rivera* did not involve forced use of fingerprinting systems by employees. Rather, it challenged a "feature" of Google Photos: Google created "face-geometry" scans of individuals tagged in photos uploaded to the Google Photos service, then used the scans to identify and tag those individuals in other photos.[183] This practice, in addition to being alarming, violated BIPA due to Google's failure to provide notice of, or obtain consent to, the practice. Yet the district court dismissed the action for lack of standing.[184] The court's reasoning included reliance on the third-party disclosure distinction elucidated in the employee fingerprinting cases, expressly relying on the non-adversarial decisions in *Howe*, *Miller*, and *Dixon*.[185]

This is a frightening example of path dependence gone awry. Path dependence is only a desirable feature of the common-law system as long as there can be confidence that the decisions against which future cases will be judged are reached fairly. Such confidence is lacking when judges are at sea in reaching their decisions, in cases in which neither party wishes to articulate a position.[186]

Nor is the problem likely to stop at the Illinois border. Numerous state legislatures are considering biometric privacy laws like BIPA.[187] To the

---

181. Hathaway, *supra* note 138, at 106–07.

182. 366 F. Supp. 3d 998 (N.D. Ill. 2018).

183. *Id.* at 1001.

184. *Id.* at 1014.

185. *Id.* at 1008–09.

186. Indeed, in *McGinnis*, the district court essentially forced the defendant to move under Rule 12(b)(1) instead of 12(b)(6). The defendant "originally stated that it was going to file a motion to dismiss the complaint for lack of standing," but then "purported to concede the standing issue and filed a motion to dismiss [the case] as time-barred." Order at 1, McGinnis v. U.S. Cold Storage, Inc., 382 F. Supp. 3d 813 (N.D. Ill. 2019) (No. 17 C 08054), ECF No. 24. The court, noting its "independent obligation to ensure that it has subject matter jurisdiction over a case before deciding the merits," ordered defendant to "file a position paper that either argues that McGinnis has adequately alleged Article III standing or expressly concedes the issue . . . . If [defendant] concedes standing, then McGinnis shall file a position paper that argues in support of standing . . . ." *Id.* at 1–2. Only after this express order did the defendant move to dismiss for lack of subject-matter jurisdiction. Incredibly, after the plaintiff refiled his suit in Illinois state court, the defendant sought to remove the case to federal court based on diversity of citizenship, swapping positions on standing in the second round. The case was again dismissed for lack of standing. *See* McGinnis v. U.S. Cold Storage, Inc., No. 19 C 00845, 2019 WL 7049921 (N.D. Ill. Dec. 23, 2019).

187. *See* Eric J. Shinabarger & Alessandra V. Swanson, *Several States Considering Laws Regulating the Collection of Biometric Data*, WINSTON & STRAWN LLP PRIV. & DATA SEC. L. BLOG (Feb. 6, 2019), https://www.winston.com/en/privacy-law-corner/several-states-considering-laws-

extent that such laws resemble BIPA,[188] it will be natural for litigants to point to the Northern District of Illinois decisions construing BIPA, and for other judges to accord some respect to those decisions.[189] This poisoned precedent could thereby hinder application of these new laws.[190]

2. Policy Preferences

Analysis of the case law suggests that standing dismissals in data-protection litigation are driven by a range of judicial policy preferences, ranging from substantive skepticism about privacy to concerns about docket management.

a. Skepticism About Privacy

Many standing decisions betray judges' skepticism about privacy harms, ranging from failure of imagination to outright hostility.[191] Judicial skepticism about privacy may have sociological and psychological roots. Lior Strahilevitz notes that some 20% of the population are "privacy unconcerned"; that is, they are individuals "not valuing their own privacy and having a difficult time understanding why anyone would care about privacy . . . ."[192] He further notes that extroverts—who are more likely to be privacy unconcerned—play an outsize role in public life, including in policymaking and serving as leaders in business and government.[193] Some Article III judges, each of whom must go through an extensive and public

---

regulating-the-collection-of-biometric-data.html [https://perma.cc/5T8V-WHUA].

188. And it is likely that they will. *See, e.g.*, *id.* (noting, for example, that proposed New York law is "substantially similar to BIPA").

189. Fortunately, the Ninth Circuit has reached the opposite conclusion of *Rivera*, affirming the presence of standing in a nearly identical lawsuit against Facebook. *See* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, __ U.S. __, 140 S. Ct. 937 (2020).

190. To end this analysis on an appropriately Kafkaesque note, *Rivera* distinguished a previous Northern District of Illinois finding standing arising from collection of face scans in violation of BIPA. One of the bases of the distinction: "it also does not appear that the parties precisely teed up this issue for the district court in that case, as the defendant did not challenge the plaintiff's standing." Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1014 n.19 (N.D. Ill. 2018).

191. The Supreme Court itself indulged in such skepticism in *Spokeo, Inc. v. Robins*, with Justice Alito opining that "[i]t is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm." __ U.S. __, 136 S. Ct. 1540, 1550 (2016). As Wu notes, this type of speculation usurps the function of the legislature, which determined the practice to be sufficiently harmful to be worth banning. *See* Wu, *supra* note 15, at 459.

192. Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2026 (2013).

193. *Id.* ("If the privacy unconcerned are indeed more disposed to participate heavily in the political process, with privacy fundamentalists tending to remain on the sidelines in political debates, the smaller group's voice in policy debates may be just as loud or even louder than the larger cohort's.").

vetting process, may be among that group that places less value on privacy. When confronted with the opportunity to evaluate the risk of harm, they might be expected to express skepticism about privacy harms, particularly those in cases of improper data collection or retention.

Concerns about psychology-based skepticism arise from the psychological concept of "motivated reasoning": a tendency to view more skeptically claims that run counter to one's own views and experiences.[194] The tendency toward skepticism is "frequently unconscious, not conscious."[195] And it may offer at least a partial explanation of, for example, *Gubala*, in which Judge Posner—a very public figure in his decades on the bench—opined that a plaintiff whose personal information has been retained by a private company in direct violation of federal law for over a decade has nevertheless suffered no harm.[196]

It is possible, too, that judges in data-protection litigation are motivated by conscious, substantive views. This phenomenon is readily observable in cases with a substantially political character; many are the Supreme Court cases whose outcome can be predicted as five to four decisions on conservative-liberal lines.[197] It may also account for the skepticism expressed by many judges when evaluating the likelihood that a particular data-protection violation may lead to harm. Take, for example, numerous cases in which judges do not heed the requirement to construe allegations in the light most favorable to the non-movant in evaluating studies of harm following data breaches, and take the curious position that there is no standing even though a substantial percentage of the proposed class *will* suffer identity theft, turning the notion of expected value on its head.[198]

---

194. Fallon, *supra* note 13, at 1098 (describing motivated reasoning as the tendency for "most of us . . . to look skeptically on factual assertions as well as arguments that contradict our prior, ideologically suffused set of beliefs").

195. *Id.*

196. *See* Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017). Nichol presents a similar argument, contending that "[a]s elite judges summarily determine which interests are worthy of legal cognizance, they unsurprisingly embrace concerns that strike closest to home, sustaining 'harms' that mirror the experiences and predilections of their own lives." Nichol, *supra* note 13, at 304. In a similar vein, Matthew Tokson notes that "courts' examination of knowledge tends to be broad and abstract rather than particular," and that, "[i]n the Fourth Amendment context, courts do this by reaching a conclusion about the collective knowledge possessed by society and then imputing that knowledge to the person at issue." Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 150 (2016).

197. *See, e.g.*, Fallon, *supra* note 13, at 1095–96 ("[T]he Justices' substantive constitutional views inevitably drive standing decisions in a number of important areas. Abundant examples confirm this thesis.").

198. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 275–76 (4th Cir. 2017) ("Even if we credit the Plaintiffs' allegation that 33% of those affected by Dorn VAMC data breaches will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm."); *In re* SuperValu,

These judges appear to hold the view that privacy harms are not real harms, and rule accordingly.

b. Pro-Business/Anti-Consumer Bias

Two broad, related trends likely exacerbate problems in data-protection litigation. First, "[i]n the past fifteen years, plaintiffs are losing, and business defendants are winning, a huge majority of Federal Rules private enforcement cases . . . ."[199] Second, courts have been increasingly hostile to class actions.[200] Almost all data-protection lawsuits in federal court fall into those buckets. Few are the data breaches affecting, or the data-gathering schemes targeting, only a handful of individuals. And standing, although not literally a Federal Rules issue, is a similar type of procedural inquiry. The frequently successful challenges to standing in data-protection litigation—especially the low standing rates in consumer protection cases—are less surprising when considered in light of these trends.

Both these broad trends and the specific context of data-protection litigation exemplify the concern that standing doctrine works to favor those with power and privilege.[201] While a full accounting of the factors underlying that tendency is beyond the scope of this Article, troubling parallels to retrenchment in private enforcement actions exist. For example, one study notes a substantial increase in amicus filings by pro-business and conservative groups in the Supreme Court's class-action cases since 1994, particularly noting increased activity from the Chamber of Commerce, the Pacific Legal Foundation, the Washington Legal Foundation, and the Defense Research Institute.[202] Each of those groups filed amicus briefs in *Spokeo*, as did numerous businesses and credit

---

Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586, 2018 WL 1189327, at *8 (D. Minn. Mar. 7, 2018) (evaluating report stating that approximately 40% of individuals "whose card numbers were compromised in 2013 became fraud victims" and concluding that "this report establishes that the majority of consumers whose payment cards are compromised in a breach will not become fraud victims as a result of the breach").

199. Stephen B. Burbank & Sean Farhang, *Class Actions and the Counterrevolution Against Federal Litigation*, 165 U. PA. L. REV. 1495, 1518 (2017).

200. *See, e.g.*, *id.* at 1518–21 (finding that pro-class action outcomes at the Supreme Court have substantially declined since the late 1980s).

201. Nichol, *supra* note 13, at 304. Nichol argues that the standing doctrine "systematically favors the powerful over the powerless. The malleable, value-laden injury determination has operated to give greater credence to interests of privilege than to outsider claims of disadvantage." *Id.*

202. *See* Burbank & Farhang, *supra* note 199, at 1525 (analyzing impact of increase in amicus filings on Supreme Court class-action jurisprudence).

bureaus.[203] In the legislative sphere, technology companies have lobbied against developing privacy laws.[204] Increased responsiveness of courts and legislators to these special interests helps explain low standing rates in data-protection litigation and the absence of legislative action to combat judicial hostility to data-protection claims.

c. Docket Management

The Seventh Circuit may have said the quiet part out loud: "The standing rule reduces the workload of the federal judiciary . . . ."[205] While literally true, that is neither an accepted nor acceptable justification for standing doctrine.[206] The existence of a "Case" or "Controversy" does not depend on how pleased the court will be to hear it. Article III does not give the judiciary the ability to set its caseload. And a dispute will be no less adversarial between the parties if it is the tenth hearing on a court's calendar rather than the first. Indeed, around the time that the Supreme Court threw standing jurisprudence for a loop in *Clapper*, it admonished that federal courts are obligated to hear cases falling within their jurisdiction.[207]

Yet the appeal of the standing dismissal to the federal judge is impossible to ignore. The massive and increasing caseload in the federal courts is well known. In the data-protection context, cases typically promise to be long and involved. Most arise from large-scale data breaches or inappropriate, indiscriminate data collection. As such, they are usually brought as class actions and implicate complex technical issues. One can certainly understand why overworked judges might be eager to get such cases off their dockets.

With that in mind, dismissal for lack of standing has a special appeal over other means of dispensing with a case: it is a non-merits dismissal. Even if erroneous or improperly motivated, a dismissal for lack of standing works relatively little injustice, as its effect is only to banish the

---

203. *See* Spokeo, Inc. v. Robins, Supreme Court Docket No. 13-1339, SUP. CT. OF THE U.S., https://www.supremecourt.gov/search.aspx?filename=/docketfiles/13-1339.htm [https://perma.cc/2FF2-YUMD].

204. *See, e.g.*, Issie Lapowsky, *Tech Lobbyists Push to Defang California's Landmark Privacy Law*, WIRED (Apr. 29, 2019, 3:09 PM), https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/ [https://perma.cc/Q4WL-9PYW] (discussing lobbying efforts to undermine the California Consumer Privacy Act).

205. Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 912 (7th Cir. 2017).

206. Wu characterizes the *Gubala* court's reliance on a "fear of being 'flooded'" with litigation as "a quintessentially legislative" determination. *See* Wu, *supra* note 15, at 458.

207. *See* Lexmark Int'l v. Static Control Components, Inc., 572 U.S. 118, 126 (2014) ("[A] federal court's obligation to hear and decide cases within its jurisdiction is virtually unflagging." (internal quotation marks omitted)).

suit to state court. Moreover, as the data show, state-law and common-law claims predominate in data-protection litigation—the majority of cases analyzed involved such claims, while fewer than half of cases asserted claims under federal law. Allowing state courts to deal with state-law claims is a hallmark feature of the federal system, CAFA notwithstanding.

The Northern District of Illinois' BIPA series of cases may proceed from this impulse. Most were brought initially in state court, then removed to federal court by defendants who seemed intent on challenging plaintiffs' right to bring suit at all. Confronted with the prospect of overseeing a lengthy, complicated class-action lawsuit brought by plaintiffs who did not want to be in federal court in the first place against defendants who appeared to be engaging in gamesmanship, the judges of the Northern District of Illinois may well have viewed dismissal for lack of standing as the best of all possible worlds.

The data are potentially consistent with this explanation. In particular, appellate courts have been significantly more solicitous of plaintiffs in data-protection cases, finding standing in 75% of cases, compared to only 51% of district courts. In data-breach cases, which likely present both the most technically complicated inquiries and the most diffuse harms, appellate courts upheld standing in 79% of cases, compared to a mere 41% of district court cases.

Figure 7:
Standing Outcome at District Court

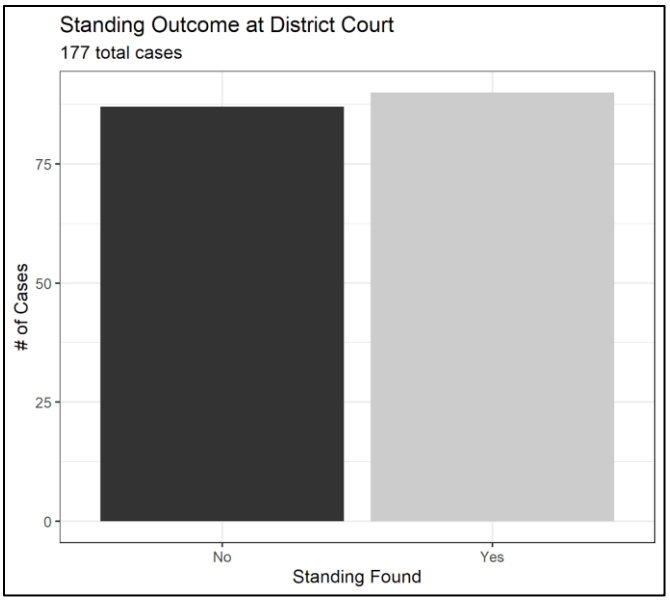
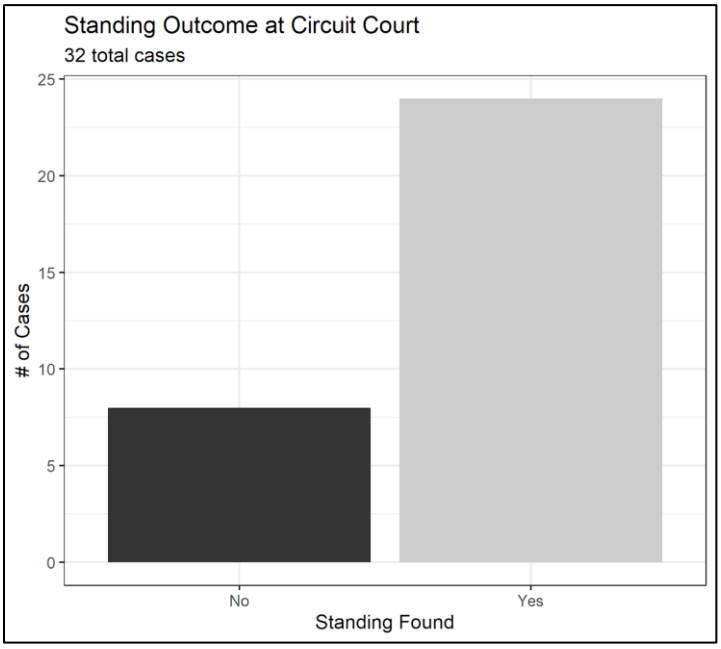


Figure 8:
Standing Outcome at Circuit Court



3. Ignorance

Perhaps more innocent, but equally troubling, is the prospect that federal judges believe there is no substantial risk of harm in data-protection cases because they do not understand issues like aggregation of information from multiple sources and non-monetary harm flowing from privacy violations.

That district court judges, and quite possibly plaintiffs' lawyers, do not understand the problem posed by aggregation is revealed by how little treatment the subject receives in the case law. And those few cases that *do* engage with the idea inspire little confidence. For example, in *Cooper v. Slice Technologies, Inc.*,[208] the plaintiffs brought a proposed class action against Slice, which operated a service called UnrollMe. UnrollMe purported to serve its users by accessing a user's email account, scanning it for spam messages, and unsubscribing users from further such messages.[209] The seasoned observer of privacy practices will not be

208. No. 17-CV-7102, 2018 WL 2727888 (S.D.N.Y. June 6, 2018).

209. *Id.* at *1.

surprised to learn that UnrollMe's actual business model was to scan the email accounts to which it was given access and then sell "anonymized" data gleaned therefrom to third parties, thereby enabling more and different spam to be sent to its customers.[210]

In alleging the harmful nature of this practice, the plaintiffs argued that research has shown that purportedly anonymized information can be trivially de-anonymized.[211] Plaintiffs emphasized that the types of messages UnrollMe harvested included Lyft ride receipts, which are even more susceptible to de-anonymization than many other types of emails as they include start points, destinations, ride times, unique customer identifiers, and other information.[212] But the district court tried to cleave these allegations into two distinct types of harm: "selling non-anonymized data," which the court found to be "the most concrete harm," and "that UnrollMe sold anonymized emails, but in such a way that the buyers could potentially 'deanonymize' the data and uncover personal information."[213] The court interpreted plaintiffs' allegations under the first point to be that UnrollMe sold "the user's email address," and found them insufficient because it was not necessarily the case "that the email address was included in the anonymized dataset that UnrollMe sold."[214] As to de-anonymization, the court pared down the complaint to allegations

> (1) that "[r]esearchers have revealed the ease [with] which particular people can be identified from purportedly anonymized data sources," particularly for taxi trips, and (2) that Uber, one of UnrollMe's clients, has a less-than-sterling reputation for snooping on customers. But the mere possibility that someone might deanonymize Plaintiffs' emails is not enough to constitute injury in fact.[215]

This crabbed reading of the complaint betrays, at best, a misunderstanding of the import of aggregation in data protection. The plaintiffs' concern is not, as the court supposed, that Uber might be able to divine the email address of a customer from the data sold to it by UnrollMe. Rather, the gist of plaintiffs' allegations is in fact that the types of emails UnrollMe harvested and sold to third parties include types of information that make it very easy to identify individuals, even if their names or email addresses are redacted. In particular, a third party might

---

210. *Id.*

211. Complaint at 12, *Cooper*, 2018 WL 2727888 (No. 17-CV-7102).

212. *Id.* at 13.

213. *Cooper*, 2018 WL 2727888, at *2.

214. *Id.*

215. *Id.*

easily glean details about individuals from their Lyft rides, such as home and work locations, schedules, and so forth. That information could, in turn, subject an individual to great harm.[216]

Whether a federal court would view even that larger risk of harm as sufficient to confer standing is, unfortunately, not clear. But at the very least, greater understanding of the risks in play in data-protection litigation should lead to better outcomes.

Ignorance of the harms in data-protection litigation may also arise from common fallacies. Ignacio Cofone and Adriana Robertson, for instance, have studied the impact of the cognitive bias known as "non-belief in the law of large numbers" (NBLLN) on privacy.[217] This bias describes the fact that afflicted individuals underestimate how informative each marginal item of information disclosed will be.[218] While Cofone and Robertson focus on explaining the "privacy paradox,"[219] this bias would also influence a judge's assessment of risk in a data-protection case.[220] Taking *Cooper* again as an example, the court's opinion certainly admits of the possibility that it does not realize how much information can accurately be deduced from Lyft ride data.[221]

Thorough analysis of the federal courts' decisions in data-protection

---

216. *See, e.g.*, Ohm, *supra* note 104, at 1705 ("Accretive reidentification makes all of our secrets fundamentally easier to discover and reveal. Our enemies will find it easier to connect us to facts that they can use to blackmail, harass, defame, frame, or discriminate against us. Powerful reidentification will draw every one of us closer to what I call our personal 'databases of ruin.'").

217. Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471 (2018) (arguing in favor of regulation of consumer data based on cognitive biases).

218. *Id.* at 1489–90 (noting that "the average person is not particularly good at estimating the informativeness of each piece of newly arriving information," and "if she suffers from NBLLN, she will underestimate *how much*" that piece of information discloses (emphasis in original)); *see also id.* (noting that an individual "might mistakenly believe that [a third-party's] belief about their personal information does not change much when they provide the [third-party] with new information that is, in fact, still informative").

219. As they put it, "[t]his paradox can be summarized by the following question: why is it that individuals consistently indicate that they value privacy, while simultaneously giving their privacy away for almost nothing?" *Id.* at 1476.

220. Relatedly, Nash notes that courts assessing probabilistic injuries may fundamentally misunderstand the analysis: "Some judges do not see that a small risk of a significant harm is the same as a certain loss of a harm of a smaller magnitude, and . . . that since the latter is a sufficient basis for standing so too should be the former." Nash, *supra* note 15, at 1310.

221. As another example, in *Antman v. Uber Technologies, Inc.*, the district court found substantial risk of harm did not exist despite allegations that defendant had lost information about the plaintiff including his "name, driver's license information, and his bank account and routing number," on the basis that this was not enough information to plausibly enable fraud or identity theft. No. 15-cv-01175-LB, 2018 WL 2151231, at *10 (N.D. Cal. May 10, 2018). No attention was given to the possibility that this information might trivially be tied to other information available about plaintiff or the possibility of harms beyond fraud and identity theft.

litigation reveals numerous flaws and inconsistencies in handling the standing inquiry. The data support various plausible explanations for these errors and may point the way toward appropriate corrective measures.

III. CORRECTING COURSE

In previous Parts, this Article showed that federal courts systematically err in assessing standing in data-protection litigation. By analyzing hundreds of these cases, this Article identified numerous factors contributing to these errors, from choices about precedent to ignorance about key factual issues. It now turns to normative points.

Increasing liability for data gatherers and brokers who violate law is desirable. Among other things, putting these entities on the hook for gathering and losing information will incentivize stronger protection while deterring overcollection. To get there, courts will have to administer the standing inquiry differently in data-protection litigation than they have to date.

This Part begins by suggesting methods to increase the percentage of data-protection cases that survive standing challenges, including reframing the standing inquiry and the potential effects of legislative action. It then discusses the implications of allowing more cases to go forward, including realigning data gatherers' incentives and advancing development of federal law. Theoretically, it contributes to the growing literature of data protection that argues for stronger protection of private information at the design and enforcement stages.

A. Reframing the Standing Inquiry

If the pathology of problems with standing doctrine in data-protection litigation can be traced to a single source, the leading candidate appears to be failure to grapple with the purpose of standing doctrine in assessing whether standing exists in a particular case. Examining the allegations in any given data-protection lawsuit from those principles will rarely support any Article III-based objection to jurisdiction, no matter how skeptical any given judge might be about privacy harms. Conversely, when analysis is unmoored from its purpose, courts, for the reasons discussed above, reach results that conflict with the purposes of Article III. The data suggest that courts are indeed at sea in most cases when assessing standing, as they typically resort to rote application of the three-part test with no discussion of its purpose. Returning to the adversity-based justification for standing as the foundation of standing analysis in data-protection litigation would lead to more consistent, coherent, and

salutary outcomes.[222]

To do so would require express recognition by the federal courts that standing must be evaluated differently in different cases. The courts have done so implicitly in their approach to other types of cases, such as those implicating the Establishment Clause.[223] Explicitly acknowledging that the doctrine applies differently in different types of cases would enable more thoughtful examination of the issues.[224]

Reframing the harms in data-protection litigation may also lead to improved outcomes. Approaching lawsuits solely from the standpoint of substantive rights and harms invites exactly the type of judicial skepticism against which this Article argues. By contrast, viewing data harms as violations of private procedural rights could simplify the inquiry around standing. In *Lujan*, for example, the Supreme Court noted that procedural rights are unique: "The person who has been accorded a procedural right to protect his concrete interests can assert that right without meeting all the normal standards for redressability and immediacy."[225]

Data protection is a perfect candidate for this kind of treatment. Construing data protection as a private procedural right would give force to statutory and common-law restrictions on gathering, using, and selling data that are too often disregarded by courts today but are intended to protect individuals' concrete, substantive interests in avoiding identity theft or exposure of private information. In the data-breach context, similar rights should be considered implied in the relationship between individual and data holder. It is hard to imagine that an individual would willingly agree to turn over their private information to an entity that had no intention to protect it. By implying a right to have data holders use reasonable care in protecting information they have acquired, the reasonable expectations of individuals and their ability to obtain redress for violations of those expectations are advanced.[226]

---

222. A corollary suggestion would be to move away from analyzing standing in any given case with reference to *Clapper* and instead focus on precedent in a closer context than that presented in *Clapper*.

223. *See, e.g.*, Fallon, *supra* note 13, at 1071–75 (analyzing the Supreme Court's Establishment Clause standing jurisprudence).

224. *See, e.g.*, *id.* at 1107–08 ("[The Supreme Court] ought to recognize that what counts as an injury depends on the provision under which a plaintiff brings suit. This modest, clarifying recognition would bring increased transparency to divisions about standing. Moreover, it should provoke no embarrassment, either to the Court institutionally or to any of the Justices individually.").

225. Lujan v. Defs. of Wildlife, 504 U.S. 555, 572 n.7 (1992).

226. The Ninth Circuit took an important step down this path in its decision on remand in *Spokeo* by agreeing with the Second Circuit that *Spokeo* stands for the proposition "that an alleged procedural violation [of a statute] can by itself manifest concrete injury where Congress conferred the procedural right to protect a plaintiff's concrete interests and where the procedural violation presents a risk of

Relatedly, passage of a federal data-privacy law could turn the tide. This Article's data show federal courts are more likely to find standing in cases asserting violations of federal statutes.[227] While the specific authorization for a cause of action should not matter in conducting the standing inquiry, better to use this systemic error to improve outcomes than to ignore its existence. Such a law could make explicit requirements for reasonable care in protecting information. Even purely technical violations of the law would likely suffice for standing under the analysis set forth in the Ninth Circuit's second *Spokeo* decision.

B. Implications of Increasing Liability for Data Gatherers

Holding data gatherers to account for their wrongdoing should benefit those who are wronged, realign data-gathering incentives to be more socially beneficial, and contribute to development of federal law on data protection.

Intuitively, the more data-protection cases that survive challenges to standing, the more frequently data gatherers will be held liable or pressed to settle in the wake of their wrongdoing. That intuition finds support in the literature. A study of litigation following data breaches from 2000–2010 shows substantially higher settlement rates in cases where plaintiffs allege actual harm, using a narrow definition of "actual harm" that tracks closely with the analysis in Part I concerning federal courts' overemphasis on PII.[228] The study found that "plaintiff allegations of financial harm are correlated with a 30% increase in the probability of settlement . . . ."[229]

By reframing what constitutes actual harm, both at the standing stage and into the merits, more cases should result in settlement rather than dismissal. Thus, more frequent findings of standing in data-protection litigation will lead to more frequent redress for individuals who suffer privacy harms. Even recognizing that significant merits challenges remain in data-protection litigation once standing is established, as more cases go

---

real harm to that concrete interest." Robins v. Spokeo, Inc., 867 F.3d 1108, 1113 (9th Cir. 2017) (internal quotation marks omitted).

227. *See supra* section II.A.3.

228. Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 95–96 (2014). They define "actual harm" for purposes of analysis as where "the plaintiff's complaint alleges an actual loss due to the breach (e.g., if the plaintiff alleges fraudulent charges on a credit card, stolen money from a checking or savings account, or other such costs incurred from criminal activity)." *Id.* "Other forms of alleged harm such as preventive costs from credit monitoring, emotional distress, invasion of privacy, or embarrassment" are not considered actual harm. *Id.*

229. *Id.* at 98.

forward, more successes (or good settlements) will follow.

Increasing liability for data holders would also lead to two related benefits: increased incentive to protect data and decreased incentive to gather or hold it. The current balance in litigation does not adequately incentivize businesses to protect the data they are holding, since they stand a good chance of escaping liability in the event of a breach. In fact, they are incentivized to extract every bit of data they can, even if to do so violates law, because they know they likely will not be held to account. Indeed, at least one study has found that technology companies are not concerned about privacy, instead focusing their resources in other areas.[230] Shifting the balance toward liability should deter marginal collectors and spur those for whom data brokerage remains viable to expend more resources on security.[231] It may also help to arrest privacy law's slide toward legal endogeneity by making it less feasible for businesses to hide behind showy compliance mechanisms that have no real force.[232]

Allowing more cases to go forward should also at least clarify the merits challenges in data-protection cases. For example, the causation conundrum identified by some courts in the standing context—whether to wait until identity theft actually occurs to sue, at the risk of defendants arguing that another intervening data breach is the cause—foreshadows a merits issue that can be expected to arise in most data breach cases. The fact that approximately half of all data-protection cases—and more than half of data-breach cases—filed in federal court are being thrown out before reaching the merits substantially slows the development of case law addressing these critical issues.

Additionally, more merits cases may help to rescue privacy law from being overtaken by consumer contract law. Omri Ben-Shahar and Lior Strahilevitz, among others, have noted the significant role played by contractual relationships in privacy suits.[233] While many data-protection

---

230. *See* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659, 685–86 (2018) ("Engineers working at start-ups 'didn't really think about privacy.' Nor did the executives, for that matter. Larger companies that say they take privacy seriously had a different problem: prioritization. Privacy was simply not a top priority for engineers because it was crowded out by other mandates." (footnote omitted)).

231. A robust federal data-protection law would arguably do better in achieving these goals. But the dream of such a law is no reason to delay correctives in the judiciary.

232. *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 778 (2020) ("As more technology companies paint creative pictures of their legal compliance, lawyers and judges become more likely to defer to the toothless structures companies create by either accepting them as evidence of substantive adherence to the law or actually incorporating them into statutes, thereby undermining the capacity for law to achieve more robust privacy protections for users." (footnote omitted)).

233. *See, e.g.*, Omri Ben-Shahar & Lior Jacob Strahilevitz, *Contracting Over Privacy:*

cases play out in the shadow of terms of service, myriad cases arise in the absence of any such relationship.[234] Permitting more of these cases to go forward should lead to increased development of privacy law at the federal level.

One concern, of course, is that allowing more cases to clear the standing bar would increase the workload of the federal bench. However, the feared flood of litigation may not come to pass. One cannot lose what one does not gather, and one cannot be sued for what one has not lost (or gathered improperly). More litigation should decrease incentives to gather data, which should therefore lead to fewer violations and fewer suits.

These changes to the law and the incentives it creates would also help remedy the distributional effects of current standing doctrine. As this Article discusses, the present balance appears to favor corporate interests and to denigrate harms like anxiety as unworthy of judicial attention. Recognizing that these types of harms are cognizable in federal court should shift that balance. Moreover, even if merits decisions begin to go against data-protection plaintiffs, those decisions may highlight gaps in existing law and serve as a rallying point for policy advocacy. Examples of this phenomenon abound, such as the recent enactment of a "revenge porn" law in New York. While many pushed for enactment of such a law for years, a 2014 criminal case crystallized some of the shortcomings of existing New York law.[235] Advocates such as the Cyber Civil Rights Initiative highlighted that decision as an example of the failings of harassment law to curb non-consensual pornography, and argue for reshaping the legal landscape to better protect the interests of women by treating non-consensual pornography as a privacy issue[236]—leading, in

---

Introduction, 45 J. LEGAL STUD. 51 (2016) (examining various interactions between contract law and privacy issues).

234. Point-of-sale breaches are a ready example, as there are typically no terms of service presented or agreed to in a retail transaction. Moreover, tech firms' increasingly voracious appetite for data leads to situations in which lawsuits arise in the absence of a contractual relationship. For example, the Google Photos face-scan case, *Rivera*, involved two named plaintiffs—one a Google Photos user subject to Google's terms of service, but the other a friend of a Google Photos user.

235. *See* Emma Grey Ellis, *New York's Revenge Porn Law is a Flawed Step Forward*, WIRED (July 24, 2019, 5:18 PM), https://www.wired.com/story/new-york-revenge-porn-law/ [https://perma.cc/T9CA-229Y] (discussing case dismissing harassment claim in which "[a] man allegedly shared nude images of his girlfriend on Twitter and sent them to her family and employer" because New York law at that time "define[d] harassment as direct communication with the victim").

236. *See, e.g.*, Danielle Citron & Mary Anne Franks, *Evaluating New York's "Revenge Porn" Law: A Missed Opportunity to Protect Sexual Privacy*, HARV. L. REV. BLOG (Mar. 19, 2019), https://blog.harvardlawreview.org/evaluating-new-yorks-revenge-porn-law-a-missed-opportunity-to-protect-sexual-privacy/ [https://perma.cc/MK38-NEPN] (highlighting problems with treating revenge porn as a harassment issue rather than a privacy issue); *see also* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 347 (2014) ("Our

part, to the narrowing of the gap in New York's harassment law. This type of pattern could play out if courts adjudicating the merits of data-protection suits continue, for whatever reason, to indulge in skepticism about data-protection issues. In short, one way or the other, developing federal law on privacy will shift the law's expression, and the public should respond accordingly.[237]

C. Theoretical Approach

Focusing on the leading Supreme Court and appellate decisions on standing in data-protection litigation leaves too much on the table. Data takes many forms, and so too the litigation arising from its use, misuse, and loss. Courts can and do tinker with what they consider precedential in any given case. Thus, this Article proceeds from the belief that examination of a much broader set of cases enables new insights into the standing quandary. From those insights, it seeks to push the federal judicial system back onto a particular path—taking seriously the applicable purpose of standing doctrine in adjudicating standing challenges. Adopting that approach would have consequences beyond the sphere of data-protection. While other areas of law are beyond the scope of this Article, it is plausible to suggest that a more explicitly nuanced approach to standing in all cases would yield more accurate decisions than the current inquiry, which might fairly be deemed one-size-fits-none. This type of approach might also diminish the potential for judges to hide preference-motivated decisions on standing behind that opaque inquiry.

Additionally, although this Article shows the connection between *Clapper* and denials of standing is strong, it can show only correlation rather than causation. Some judges undoubtedly feel they are bound by the reasoning and approach set forth in *Clapper*. Others may reach to *Clapper* to justify skepticism about the harms asserted in a particular case. The motivating factors discussed in section II.B suggest that the latter situation occurs more often than might be desired. Either way, this Article hopes to remedy the issue to some extent by laying bare *Clapper*'s lack of connection to data-protection litigation.

None of this should be read to suggest that fixing the federal courts'

---

society has a poor track record in addressing harms that take women and girls as their primary targets. Though much progress has been made towards gender equality, much social, legal, and political power remains in the hands of men. The fight to recognize domestic violence, sexual assault, and sexual harassment as serious issues has been long and difficult, and the tendency to tolerate, trivialize, or dismiss these harms persists.").

237. *See, e.g.*, Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2025 (1996) (arguing that "the expressive function of law makes most sense in connection with efforts to change norms").

approach to standing in data-protection litigation (or elsewhere) is a panacea, nor that every data-protection lawsuit is meritorious. Rather, this Article seeks to offer solutions to a threshold problem, a necessary step on the path to enable a substantial shift in the treatment of private information in both theory and practice.

Connected to that goal is the question of whether private enforcement can or will move the needle. There is reason to believe that it could. Waldman, for instance, finds that regulatory action has had some success in inducing industry to emphasize privacy more strongly in their design activities.[238] Private enforcement could have a similar impact. In light of the FTC's recent, widely criticized resolution of privacy issues with both Facebook[239] and Equifax,[240] more robust private enforcement becomes even more attractive. These lackluster settlements suggest deep capture is at work, diminishing the FTC's appetite and ability to regulate industry players sufficiently.[241]

CONCLUSION

By looking beyond the relative handful of cases studied in existing literature, this Article's comprehensive approach identifies systemic pressures that contribute to the courts' erroneous decisions in data-protection litigation. Most notably, those pressures include widespread overreliance on case law with little application to the issues posed by data-protection lawsuits and failure to consider the purpose of standing doctrine in administering the inquiry. It then proposes new solutions tailored to those systemic pressures, most importantly the need for federal

---

238. *See* Waldman, *supra* note 230, at 665–66 ("[C]ompanies who have been the subjects of strong regulatory intervention are more successful at embedding the importance of consumer privacy into design. This opens a pathway for using robust FTC enforcement to make a difference.").

239. *See, e.g.*, *Challenge to FTC/Facebook 2019 Settlement*, ELEC. PRIV. INFO. CTR. (2019), https://epic.org/privacy/facebook/epic2019-challenge/ [https://perma.cc/W57A-RYFA] ("[The FTC's settlement with Facebook] does not incentivize Facebook to fix its deeply problematic business model and practices. Instead, the settlement fails to meaningfully limit Facebook's collection, use, and sharing of consumer data or impose any actually independent oversight over Facebook's use of personal data. On the whole, the settlement is not meaningfully different from the 2012 Consent Order that proved to be woefully inadequate in the wake of Facebook's continued privacy violations from 2012 to the present."); *see also id.* (collecting political and media criticism of the settlement).

240. *See, e.g.*, Rachel Siegel, *'Did Someone Forget to do the Math?' Consumers, Advocates Rail Against Lowered Equifax Cash Payouts*, WASH. POST (Aug. 1, 2019, 2:53 PM), https://www.washingtonpost.com/technology/2019/08/01/did-someone-forget-do-math-consumers-advocates-rail-against-lowered-equifax-cash-payouts/ [https://perma.cc/44TH-TSK5] (discussing criticism of distribution of settlement funds in Equifax's settlement with the FTC).

241. *See* Cohen, *supra* note 15, at 555 ("Deep capture—or capture at the level of ideology—proceeds as well-resourced repeat players work to craft compelling narratives about the contours of legal entitlements and the structure of legal institutions.").

judges to reorient their approach to the standing inquiry by focusing on the need to preserve adversarial presentation of the issues. Resolving the systemic errors in decisions on standing should advance the goal of data protection by permitting additional lawsuits to go forward, thereby better aligning private incentives with the public good.