PRIVACY STANDING

Ignacio Cofone[*]

Courts struggle with how to identify and assess privacy harm and privacy injuries. This uncertainty has produced a circuit split (and lower court split) on the requisite privacy injury sufficient for federal standing, recently addressed by the Supreme Court, albeit poorly, in TransUnion. This Article provides a framework for distinguishing which actions involve harm to people's privacy interests and which do to other interests. It provides courts with guidance to assess privacy injuries and proposes a solution to the circuit split that satisfies constitutional requirements without gutting private rights of action.

To address privacy standing while navigating Supreme Court case law hostile to privacy claims, federal courts should do three things. First, inquire whether someone faced a loss of privacy. Second, identify whether such a loss produced privacy harm by looking at normative aspects. Third, determine whether from such harm stems an actionable privacy injury by looking at tort law and statutory privacy to find whether there is a common law wrong or statutory wrong.

This Article's approach has theoretical and practical benefits. Theoretically, it sheds light on the relationship between privacy loss and actionable injuries. It is well-suited for evaluating grey areas by showing how privacy claims can be evaluated on a continuum. Practically, it gives courts a tool to better identify and navigate privacy harm, which is an increasingly relevant impediment to private rights of action in federal statutory privacy and which courts have manifested they need.

* Assistant Professor and Canada Research Chair in A.I. Law & Data Governance, McGill University Faculty of Law; Affiliated Fellow, Yale Information Society Project (ignacio.cofone@mcgill.ca). I'd like to thank Alex Abdo, BJ Ard, Thomas Haley, Woodrow Hartzog, Dennis Hirsch, Yoel Inbar, Jameel Jaffer, Thomas Kadri, Joshua Karton, Ido Kilovaty, Nancy Kim, Alyssa King, João Marinotti, Kirsten Martin, William McGeveran, Sunoo Park, Jon Penney, Neil Richards, Adriana Robertson, Clare Ryan, Yan Shvartzshnaider, Scott Skinner-Thompson, Lionel Smith, Daniel Solove, Lior Strahilevitz, Cristina Tilley, Felix Wu, and Benjamin Zipursky for their helpful comments. The Article also benefited from comments received at the Yale/Harvard Workshop on Private Law & Emerging Technology, the Symposium on Applications of Contextual Integrity, the Privacy Law Scholars Conference, and internal presentations at the Knight First Amendment Institute, McGill University Faculty of Law, and Queens University Faculty of Law. This research was undertaken, in part, thanks to funding from the Canada Research Chairs Program and the Social Sciences and Humanities Research Council. I also thank Malaya Powers, Jordan Bitan, Ana Qarri, and Alessia Zornetta for their fabulous research assistance and the editors of the *University of Illinois Law Review* for their work on the piece.

TABLE OF CONTENTS

I. INTRODUCTION

When considering privacy claims, courts are often unsure how to determine privacy harm.[1] Courts' difficulty with defining and identifying the privacy harm is deeply problematic because harm plays an important role in granting standing. This leads to inconsistent and normatively worrisome results at the district and appellate levels as to which statutory privacy lawsuits proceed and which do not.[2]

Courts will likely be increasingly called on to resolve evolving problems of privacy harm in a trial on the merits and, therefore, will require a comprehensive

1. *See* discussion *infra* Section II.A.
2. *See* discussion *infra* Section II.B.

framework to evaluate privacy harm. As Thomas Haley explains, "[d]ata-protection lawsuits are private-rights actions and should typically survive standing challenges. Nonetheless, the data suggest that federal courts are not employing this approach, … only 55% of the cases studied survived challenges to standing."[3] Guidance on how courts, particularly at the federal level, can determine privacy standing is needed.

This Article develops a framework for courts to reduce such uncertainty by better identifying privacy harm. It does so by distinguishing between actions that involve a legally cognizable harm to people's privacy interests—and thus should proceed—and those that do not.[4] This framework can be used to determine federal privacy standing.[5] It can be used to navigate recent Supreme Court cases such as *TransUnion v. Ramirez*.[6]

The framework has three steps. First, courts must identify whether there was a loss of privacy. This is the step to which this Article devotes the most attention, under the conjecture that this is the identification that courts find most difficult. Loss of privacy depends on whether the observer gained probabilistic information about the observed.[7] Second, if step one is answered in the affirmative, courts will sometimes be required to identify whether the loss of privacy constituted harm. Privacy harm depends on whether the privacy loss violated privacy's normative values, such as autonomy and intimacy.[8] Privacy harm should be broader than the injuries usually recognized as it is independent of other harms, such as reputational. Third, if step two is answered in the affirmative, courts must determine whether the privacy harm is actionable. This will depend on judicial precedent and statutory interpretation as to whether a statute grants standing.[9] Courts' most common mistake is answering the first and second questions through the third, muddling constitutional requirements with statutory interpretation.[10]

Separating and appropriately addressing each of these three steps has long-term consequences for corporate liability and consumer redress. More specifically, the framework makes three contributions. The first is infusing clarity into federal standing doctrine. One dominant and undesirable judicial trend in privacy is the federal circuit split in relation to standing doctrine's injury requirement.[11] Most circuit courts hold that the risk of future injury (*i.e.*, threat of future harm) from a data breach is insufficient to confer standing.[12] Other

3. Thomas Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193, 1224 (2020).
4. *See* discussion *infra* Part V.
5. *See* discussion *infra* Sections VI.A–B.
6. *See* discussion *infra* Section VI.C.
7. *See* discussion *infra* Part III.
8. *See* discussion *infra* Sections IV.A–B.
9. *See* discussion *infra* Section V.C.
10. *See* discussion *infra* Section V.C.
11. Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 91–105 (2017) (explaining the details of the circuit split).
12. Daniel Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 756–74 (2018).

circuit courts hold that substantial risk of future harm can be sufficient for determining injury for standing. This divide extends to lower courts.[13]

This divergence between federal courts demonstrates that judges struggle with how to constitute a privacy injury.[14] This creates the doctrinal problem of inconsistency of the law at the federal level. It also creates a policy problem: for some, the policy problem is that plaintiffs lack sufficient redress; for others, it is a problem of forum shopping where plaintiffs can creatively find an easier jurisdiction to sue. This Article's proposal on how to assess and address privacy harm aims to aid in achieving consistency among jurisdictions and resolving the circuit split.

The second contribution is demonstrating that privacy loss exists on a continuum in which privacy can decrease in varying amounts and is not a binary concept.[15] Actions can interfere with a person's levels of privacy differently and, when privacy injuries lead to other injuries, these often happen in the future and are difficult to prove because they usually occur by aggregating information. Privacy is different from assault, in which, once causality is established, there is a clear, consequent harm. Moreover privacy-harming actions take place increasingly often—they are no longer an exception.

The third contribution, building on scholarship about the wide range of data harms that can fall under privacy lawsuits,[16] is clarifying how each of them works differently.[17] For example, courts often refer to *Spokeo v. Robins* as a privacy injury case, but it is best seen as a reputation injury case.[18] When courts search for a privacy injury in cases like *Spokeo*, instead of a reputational injury, the harm can become unapparent, negatively affecting standing.[19] When courts search for a material harm when there is privacy harm the problem is worsened, systemically denying standing for meritorious claims.

The next Part identifies the core doctrinal difficulty: courts lack a systematic way to identify privacy harm to determine standing and compensation. Part III develops step one of the framework: how to identify privacy loss. Part IV develops step two: how to identify privacy harm and distinguish it from nonharmful privacy losses as well as from nonprivacy harms. Part V develops step three: identifying which privacy harms constitute injuries and should be granted standing and compensation. Part VI spells out the consequences of these findings for privacy law more generally, including how they relate to *TransUnion*. Part VII concludes with doctrinal and policy considerations for privacy standing.

13. *See, e.g.*, Rosenbach v. Six Flags Ent. Corp, 129 N.E.3d 1197, 1204 (Ill. 2019).
14. Danielle Citron & Daniel Solove, *Privacy Harms*, 102 B.U. L. REV. (forthcoming 2022).
15. *See* discussion *infra* Section III.E.
16. Citron & Solove, *supra* note 14.
17. *See* discussion *infra* Section V.C.
18. *See* discussion *infra* Section V.C.
19. *See* discussion *infra* Section V.C.

II. THE PROBLEM: COURTS GRAPPLE TO IDENTIFY PRIVACY HARM

A. The Harm Challenge

Federal courts struggle with identifying privacy harm arising from statutory violations.[20] In several cases, federal courts have required an injury beyond the statutory violation to satisfy standing.[21] In *Meyers v. Nicolet Restaurant*, for example, the Seventh Circuit dismissed a case where a store did not adequately truncate credit card numbers.[22] The Third Circuit reached the same conclusion in *Kamal v. J.Crew*,[23] as did the Ninth Circuit in *Bassett v. ABM*,[24] the Eleventh Circuit in *Tsao v. Captiva*,[25] and the Second Circuit in *Katz v. Donna*[26] and in *Crupar-Weinmann v. Paris Baguette*—all Fair and Accurate Credit Transaction Act ("FACTA") cases.[27] These cases were dismissed because the plaintiffs did not prove financial harm based on the statutory violation.[28]

This conclusion has extended beyond financial information. In *Beck v. McDonald*, where a laptop containing veterans' medical information was stolen or misplaced, the Fourth Circuit stated that the Privacy Act requires "actual injury" and declined to decide on whether a statutory violation can create a de facto injury because plaintiffs did not assert it.[29] The Seventh Circuit reached this conclusion in the famous *Gubala v. Time Warner Cable* case, denying standing based on the Cable Communications Policy Act because the plaintiffs had not demonstrated any harm besides alleging the statutory violation.[30] In *Braitberg v. Charter Communications, Inc.*, similarly, the Eighth Circuit found that a statutory violation of the Cable Communications Policy Act was insufficient for

20. Citron & Solove, *supra* note 14.

21. *See infra* notes 22–27 and accompanying text.

22. 843 F.3d 724, 729 (7th Cir. 2016) ("This case asks whether the violation of a statute, completely divorced from any potential real-world harm, is sufficient to satisfy Article III's injury-in-fact requirement. We hold that it is not. Therefore, neither the district court nor this court has the authority to certify a class action.").

23. 918 F.3d 102, 113 (3d Cir. 2019) ("Kamal has pleaded two allegedly 'concrete' injuries: 'the printing of the prohibited information itself,' *i.e.*, a violation of FACTA's plain text, and the 'increas[ed] risk of identity theft' resulting from that printing. . . . But the procedural violation is not itself an injury in fact, and Kamal has not otherwise alleged a risk of harm that satisfies the requirement of concreteness.").

24. 883 F.3d 776, 777 (9th Cir. 2018) ("Bassett sued but alleged only a statutory violation and a potential for exposure to actual injury. . . . [W]e conclude that Bassett failed to allege a concrete injury sufficient to give him standing.").

25. 986 F.3d 1332, 1336 (11th Cir. 2021) (concluding Tsao lacked standing due to a lack of concrete harm as Tsao importantly did not suffer from identity theft or robbery as a result of the data hack because he cancelled his credit cards and so he argued "that he had standing (1) because he and the class were at an elevated risk of identity theft, or, alternatively, (2) because he took 'proactive' steps to mitigate the risk of identity theft").

26. 872 F.3d 114, 121 (2d Cir. 2017) (holding that the plaintiff had not established a concrete injury sufficient to maintain Article III standing as the bare procedural violation in question did not raise a material risk of harm).

27. 861 F.3d 76, 78 (2d Cir. 2018) ("[A] receipt with a credit card expiration date does not raise a material risk of identity theft, and finding that the bare procedural violation alleged by the plaintiff does not present a material risk of harm, we conclude that allegations in her amended complaint do not satisfy the injury-in-fact requirement necessary to establish Article III standing to bring suit.").

28. *See supra* notes 22–27 and accompanying text.

29. 848 F.3d 262, 271 (4th Cir. 2017).

30. 846 F.3d 909, 911 (7th Cir. 2017).

standing as the plaintiffs had not demonstrated another harm or material risk of harm arising from the statutory violation.[31]

Other courts, particularly state courts free of constitutional limitations on standing, have ruled that no harm beyond the statutory violation is needed under some privacy statutes. For instance, in *Rosenbach v. Six Flags*, the Illinois Supreme Court concluded that an individual need not allege an actual injury or adverse effect to be considered an "aggrieved" individual beyond violation of her rights under the Illinois Biometric Information Privacy Act ("BIPA").[32] This is because the statute requires that companies obtain written consent and disclose how they collect, retain, disclose, and destroy biometric information from the public and establishes that aggrieved individuals have a right to sue.[33] More importantly, it is also because, as a state court, the Illinois Supreme Court does not face the Supreme-Court-established Article III limitations on jurisdiction, as explained in more detail below.[34]

Both judicial positions are problematic in different ways. On the one hand, courts that categorically deny standing on the basis that they must require an injury ignore the nature of privacy injuries.[35] They require something else: that the privacy injury led to a different downstream injury (financial, reputational, etc.) that courts are used to identifying and measuring.[36] This requirement is problematic because these consequential injuries often do not materialize until much later and, when they materialize, causality is extremely difficult to establish, leading to such injuries frequently being left unaddressed.[37] As a consequence, people who had a privacy injury are systematically denied standing—before even opening a conversation about appropriate compensation or remedies.[38]

On the other hand, finding for a plaintiff based on a defendant's statutory violation alone also leads to challenges. For federal courts, suggesting that the statutory violation itself is the injury may lead to constitutional problems for deviating from the Supreme Court's interpretation of Article III.[39] For plaintiffs

31. 836 F.3d 925, 930 (8th Cir. 2016) ("His complaint asserts 'a bare procedural violation, divorced from any concrete harm.' . . . Braitberg alleges only that Charter violated a duty to destroy personally identifiable information by retaining certain information longer than the company should have kept it. . . . He identifies no material risk of harm from the retention; a speculative or hypothetical risk is insufficient.").

32. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1204 (Ill. 2019).

33. *Id.*

34. *See* discussion *infra* Sections II.B–C.

35. *See* discussion *infra* Sections II.B.

36. *See* discussion *infra* Section II.B.

37. *See* discussion *infra* Sections VI.A–B.

38. *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016).

39. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013); Bradford C. Mank, Clapper v. Amnesty International*: Two or Three Competing Philosophies of Standing Law?*, 81 TENN. L. REV. 211, 213, 255 (explaining that the Supreme Court held in *Clapper* that Article III's language imposes standing requirements for plaintiffs before federal courts can consider the merits of a case and demonstrating that there has been considerable debate about the extent to which Congress may enlarge the definition of concrete injury under Article III by statute, and the extent to which the separation of powers limits congressional authority to grant universal standing rights to plaintiff who lack a concrete injury); *see also* Ass'n of Data Processing Serv. Orgs., Inc. v. Camp, 397 U.S. 150, 153 (1970) (landmark case separating the invasion of a legal interest from an injury-in-fact).

who find themselves in any court, it may ironically lead to under-compensation (or over-compensation) downstream due to granting standing without an evaluation of actual harm.[40] What is needed, instead, is a way to identify privacy injuries even when consequential harms (such as financial) are absent.

B. The Problem of Determining Privacy Standing

Standing determines whether the plaintiff has the right to sue.[41] It asks whether the person suing suffered real injuries caused by the defendants that can be addressed by the court.[42] At the federal level, standing goes hand-in-hand with harm.[43]

To have standing and invoke federal jurisdiction a plaintiff must establish the three requirements of Article III: (1) injury-in-fact (*i.e.*, an imminent or a concrete and particularized invasion of a legally protected interest that affects the plaintiff differently than everyone else), (2) causation (*i.e.*, a fairly traceable connection between the alleged injury and the alleged conduct of the defendant), and (3) redressability (*i.e.*, it is likely and not merely speculative that the plaintiff's injury can be remedied by bringing suit).[44] Article III standing since *Clapper v. Amnesty International* requires potential plaintiffs to show that they suffered an injury that is concrete, particularized, and actionable or imminent; fairly traceable to the challenged action; and subject to redress by a favorable ruling.[45]

The first of these requirements is important and controversial in privacy. Federal courts' power to review cases and controversies means that plaintiffs must have suffered an injury-in-fact.[46] To satisfy the injury-in-fact requirement, the plaintiff must show that the invasion of her legally protected interest is concrete and particularized.[47] For it to be concrete, it must be real, not abstract; it must be "actual or imminent, not conjectural or hypothetical."[48] For it to be particularized, it must "affect the plaintiff in a personal and individual way."[49] When a plaintiff lacks an injury-in-fact, federal standing is denied to them.[50] Consequently, the difficulties in identifying privacy harm translate directly into difficulties in establishing privacy standing.

40. *See supra* notes 13, 22–27 and accompanying text.

41. *See* Meyers v. Nicolet Rest. of De Pere, LLC., 843 F.3d 724, 726 (7th Cir. 2016).

42. *See id.* at 729.

43. U.S. CONST. art. III, § 2, cl. 1; *Clapper*, 568 U.S. at 408 ("One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue.").

44. William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 229 (1988).

45. *Clapper*, 568 U.S. at 409 (adding that these Article III requirements lead to the requirement that a "'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient").

46. *See id.*

47. *See id.* at 420.

48. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (internal quotation marks omitted) (holding that a group of wildlife conservation and environmental organizations lacked standing to challenge regulations of the Endangered Species Act, and that the irreducible constitutional minimum of standing contains three elements).

49. *Id.* at 560 n.1.

50. *See id.* at 578.

The scope of standing in privacy litigation in light of this requirement was addressed (albeit unsatisfactorily) in the 2016 decision *Spokeo v. Robins*. Robins alleged that Spokeo, a company that collects data from individuals and provides it to potential employers, had false information about his age, employment, marital status, and education, and that such information worsened his chances of finding a job and produced emotional distress.[51] The Ninth Circuit ruled unanimously that Robin's harm based on Spokeo's breach of the Fair Credit Reporting Act ("FCRA") satisfied federal standing (it was an injury-in-fact).[52] The Supreme Court vacated and remanded.[53]

The Court held that, as a constitutional matter, "Article III standing requires a concrete injury even in the context of a statutory violation" and failed to identify privacy harm as constituting such a concrete injury.[54] The Court rejected that "a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[55]

Thus, plaintiffs seeking redress for privacy harm at the federal level must identify a cognizable real-world harm that they suffered. It remains unclear what exactly such a cognizable real-world harm means in the privacy context.[56] But, based on *Spokeo*, numerous privacy cases have turned on standing, often being dismissed for lack of injury-in-fact based on a narrow definition of concrete injury, long before such cases reach trial.[57]

This leads to what may be *Spokeo*'s most consequential characteristic: the circuit court (and lower court) split on standing in relation to injury.[58] Currently, the First, Second, Third, Fourth, and Eighth Circuits hold that a threat of future harm from a data breach alone is insufficient to confer standing if not coupled with a more concrete injury.[59] These courts consider that plaintiffs must allege more than the fact that their information was stolen to show an Article III injury for standing.[60] In other words, these courts consider the privacy harm of a data breach insufficient and require other particularized harms such as financial harm. The risk of future harms due to the privacy violations has also been deemed insufficient. For example, in the case of stolen financial information, these courts consider that allegations of heightened risk of identity theft, or prophylactic measures taken to reduce such risk, cannot be the basis for standing.[61] By

51. Robins v. Spokeo, Inc., 742 F.3d 409, 412–14 (9th Cir. 2014).

52. *Id.*; *see also* 15 U.S.C. §§ 1681–1681x. *See generally* Robins v. Spokeo, Inc., No. CV10–05306, 2011 WL 11562151, at *1 (C.D. Cal. Sept. 19, 2011) (dismissing the case).

53. *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 333 (2016).

54. *Id.* at 341.

55. *Id.* ("Article III standing requires a concrete injury even in the context of a statutory violation.").

56. *Cf. id.* at 340–41.

57. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934 (2013) ("Courts frequently dismiss challenges to such [security] programs for lack of standing, under the theory that mere surveillance creates no harms.").

58. *See Spokeo*, 578 U.S. at 343.

59. Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1340 (11th Cir. 2021).

60. *See, e.g.*, Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (E.D.N.Y. 2017) (memorandum opinion).

61. *See id.*

contrast, the Sixth, Seventh, and Ninth Circuits have ruled that substantial risk of future harm is sufficient for determining injury for standing.[62]

C. The Circuit Split and Spokeo v. Robins

As the Fourth Circuit explained in *Beck v. McDonald*, "[o]ur sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft."[63] Similarly, in a 2021 ruling the Eleventh Circuit explained that "the Sixth, Seventh, Ninth, and D.C. Circuits have all recognized—at the pleading stage—that a plaintiff can establish injury-in-fact based on the increased risk . . . [while] the Second, Third, Fourth, and Eighth Circuits have declined to find standing on that theory."[64]

An injury-in-fact need not be tangible for it to be concrete or real.[65] To determine whether an intangible harm constitutes an injury-in-fact, courts must consider two things under *Spokeo*: history and Congress's judgment.[66] First, courts should consider "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[67] Second, they should consider Congress's statutory determination on standing—which *Spokeo* indicates is "instructive and important."[68]

Instructive and important, however, does not mean sufficient. Violating a privacy law statutory requirement does not automatically create standing according to the Court because these violations may result in no harm that is particularized enough.[69] That said, Congress has the power to transform injuries that were not legally cognizable into legally cognizable ones by elevating them into concrete injuries by statute.[70] Although the violation of a statutory right is not in itself enough to constitute an injury-in-fact, some particular statutory violations do establish an injury-in-fact.[71]

As Daniel Solove explains:

> Congress is not limited to the types of injuries the courts define as concrete. Thus, Congress can deem even injuries "previously inadequate in law" to be concrete injuries sufficient to confer standing. Congress can thus

62. *See Tsao*, 986 F.3d at 1340.

63. Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017) ("The Sixth, Seventh, and Ninth Circuits have all recognized, at the pleading stage, that plaintiffs can establish an injury-in-fact based on this threatened injury. . . By contrast, the First and Third Circuits have rejected such allegations."); *see also* Citron & Solove, *supra* note 14.

64. *Tsao*, 986 F.3d at 1340 (citations omitted).

65. Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016).

66. *Id.*

67. *Id.*

68. *Id.* at 341 ("[B]ecause Congress is well positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important.").

69. *See id.* at 342. Scholars disagree as to whether *Spokeo* should be construed as referring only to a statute's procedural requirements or also substantive statutory requirements.

70. *Id.* at 341 (explaining that the "status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law" (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992))).

71. *Id.* at 342.

> independently define "concrete injury" in a way that enlarges the concept and brings cases to the courts that courts ordinarily wouldn't hear because of more narrow judicial definitions of "concrete injury."[72]

The unresolved question is which statutes have this effect.

Thus, an enormously consequential role of any federal court in privacy law is to determine which statutes establish a legally cognizable privacy injury. Any federal privacy statute with a private cause of action not requiring proof of specific harm is a good candidate. These include the Electronic Communications Privacy Act,[73] the Stored Communications Act,[74] the Driver's Privacy Protection Act,[75] the Video Privacy Protection Act,[76] and the Cable Communications Policy Act.[77] It is unclear whether a violation of any of these statutes would sufficiently establish injury-in-fact for the Supreme Court, but there is nothing in any of them that would prevent a lower court from interpreting that they do.

To comply with *Spokeo*, federal courts must abide by Congress' power to define harms in federal statutes while also holding that a statutory violation does not always, by itself, create an injury-in-fact.[78] This did not have to be that way: statutory standing requirements could have been construed with closer similarity tort law, where a technical violation is often enough. But in the current legal context, complying with *Spokeo* (and *Transunion*) without emptying privacy rights of their content requires a cohesive theory of privacy harm. Such theory involves first identifying privacy loss and then distinguishing which losses were harmful.

III. STEP 1: A FRAMEWORK TO IDENTIFY LOSS OF PRIVACY

A. How to Identify Privacy Loss

Neil Richards explains that "[d]espite often displaying an intuitive understanding that surveillance might be potentially harmful, courts have struggled to understand why. This absence of clarity has led to courts misunderstanding and diminishing privacy interests."[79]

72. Daniel Solove, *When Is a Person Harmed by a Privacy Violation? Thoughts on* Spokeo v. Robins, TEACHPRIVACY: PRIV. + SEC. BLOG (May 17, 2016), https://teachprivacy.com/thoughts-on-spokeo-v-robins/ [https://perma.cc/LB88-YU2E] ("For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III.") (quoting *Spokeo*, 578 U.S. at 341).

73. 18 U.S.C. §§ 2510–2523.

74. *Id.* §§ 2701–2713.

75. *Id.* §§ 2721–2725.

76. *Id.* §§ 2710.

77. 47 U.S.C. §§ 521–573.

78. *See* Spokeo, Inc., v. Robins, 578 U.S. 330, 341 (2016).

79. Richards, *supra* note 57, at 1951 (adding that diminishing privacy interests in such a way conflicts with other values of the legal system).

Responding to this concern, in a 2018 article, Adriana Robertson and I propose how to add specificity to privacy loss in tort law.[80] An adapted version of that idea can help identify privacy loss in private rights of action for statutory privacy. In tort law, strictly speaking, there is no law of standing: everyone whose right has been infringed holds a power to sue the infringer. The parallel is that identifying whether there is privacy loss in a statutory case determines whether there is a privacy interest at play beyond a mere statutory violation in terms of *Spokeo*, thus warranting a harm analysis.

Two cases demonstrate the issue of privacy loss. In *Hancock v. Urban Outfitters*, the company allegedly violated D.C.'s Use of Consumer Identification Information Act, which prohibits retailers from asking for a customer's address in connection with a credit card transaction.[81] The injury that the named plaintiffs claimed to have suffered was that they were asked for a zip code in violation of the statute. The D.C. Circuit dismissed the claims for lack of standing.[82] According to the court, the plaintiffs failed to allege an injury, as required for standing—mere collection of data, even if illegal, was not an injury sufficient for standing under Article III.[83]

By contrast, in *Patel v. Facebook*, plaintiffs filed a class action against Facebook for using facial-recognition software on pictures that people uploaded to the platform without acquiring consent in their "tag suggestions" feature, in violation of BIPA.[84] The Ninth Circuit ruled that plaintiffs suffered a harm to their privacy interest that is recognized by BIPA, granting them standing.[85] Similarly, in *Rosenbach v. Six Flags*, a state court case mentioned above, a putative class action alleged that the defendant theme park collected the plaintiff's teenage son's thumbprint as part of his purchase of a season pass to the theme park.[86] The plaintiff contended that neither she nor her son gave informed consent to the collection or retention of that biometric data, contrary to Illinois's BIPA, which requires that companies obtain written consent and reveal how they collect, retain, disclose, and destroy biometric identifiers.[87] The plaintiff sought monetary damages and injunctive relief under the Act but did not allege that her son suffered any actual harm as a result of the thumbprint

80. Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1049–58 (2018) (developing a continuous privacy model that considers privacy preferences and captures the tradeoffs associated with privacy and privacy law and the essence of privacy loss).

81. Hancock v. Urb. Outfitters, Inc., 830 F.3d 511, 512 (D.C. Cir. 2016).

82. *Id.*

83. *Id.* at 514 ("The Supreme Court's decision in *Spokeo* thus closes the door on Hancock and White's claim that the Stores' mere request for a zip code, standing alone, amounted to an Article III injury."). Even though the court did not make explicit that the illegality of the collection is irrelevant, this conclusion follows from the facts: not even is collection of data not enough for standing, in this case it was an illegal collection of data since the Consumer Identification Act prohibited it.

84. Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019).

85. *Id.* at 1275 ("Because we conclude that BIPA protects the plaintiffs' concrete privacy interests and violations of the procedures in BIPA actually harm or pose a material risk of harm to those privacy interests, . . . the plaintiffs have alleged a concrete and particularized harm, sufficient to confer Article III standing.").

86. Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶ 6.

87. *Id.*, ¶ 1.

collection.[88] The Illinois Supreme Court held that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[89]

Urban Outfitters, *Patel*, and *Six Flags* had similar alleged injuries, but their outcomes were diametrically opposite.[90] The cases involved different types of courts (federal and state) and were based on different statutes,[91] but involved statutorily prohibited information collection or use.[92] The question was not whether the activity was authorized, but how the unauthorized activity impacted the plaintiff.

Another example helps illustrate how these cases relate to privacy loss and harm. In the (yet unresolved) complaint in *Brown v. Google*, plaintiffs filed a class action against Google for interception of communications and misrepresentation of its tracking activities.[93] Google profits from selling targeted advertising spots allocated based on a user's personal information and tracks its users to more effectively place those advertisements.[94] Imagine a member of the *Brown* class called Arianna, who has some personal characteristic that Google would like to know in order to place ads more effectively, such as her willingness to pay for running shoes.[95]

Suppose that, initially, Google has no knowledge about the information it seeks about Arianna—she is uniquely new to the internet. It is unable to collect that information directly: it cannot email Arianna to ask for her willing price range for running shoes. However, Google has a good estimation about the overall distribution of that information in the population (the distribution of how much people are willing to pay for running shoes).[96] Google also has some information about Arianna, such as her gender and age, that allow it to start from

88. *Id.*, ¶ 22.

89. *Id.*, ¶ 40.

90. *Compare id.*, *with Urb. Outfitters*, 830 F.3d at 514.

91. Note that, importantly, the court in *Urban Outfitters* was bound by Article III while the court in *Six Flags* was not.

92. *Compare Six Flags*, 2019 IL 123186, ¶ 1, *with Urb. Outfitters*, 830 F.3d at 512.

93. Brown v. Google LLC and Alphabet Inc., No. 20-3644 (N.D. Cal. filed June 2, 2020) ("Google accomplishes its surreptitious tracking through means that include: Google Analytics, Google Ad Manager, and various other application and website plug-ins, such as Google applications on mobile devices and the 'Google Sign-In button' for websites. When an internet user visits a webpage or opens an app that uses such services (over 70% of all online publishers use such a service), Google receives detailed, personal information such as the user's IP address (which may provide geographic information), what the user is viewing, what the user last viewed, and details about the user's hardware.").

94. *See* Ben Popken, *Google Sells the Future, Powered by Your Personal Data*, NBC NEWS (May 10, 2018, 3:30 AM), https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501 [https://perma.cc/L82J-HXL7].

95. *See* Cofone & Robertson, *supra* note 80, at 1049–50 (proposing a similar example to illustrate the privacy model, in which an employer seeks to know more about a prospective employee's characteristics in order to know how desirable she is as an employee).

96. *See id.* at 1050 (explaining that an employer has a fairly good idea about the overall population of workers in the community and the general shape of the distribution of the community's workers). Google knows the mean, the standard deviation, and the general shape of the distribution—whether individuals are evenly spread out or whether they tend to be bunched together with only a few outliers.

the more precise distribution for that gender and age group, rather than the distribution for the general population.

Google can also observe things about Arianna that allows it to guess more about Arianna's target information, which one can call clues.[97] Each of these clues represents a piece of information about Arianna. For example, Google may observe that Arianna browses expensive furniture stores and four-star hotels. These clues will not give Google complete certainty about what it would like to know about Arianna (her willingness to spend on running shoes). But Google can form a clearer picture about the target information by running analytics on these clues. When it aggregates these clues, Google can undertake its best guess about Arianna's target information.[98] Each time Google observes another clue about Arianna, it can become more certain about her target information. Because it knows that this is only an informed guess, it still has some uncertainty—it might guess slightly wrongly.[99]

Depending on how good Google's guess about Arianna's target information is, Arianna has a loss of privacy with respect to Google and her target information.[100]Arianna has less privacy towards Google the more certain that Google is about the target information—and more privacy the less certain Google is.

Privacy loss is a descriptive concept, and privacy harm is a normative concept. Factors such as Arianna's loss of autonomy due to the learned information, and whether Google breached any social norms in acquiring it, enter at a later stage in a normative assessment of privacy harm.

In *Urban Outfitters*, the plaintiff faced privacy loss: the company knew more about the customer after the illegal collection of their address than before, and it did so about relevant and sensitive personal information.[101] The plaintiff in *Six Flags* also experienced privacy loss*:* by illegally collecting a fingerprint, the company knew more about the child than before—and it did so about relevant and sensitive personal information.[102] The same is true of the plaintiffs in *Patel*: Facebook knew more about them after processing their biometrics with facial recognition software. This alone does not resolve the standing issue, but it does show why diverging results on similarly situated plaintiffs is puzzling to the observer and potentially problematic.[103] In all three cases, in other words, plaintiffs faced privacy loss due to conduct prohibited by statute, but normative

97. *See id.* (using the employer/prospective-employee example to demonstrate that "while [the employer] may not know exactly how desirable she is as an employee (her 'type'), [the employer] may be able to learn where she went to college, how many jobs she has had in the last year, and whether she has ever been convicted of a felony").

98. *See id.* ("None of these signals fully reveal [the prospective employee's] type (her desirability as an employee) on their own. They do, however, allow [the employer] to form a clearer picture about it. Specifically, when he aggregates these signals, [the employer] can form his best guess about [the prospective employee's] type.").

99. *See id.*

100. *See id.* at 1050–51.

101. Hancock v. Urb. Outfitters, Inc., 830 F.3d 511, 512 (D.C. Cir. 2016).

102. *See* Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶ 6.

103. *Compare id.*, ¶ 40, *with Urb. Outfitters*, 830 F.3d at 514.

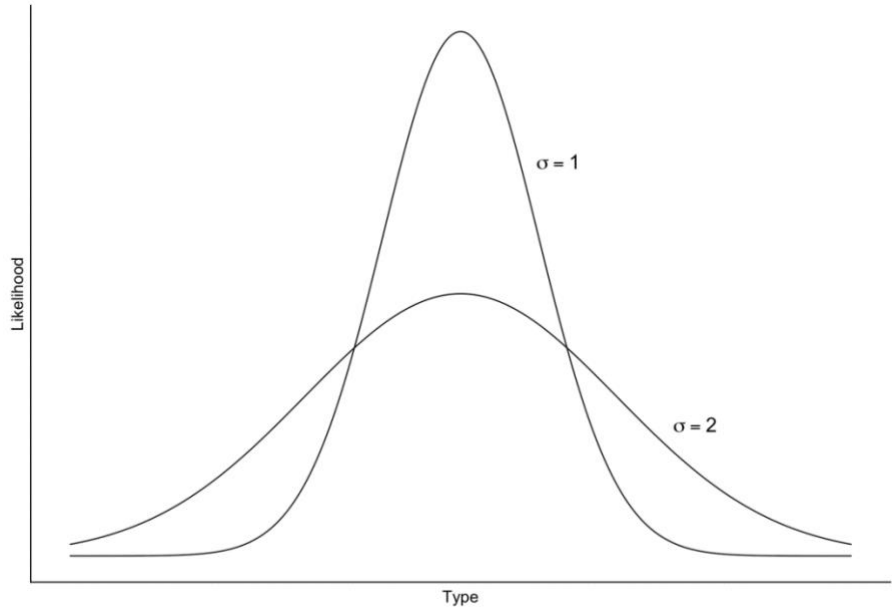
factors determine whether this privacy loss resulted in privacy harm and whether the cases can be distinguished.[104]

104. *See* discussion *infra* Sections IV.A–B.

B. An Illustration of the Framework: Google and Grindr

Every increase in Google's certainty results in an equivalent privacy loss to Arianna. In Bayesian terms, Google's certainty increases when the variance of its probability distribution shrinks (in Figure 1, the variance is the width of each distribution).[105] Google's certainty about Arianna and Arianna's privacy towards Google are correlative. Thus, one can identify whether Arianna suffered privacy loss by looking at whether the variance of Google's bell-curved probability distribution changed.[106] Figure 1, below, illustrates this idea.

FIGURE 1: ARIANNA HAS MORE PRIVACY WITH REGARDS TO GOOGLE WHEN GOOGLE'S DISTRIBUTION IS SHORTER AND WIDER.



In Figure 1, Arianna's target information can be any point on the x axis.[107] Imagine Google is determining which running shoes ads to show Arianna. The left end of the x axis is a willingness to pay zero dollars for running shoes, perhaps because Arianna already owns too many.[108] The further down the x axis that Arianna is, the more she is willing to pay for a pair of running shoes. At the

105, *See* Cofone & Robertson, *supra* note 80, at 1051.

106. *See id.*

107. *See id.* at 1052. This does not imply that type summarizes only one category of information. Just as the price of a car summarizes a host of factors about the vehicle itself, as well as factors related to the local market and, in certain cases, the buyer, an individual's type can be interpreted as a summary of all relevant information about her for the purposes for which the acquirer gathers her information.

108. One may object to this statement that there is no such thing as owning too many pairs of running shoes. If one were to make this objection, then one's placement on Google's x axis would never be far to the left. Learning this belief would be important for Google.

far right of the x axis, one would place the most expensive pair of running shoes available. The y axis represents the likelihood of each option.

When Google has few clues about how much Arianna is willing to pay for her next pair of running shoes, its probability distribution may resemble the wider curve $\sigma^2=2$.[109] In this scenario, it knows that there is a wide range of options. Some of those options, such as a willingness to pay zero dollars or a lot of money for running shoes, are not very likely (in the tails of the distribution). Other options are more likely (closer to the center of the distribution). When Google only knows basic information, such as Arianna's age and gender, its probabilistic knowledge, which we could call belief distribution, has the shape of this curve.

When Google collects more information about Arianna, its knowledge moves from the wider curve $\sigma^2=2$ to one like the narrower curve $\sigma^2=1$.[110] Here, the distribution becomes narrower because Google has a better idea about Arianna, so the range of possible amounts that Arianna may pay for running shoes is reduced. The distribution also becomes taller in the center and shorter in the tails because some options become more likely than before, and some become less likely. If Google's belief traces this curve, it may know more about its target information, for example by learning that Arianna usually stays in four-star hotels. This clue suggests that Arianna has some disposable income, so she is less likely to pay zero for running shoes, but is also not rich, so is also less likely to pay for the most expensive designer options.

As Google collects more information about Arianna, it can move from the narrow curve $\sigma^2=1$ to a new, even narrower curve.[111] Google would then have an even better idea about what it wants to know about Arianna; it could rule out the possibility that Arianna's target information will be located in either of the tails of the distribution, and focus on the narrow range of highly plausible values.[112] If Google's belief traced such a curve, it would have more specific information, such as how much Arianna has previously paid for running shoes.

One can turn to real-world present controversies to apply the framework. In January 2021, queer dating app Grindr faced a historic fine of 10% of its global turnover by the Norwegian Data Protection Authority (the "Authority").[113] The fine arose from having inadequate consent provisions for sharing information with third parties: a take-it-or-leave-it option in their privacy policy, the Authority ruled, was insufficient due to the sensitivity of Grindr's information

109. *See* Cofone & Robertson, *supra* note 80, at 1050.

110. *See id.* at 1050–51.

111. *See id.* at 1051.

112. Clues can have different levels of informativeness. Some clues may not be very informative—just as some facts are unhelpful in answering a question. Each of these uninformative clues would have less of an effect on Google's probability distribution than would informative clues.

113. Finn Myrstad & Øyvind H. Kaldestad, *Historic Victory for Privacy as Dating App Receives Gigantic Fine*, FORBRUKERRADET (Jan. 26, 2021), https://www.forbrukerradet.no/news-in-english/historic-victory-for-privacy-as-dating-app-receives-gigantic-fine/ [https://perma.cc/8YF9-E65K] (explaining the Norwegian Data Protection Authority's decision and declaring it as a "milestone in the ongoing work to ensure that consumers' privacy is protected online").

about users, which includes sexual orientation and HIV status.[114] In response, Grindr's lawyers "argued that sexual orientation, a specially protected category of data, was not exposed by selling its users' data, since some of them may be straight."[115] That is, they reminded the Authority that not every man who has sex with a man is gay and thus argued that exposing who was looking to have or considering having sex with a man on Grindr does not actually reveal sexual orientation.[116]

The framework presented above helps identify why Grindr's argument is incorrect. While having a Grindr account certainly does not provide conclusive evidence of sexual orientation (only of interest in a sexual activity), it profoundly matters probabilistically.[117] A man with a Grindr account is much more likely to be gay than a man without a Grindr account.[118] That is, every Grindr client who had their information shared with third parties had the information regarding their sexual orientation moved, in terms of Figure 1, from the wide to the narrow belief distribution. This means that the third parties' knowledge about the users' sexual orientations was more certain than before the information was shared. Grindr's argument is incorrect because people do not only lose privacy when someone produces conclusive evidence about them: loss of privacy can be probabilistic. Probabilistic beliefs also negatively affect privacy because probabilistic knowledge is still knowledge.[119] In other words, probabilistic knowledge produces privacy loss.

As a general rule, the information that will give a company a more precise probability distribution will not be one individual but significant clue, but rather an aggregation of an enormous amount of rather insignificant clues.[120] This takes us to a key problem that this interaction presents for data subjects, which is explored in the next subsection: the problem of inferred information.

114. Press Release, *Norwegian DPA: Intention to Issue € 10 Million Fine to Grindr LLC*, EUROPEAN DATA PROT. BD. (Jan. 26, 2021) [hereinafter EUROPEAN DATA PROT. BD.], https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-intention-issue-eu-10-million-fine-grindr-llc_en [https://perma.cc/BV3M-QUEJ].

115. Alex Hern, *Grindr Fined £8.6m in Norway over Sharing Personal Information*, GUARDIAN (Jan. 26, 2021, 11:36 AM), https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information [https://perma.cc/S474-5CYP] ("That argument was rejected by the Norwegian authorities, who noted that the app explicitly markets itself as 'exclusively for the gay/bi community.'").

116. *See id.*

117. *See id.*

118. William C. Goedel & Dustin T. Duncan, *Geosocial-Networking App Usage of Gay, Bisexual, and Other Men Who Have Sex with Men: Survey Among Users of Grindr, a Mobile Dating App*, 1 JMIR PUB. HEALTH & SURVEILLANCE 1, 1 (2015).

119. *See generally* SARAH MOSS, PROBABILISTIC KNOWLEDGE (2018) (explaining that, in addition to full beliefs and beliefs about a probability, credences constitute knowledge).

120. *See* Sachin Gupta & Matthew J. Schneider, *Protecting Customers' Privacy Requires More than Anonymizing Their Data*, HARV. BUS. REV. (June 1, 2018), https://hbr.org/2018/06/protecting-customers-privacy-requires-more-than-anonymizing-their-data [https://perma.cc/3GKZ-2MCL].

C. The Problem of Inferred Information: Credit Cards and Receipts

Recall the facts of *Meyers v. Nicolet Restaurant* and *Kirchein v. Pet Supermarket*.[121] In *Meyers*, a restaurant allegedly violated FACTA by printing the expiration date of a credit card on a sales receipt.[122] In *Kirchein*, a supermarket printed more than five digits of credit card numbers on customers' receipts, which is a violation of prohibitions on printing more than the last five digits of the credit card number or expiration date on the receipt provided to the customer.[123] In both cases, the plaintiffs alleged that the company increased the risk that the customers' identity would be compromised, for example through identity theft. In both cases, the court dismissed the case based on lack of standing resulting from the plaintiff's failure to demonstrate the suffering of an actual harm.[124] In *Meyers*, the Seventh Circuit considered that the plaintiff's allegation of a statutory violation without alleging how that violation injured him failed to establish the concrete injury required by *Spokeo v. Robins*.[125] In *Kirchein*, the U.S. District Court for the Southern District of Florida dismissed the claim for lack of subject-matter jurisdiction because the plaintiff failed to identify actual harm arising from the statutory violation.[126]

These cases highlight a major policy aspect of privacy harm decisions: it is rare that a piece of disclosed personal information is the information that produces harm to that person. Most often, information acquires its harmful characteristic through the process of aggregating different pieces of personal information and inferring new information out of them.[127] In other words, harmful information is rarely collected information and is frequently inferred information—produced by aggregating different pieces of seemingly inoffensive collected information.[128] An expiration date alone is unlikely to lead to identity theft or credit card fraud. Neither will a couple of added exposed digits of a credit card number. But each of these pieces of information aggregated with the other may very well lead to serious harm.[129] When we share something about us, we

121. Meyers v. Nicolet Rest. of De Pere, LLC, 843 F.3d 724, 725–26 (7th Cir. 2016); Kirchein v. Pet Supermarket, Inc., 297 F. Supp. 3d 1354, 1356 (S.D. Fla. 2018).

122. *Meyers*, 843 F.3d at 725 ("Meyers was given a copy of his receipt after dining at Nicolet. . . . He noticed that Nicolet's receipt did not truncate the expiration date, as the FACTA requires.").

123. *Kirchein*, 297 F. Supp. 3d at 1356 ("Kirchein filed a putative class action alleging that the Defendant violated the Fair and Accurate Credit Transactions Act, which prohibits printing 'more than the last five digits of the credit card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction.'").

124. *Meyers*, 843 F.3d at 725; *Kirchein*, 297 F. Supp. 3d. at 1357–60.

125. *Meyers*, 843 F.3d at 727; *see also* Spokeo, Inc. v. Robins, 578 U.S. 330, 339 (2016) (holding that a standing injury must be both concrete and particularized).

126. *Kirchein*, 297 F. Supp. 3d. at 1360.

127. *See* Haley, *supra* note 3, at 1213–16 (discussing *Supervalu* and the Equifax data breach).

128. Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 98 (2013) ("[I]mperfect consumer information about the potential harms of data collection, company data practices, and means to mitigate data collection combine with the properties of information aggregation and with common behavioral economics concerns to undercut the market's responsiveness to consumer preferences.").

129. *See* Solove & Citron, *supra* note 12, at 757 ("Victims . . . may be forced to file for bankruptcy, and some may lose their homes. Victims may be turned down for loans . . . or [t]heir utilities may be cut off and their services denied.").

simply do not know what other information is out there for malicious actors to aggregate and use. Thus, if no remedy is provided for each illegally disclosed piece of information that contributes to the aggregation, but the aggregation that can produce harm is invisible to the law, no remedy will ever be provided.

When faced with large amounts of data, the average person is also not good at estimating the informativeness of each newly arriving piece of information.[130] In the context of one's online data, this means that individuals tend to underestimate the amount of privacy that they cede online to commercial parties.[131] The amount of data that can feasibly be collected in the information economy is exponentially larger than in the non-digital world.[132] People find it particularly difficult to understand how informative each piece of digital data that they release is about them.[133] They face an information overload.[134] As processing costs continue to fall, and as machine learning processing of personal data becomes more pervasive, the amount of information that can be inferred only increases, exacerbating this problem.

The aggregation/inference problem translates into three estimation mistakes, all of which lead people to face a larger privacy loss than they think they faced. The first is people's perceived number of clues. In the *Brown*-based example above, Arianna might give Google, say, five extra clues (five new pieces of information), mistakenly believing that she is giving away one. For example, she may use a Google sign-in for gaytravel.com thinking that she is giving information about liking a company, but she is giving information (clues) about liking a company, her sexual orientation, her disposable income, the type of vacations that she likes, being a liberal, and friend group composition.[135]

The second estimation mistake relates to the informativeness of those clues. Users may provide platforms with several pieces of information knowing that

130. *See* Daniel Kahneman & Amos Tversky, *Subjective Probability: A Judgment of Representativeness*, 3 COGNITIVE PSYCH. 430, 444 (1972) (observing that "[t]he notion that sampling variance decreases in proportion to sample size is apparently not part of man's repertoire of intuitions").

131. Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471, 1488–97 (2018) (suggesting that individuals may mistakenly believe that another party's belief about their personal information does not change substantially when they provide that party with new information that is, in fact, informative); Strandburg, *supra* note 128, at 130–52 ("[I]t is nearly impossible for a consumer to estimate the increment in expected harm associated with a given instance of data collection.").

132. Cofone & Robertson, *supra* note 131, at 1490.

133. Strandburg, *supra* note 128, at 96 ("Internet users do not know the 'prices' they are paying for products and services supported by behavioral advertising because they cannot reasonably estimate the marginal disutility that particular instances of data collection impose on them.").

134. Cofone & Robertson, *supra* note 131, at 1490 (explaining that the amount of data that can feasibly be collected is exponentially larger in the digital world than in the analogue world, which leads individuals to not fully grasp how valuable digital data is and suffer from information overload).

135. *See* Ariana Tobin, *Facebook Promises to Bar Advertisers from Targeting Ads by Race or Ethnicity. Again.*, PROPUBLICA (July 25, 2018, 2:47 PM), https://www.propublica.org/article/facebook-promises-to-bar-advertisers-from-targeting-ads-by-race-or-ethnicity-again [https://perma.cc/5VCM-WPAM] (explaining that Facebook's software made it possible for marketers to tailor who saw Facebook ads by race, gender, nationality and other protected characteristics); Ariana Tobin & Jeremy B. Merrill, *Besieged Facebook Says New Ad Limits Aren't Response to Lawsuits*, PROPUBLICA (Aug, 23, 2018, 12:48 PM), https://www.propublica.org/article/facebook-says-new-ad-limits-arent-response-to-lawsuits [https://perma.cc/7LXG-SKML] (explaining how Facebook has 5,000 categories that enable the possibility of discrimination by advertisers).

they are doing so but mistaking their informativeness: Arianna may mistakenly believe that the effect of those pieces of information on Google's new and improved belief distribution is similar to the effect of giving it one piece of information. When considering whether to buy a Fitbit device, Arianna may think that her phone is tracking her location already so she might as well accept location tracking on a new app.[136] Arianna knows that she would be granting access to the data she produces to the creator of the application (Fitbit). Although she realizes that Fitbit can use this information to learn about her, she underestimates *how much* Fitbit can learn about her. She knows that she is only additionally giving away heart rate data, but she does not know that combining the watch and cellphone data from the app is informative of "mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity."[137] This may lead her to buy a Fitbit device to trace her runs when it may not be in her best interest to do so. In other words, she will underestimate her privacy loss, causing her to undervalue her private data.

The third is how the clues are aggregated. Arianna may not know how the data is combined with other data that she shares with Google. For example, if the two companies have a data sharing agreement, they are owned by the same parent company, or either of them sells information to a data broker.[138] That means that Arianna has an additional problem. She will mistakenly think that Google's knowledge about her does not change much when she provides the company with new information that, when aggregated, is informative. For example, in January 2021 Google bought Fitbit, which collects heart rate and location data from millions of people through watches and wristbands.[139] Google promised it will not aggregate its data with Fitbit data[140]—similar to Facebook's promise with WhatsApp a few years prior, before Facebook rescinded the promise.[141] In short,

136. *See* Ignacio Cofone, *Immunity Passports and Contact Tracing Surveillance*, 24 STAN. TECH. L. REV. 176, 203 (2021) (discussing a response to this common argument).

137. Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 93, 115–16, 120–21, 124 (2014) (introducing the concept of sensor fusion and arguing that, when sensors are connected "everything reveals everything").

138. Dan Milmo, *Facebook and Instagram Gathering Browsing Data from Under-18s, Study Says*, GUARDIAN (Nov. 16, 2021, 4:34 AM), https://www.theguardian.com/technology/2021/nov/16/facebook-and-instagram-gathering-browsing-data-from-under-18s-study-says [https://perma.cc/B3YG-WX9D] (explaining Facebook and Instagram's parent companies' data gathering efforts).

139. Heather Landi, *Google Closes $2.1B Acquisition of Fitbit as Justice Department Probe Continues*, FIERCE HEALTHCARE (Jan. 14, 2021, 10:56 AM) https://www.fiercehealthcare.com/tech/google-closes-2-1b-acquisition-fitbit-as-justice-department-probe-continues [https://perma.cc/2MKD-XX3Z] (discussing the history of the acquisition).

140. Natalie Gagliordi, *Google's $2.1 Billion Purchase of Fitbit Is Complete*, ZD NET (Jan. 14, 2021), https://www.zdnet.com/article/googles-2-1-billion-purchase-of-fitbit-is-complete/ [https://perma.cc/69G7-52J7] ("Google said its interest in Fitbit 'has always been about devices, not data', and that it remains committed to protecting Fitbit users' privacy.").

141. Chris Smith, *Facebook Practically Forces WhatsApp Users to Share Data with Facebook*, BGR (Jan. 7, 2021, 6:50 AM), https://bgr.com/2021/01/07/whatsapp-privacy-policy-change-data-sharing-facebook/ [https://perma.cc/F4C8-SKY7] ("When Facebook announced plans to purchase WhatsApp several years ago, it promised not to link user data between the two services. It turned out to be a lie, as Facebook initiated a process to link accounts just two years later.").

she will mistakenly think that Google cannot learn much from the new information. As a result, she will be willing to give up her personal information too easily and may agree to grant Google better access to her target information without knowing it.

A combination of the three estimation problems is present in *Patel v. Facebook*.[142] Facebook's ability to use artificial intelligence to ascertain individuals' unique facial features based on innocuously added pictures to their Facebook pages was alarming to members of the class because they ignored (i) the amount of information about their facial features that they were providing Facebook by uploading pictures featuring their face in different angles and lighting, (ii) how informative each of those pictures were regarding their facial features, and (iii) how Facebook could analyze them through machine learning to elicit their biometric profile.[143] More broadly, the case illustrates tech giants' ability to harness information about everyday users that, on the surface, seems unlikely to be exploited: for Arianna, her Fitbit data, and for Patel, sharing a memory online for his friends to see.

In these three situations, companies' probability distributions about a person become tighter than what the person believes them to be. As a consequence, people will systematically underestimate their privacy harm for each piece of information they give away.[144] The consequence of this underestimation is that individuals tend to give away their personal information too easily.[145]

This idea ties back to *Meyers* and *Kirchein.* Printing a full credit card number instead of its last four digits, or printing the expiration date together with the last four digits, may seem harmless in isolation. But, if businesses are not sanctioned for breaching FACTA in such a way and a malicious actor can hack the systems of a few restaurants, that may make it easier for them to duplicate credit cards.[146] If that happens, it will be extremely difficult for consumers to trace back the duplicated credit cards to the aggregation of different pieces of extra credit card information from the different restaurants.[147] Because of the issue of aggregation, it is problematic that courts dismiss claims for harm only on the basis of one piece of information, given that the harm is in the aggregation of information—which is untraceable once aggregated.

While *Meyers* and *Kirchein* exemplify this problem for leaked information, the same problem is present for the collection of information. Lawsuits against

142. *See generally* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

143. *Id.* at 1272–73.

144. Cofone & Robertson, *supra* note 131, at 1490 (explaining that individuals are likely to underestimate their privacy loss when giving away new information, causing them to undervalue their private data).

145. *Id.*; Strandburg, *supra* note 128, at 95 (arguing that it is misleading to say that internet users "pay" for goods and services with their data because there is no functioning market for personal information exchanges).

146. *See, e.g.*, Meyers v. Nicolet Rest. of De Pere, Inc., 843 F.3d 724, 725–26 (2016) ("Congress enacted the FACTA in response to what it considered to be the increasing threat of identity theft. The provision at issue here was intended to 'reduce the amount of potentially misappropriateable information produced in credit and debit card receipts.'" (quoting Meyers v. Oneida Tribe of Indians of Wis., 836 F.3d 818, 820 (7th Cir. 2016))).

147. Solove & Citron, *supra* note 12, at 756–57 ("A problem is that fraud may not surface until after an identity thief combines leaked personal data with other information.").

Clearview AI, currently in early stages, serve as an example.[148] Clearview AI runs a facial recognition program on (mostly) publicly available images.[149] Its argument is that, because those images were publicly available, their collection and processing does not invade individuals' privacy and, moreover, it is a First Amendment protected activity.[150] But people's privacy loss is substantively different when images about them are publicly available than it is when they are individually identified from their facial features based on a machine learning process that produced information about them (their biometrics) based on those images.[151] Performing the privacy loss analysis based on the collected information (the images) as opposed to all the information (the images and the biometrics) misses the mark.

If courts only consider the specific piece of collected or leaked information in a case where information can be aggregated, they will overlook the magnitude of privacy loss—and the risk of consequential harms. Instead, courts must keep the problem of aggregation and the context of the digital domain present—considerations that are seemingly missing in most case law.

The next subsection introduces another problem that is relevant for courts in assessing privacy loss: disclosures to third parties.

D. Disclosure to a Third Party: Frank v. Gaos

The case *Frank v. Gaos* highlights an additional layer to the privacy loss conundrum.[152] Google allegedly leaked information about users' search terms to third parties, providing websites with users' personal information, as well as informing them of the search terms that led the users to their website.[153] The plaintiffs alleged that the collection and unauthorized disclosure led to feelings of being under surveillance.[154] This led to what seems to be a disagreement between the Supreme Court, who questioned standing at length before remanding, and the District and Circuit courts, who granted standing.[155]

Imagine that Arianna was also part of the *Frank* class, and Google sold information about Arianna to a third party—something that, if it satisfies its publication requirement, could be actionable under the tort of public disclosure of private facts.[156] These private facts are clues about Arianna that the third party

148. Complaint at 1, Am. C.L. Union v. Clearview AI, Inc., No. 2020 CH 04353 (Ill. Cir. Ct. May 28, 2020).

149. *Id.* at 1–2.

150. Defendant's Memorandum of Law in Support of Its Motion to Dismiss at 18, Am. C.L. Union v. Clearview AI, Inc., No. 2020 CH 04353 (Ill. Cir. Ct. Oct. 7, 2020) (citing *U.S. v. Khan*, No. 15-cr-286, 2017 U.S. Dist. LEXIS 82493, at *19–20 (N.D. Ill. May 31, 2017)).

151. *See* Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC NEWS (Mar. 17, 2019, 10:25 AM), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 [https://perma.cc/SVJ2-4DPJ].

152. *See generally* Frank v. Gaos, 139 S. Ct. 1041 (2019).

153. *Id.* at 1044.

154. *See id.*

155. *Id.* at 1045–46; *In re* Google Referrer Header Priv. Litig., 465 F. Supp. 3d 999, 1013 (N.D. Cal. 2020).

156. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 392–98 (1960) (discussing the requirements for the public disclosure of private fact tort); Whitney Kristen McBride, Comment, *Lock the Closet Door: Does*

gained.[157] By giving these clues to the third party, Google is allowing *the third party* to reduce the standard deviation of *her* probability distribution about Arianna. Because of that increase in certainty, Arianna will face privacy loss. However, Arianna's privacy loss will be to the third party rather than to Google. Google's knowledge (its belief distribution) remains unchanged, since the act of disclosing private facts to the third party did not cause it to learn anything new about Arianna.[158] Under the privacy tort, however, Arianna's claim is against Google, not the third party.[159] Although the loss of privacy is to the third party, it is Google that caused Arianna's loss. It is therefore appropriate for Google to be the party to compensate Arianna.

This leads to a distinction for privacy tort law: the key difference between an intrusion tort and a public disclosure tort is *whose* bell curve is narrowed by the information.[160] When committing an intrusion, the perpetrator improves or aims to improve the probability curve of its knowledge about the target person.[161] When publicly disclosing, the perpetrator narrows the probability curve of a third party. In both cases, the blameworthy party, and thus the defendant, should be the perpetrator. But the type of loss that must be shown by the plaintiff differs.

The Grindr investigation and sanctions illustrates this distinction's applicability.[162] In the case, Grindr already had the information about its users' interest in sex with men and, for some of them, their HIV status.[163] It would be wrong to argue that, because Grindr's belief remained uncharged, these users had no privacy loss when Grindr shared that information with third parties. While the probability distribution of Grindr with regards to such users' information was already tall and narrow, the probability distribution of the third parties towards them was short and wide.[164] Sharing that information produced privacy loss for Grindr users because, after acquiring the information, the probability distributions of the third parties improved.[165] Grindr's knowledge, in other words, remained the same, but the third parties became more certain due to Grindr's actions.

Because the key difference between an intrusion tort and a public disclosure tort is *whose* bell curve is narrowed by the information, the Grindr case would be a candidate for a public disclosure tort. Grindr narrowed a third party's probability curve with respect to sexual orientation and HIV status of the Grindr

Private Mean Secret?, 42 MCGEORGE L. REV. 901, 904–08 (2010) (discussing the public disclosure of private facts tort and how what is considered a private fact is context-dependent and that certain categories of true facts are different than others).

157. *See* discussion *supra* Sections III.A–B.
158. Cofone & Robertson, *supra* note 80, at 1059–60.
159. *Cf. id.*
160. *Id.*
161. *Id.*
162. EUROPEAN DATA PROT. BD., *supra* note 114.
163. *See id.*
164. See *supra* Section III.B for an explanation of probability distributions.
165. See *supra* Section III.C for more information about probability distributions.

users included in the database.[166] Because Grindr's probability distribution is irrelevant to this loss, users should not have to show illegitimate collection.

How is this helpful for *Frank v. Gaos*? It illustrates that the plaintiffs in the case faced privacy loss. It also illustrates that Frank's privacy loss was vis-à-vis the third-party website and it was caused by Google. To privacy interests, it is irrelevant that Google already had the information (that it was "out there") and it is also irrelevant that Google obtained the information lawfully. Doing an intrusion-type analysis in *Frank v. Gaos* (*i.e.*, asking whether the information was already public or asking if the collection was legitimate) is thus asking the wrong question. Instead, to adequately account for the privacy interest involved, a disclosure-type analysis should be performed: asking whether the information disclosure produced privacy loss and whether Google had the right to disclose.

E. Moving Past Binary Uses of "Loss of Privacy"

A key takeaway from this Part is that privacy loss is not binary. It exists on a continuum. People's privacy can decrease by different magnitudes, which depend on the informativeness of the clues that other people learn. People's privacy can also increase by different magnitudes.

Thinking of privacy loss as existing on a continuum is a useful way for courts to think about privacy for two reasons. The first is that it captures intuitions about privacy better than binary views where people either have or do not have privacy.[167] When Google gains more knowledge about Arianna, it is false to say that Arianna no longer has *any* privacy—as it is to say that she had perfect privacy before. But it is also incorrect to say that nothing happened to her privacy. Privacy loss is about Arianna's level of privacy dropping from one level to another.[168]

This idea has become increasingly important to recognize. In the age of algorithms, there are recidivist privacy invaders in a way that daily social interactions lacked before. A binary conception of privacy might have been adequate for a world where a person could open only one of your letters (a single intrusion) and publicize its contents (a single disclosure), but it would be unlikely to go much beyond that. That same person was unlikely to open and disclose many more of your letters in the future because it would be difficult for them to have the resources to do so. In contrast, we now all have repeated and ongoing interactions with actors that reduce our privacy, making a continuous concept of privacy loss paramount. Privacy loss, for this reason, is a particularly apt foundation for privacy harms in the digital sphere.

Second, viewing privacy in a nonbinary way better captures the tradeoffs that exist for people regarding their losses of privacy—such as gains in intimacy. Binary conceptions of privacy restrain courts to only two possible readings of

166. See *supra* Section III.C for more information about probability distributions.

167. Cofone & Robertson, *supra note* 80, at 1052–53 (explaining that privacy loss is about moving between levels of privacy).

168. *Id.* at 1053.

the world: there was a violation of privacy or there was no violation of privacy. This impedes courts from evaluating grey areas, which require the more nuanced analysis that this Article's framework can offer.[169] Accounting for continuity is paramount because most privacy cases that get to court, like *Urban Outfitters*, *Patel*, *Six Flags*, *Meyers*, *Kirchein*, *Frank*, and the Grindr investigation, involve grey areas. Cases that make it to court involve different gradations of privacy losses and some of them, but not all, may involve required privacy harm.[170] While any continuous view needs line-drawing—for example, understanding that levels of care exist in a continuum but setting a negligence standard—continuity makes a difference. A binary view of privacy interests would force courts to grant standing in all of them or none of them.

After identifying plaintiffs' privacy loss, the relevant step that remains in these cases is to identify whether the plaintiff's privacy loss constitutes privacy harm and, in turn, an actionable privacy injury. The next part addresses this question. As this Part has introduced a framework of privacy loss including two often overlooked aspects that courts should be alert to (aggregation and third parties), the next Part proposes how courts should identify which subset of privacy losses provide a basis for standing.

IV. STEP 2: HOW COURTS CAN IDENTIFY PRIVACY HARM

A. Moving from Privacy Loss to Privacy Harm

When do people suffer privacy harm? Privacy loss, in this framework, identifies when someone faces a reduction of their privacy. But federal courts are not concerned with reductions of privacy unless they constitute harm to a privacy interest. The considerations presented so far about privacy loss have been descriptive. But privacy harm is normative. Privacy harm lies at the core of Article III requirements under Supreme Court case law.

The endeavor of identifying privacy harm is determinative of standing and remedies. As Ryan Calo puts it: "Describing the outer boundaries and core properties of privacy harm helps to reveal values, identify and address new problems, and guard against dilution."[171]

Privacy's different normative conceptions allow building this second step and determine, among situations that produce privacy losses, which ones produce privacy harm. Daniel Solove famously identified six ways to conceptualize privacy: as the right to be let alone, autonomy or the limited access to the self, secrecy or concealment of discreditable information, control over one's personal information, personhood and preservation of one's dignity, and intimacy and the

169. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 131–36 (2004).

170. *See, e.g.*, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1200–01 (Ill. 2019); Hancock v. Urban Outfitters, Inc., 830 F.3d 511, 512 (D.C. Cir. 2016).

171. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1142 (2011) (offering an account of the contours and mechanics of privacy harm, suggesting that privacy harms fall into two categories).

promotion of relationships.[172] These normative conceptions reflect the social values that relate to privacy and that privacy protects.[173]

Some privacy losses violate these values, but not all of them do. The Grindr users that had their sexuality and HIV status information leaked had their intimacy violated,[174] as well as their autonomy.[175] *Spokeo* class members lost control over their personal information when the company portrayed false information about them to employers.[176] Class members in *Brown* lost their limited access to the self with Google's stealthy tracking.[177]

People cannot suffer privacy harm without facing privacy loss. But they can certainly face privacy loss without suffering privacy harm. Sharing with friends that I have no plans this Friday evening, for example, is a privacy loss, but does not produce, by itself, privacy harm.

Relatedly, the idea that privacy losses exist along a continuum (rather than as a dichotomy) allows courts to account for the fact that losing a small amount of privacy is different from losing a significant amount of it. For example, Arianna may suffer a small privacy loss if Google finds out something about her, such as her favorite travel destination, and if Google knows nothing else about her. But the same clue could produce a large privacy loss if Google already knows a lot about Arianna (its probability distribution is tall and narrow). This difference in magnitude could determine whether Arianna suffered privacy harm.

People's preferences and expectations over privacy losses are also relevant to separate privacy losses that do not constitute harm from privacy losses that do. And this will vary depending on context. Revealing someone's sexual orientation can be irrelevant or even desirable for some people and intrusive or upsetting for others—even without leading to negative external consequences. Similarly, the same person may find it to be a harmless loss of privacy to share that same information with a close group of friends but find it upsetting if people at their workplace or church found out. People have an intrinsic desire for privacy that is tied to privacy's normative conceptions.[178]

172. Daniel Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1092 (2002).

173. *See id.* at 1099–1121.

174. *See* Stefanie Roehrs, *Privacy, HIV/AIDS and Public Health Interventions*, 126 S. AFRICAN L.J. 360, 369 (2009) ("Most people would consider their HIV status to be a private affair, because due to the way of transmission and the lack of a cure, HIV is a condition related to sex, death and disease-topics that allude to the most existential aspects of life and are therefore perceived as highly intimate."); Joshua Blecher-Cohen, *Disability Law and HIV Criminalization*, 130 YALE L. J. 1560, 1570–77 (2021) (discussing intimacy-related claims).

175. *See* LAWRENCE GOSTIN, AIDS PANDEMIC: COMPLACENCY, INJUSTICE, & UNFULFILLED EXPECTATIONS 91–100 (2004) (discussing how HIV mandated disclosure clashes with privacy notions of autonomy); Tony Ficarrotta, *HIV Disclosure Laws Are Unjustified*, 24 DUKE J. GENDER L. & POL'Y 143, 152–63 (2017).

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

177. *See* Brown v. Google LLC, 525 F. Supp. 3d 1049, 1055 (N.D. Cal. 2021).

178. Ignacio Cofone, *Nothing to Hide, but Something to Lose*, 70 UNIV. TORONTO L.J. 64, 65, 73 (2020) (demonstrating that while some individuals might value privacy because it allows them to conceal undesirable facts, individuals like privacy for its intrinsic value).

The fact that people desire privacy for privacy's own sake does not impede that they can sometimes seek privacy instrumentally.[179] For example, people sometimes pay with cash when they do not want a purchase recorded, for example when purchasing marijuana in a state where it is legal—but knowing it could get them in trouble federally in the future. This choice could be driven by an intrinsic desire to keep their marijuana use private, an instrumental desire to avoid problems with the federal government in the future, or a combination of both.

Privacy's normative elements are determinant of whether cases like *Urban Outfitters* and *Patel* can be distinguished. In these terms, one can find one relevant difference between the two cases. In *Patel*, the information was processed without valid consent.[180] But in *Urban Outfitters*, while the financial information request was illegal, it was not asked in a context of coercion or power asymmetry that would deprive the plaintiff from their autonomy or their choice not to provide the information.[181] Treating these cases differently was thus defensible from a purely normative standpoint. What is incorrect is the reasons for which they were considered different. And this error is hugely consequential.

B. Privacy Harm through Contextual Integrity

Above, it was explained that factors such as loss of autonomy and breach of social norms in producing privacy loss form a normative assessment over such loss.[182] These normative factors differentiate between privacy loss and privacy harm.

From the last subsection, a reader may wonder: "how can a court know whether a loss has been harmful to that person when assessing a plaintiff's claim?" This is for federal courts a necessary step to determine whether the harm (if any) is a cognizable injury.[183] The existence of privacy harm depends on what Helen Nissenbaum has named the contextual integrity of the information acquisition, use, or distribution.[184] Privacy's normative values are breached when the contextual integrity of information is breached.

Privacy social standards or, in other words, what is socially acceptable, are determined by social norms.[185] These social norms vary depending on who are the actors involved in the information collection or disclosure, in what context they do so, what type of information is involved, and through which means the information is transmitted.[186] Social norms distinguish some types of privacy

179. *Id*. at 71–80 (demonstrating that privacy can have an intrinsic or an instrumental value).
180. Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019).
181. *See* Hancock v. Urb. Outfitters, Inc., 830 F.3d 511, 512 (D.C. Cir. 2016).
182. *See supra* Section III.A.
183. *See infra* Section IV.C.
184. Nissenbaum, *supra* note 169, at 136–57.
185. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 132–47 (2009) (explaining contexts, informational norms, actors, attributes, and transmission principles); Helen Nissenbaum, *Contextual Integrity Up and Down the Data Food Chain*, 20 TH. INQ. L. 221, 224–28 (2019).
186. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 185, at 140–47.

invasions from others in terms of what is deemed socially acceptable to do, as explained in the last subsection. As Helen Nissenbaum explains, "what makes us indignant, resistant, unsettled, and outraged in our experience of contemporary systems and practices of information gathering, aggregation, analysis, and dissemination is not that they diminish our control and pierce our secrecy, but that they transgress context-relative informational [social] norms."[187]

People's reasonable expectations of privacy depend on what that information is, who is involved (who shares the information and who receives it), and how it is communicated.[188] Those three parameters, together, determine the information flow and its appropriateness. The social norms that the contextual integrity framework describes encompasses people's expectations.

The first relevant factor to determine harm is the type of information. For some types of information, Arianna's disutility regarding privacy will be flat, rather than decreasing, if Arianna does not care who learns about it.[189] This could overlap with information that a lot of people have already, like her gender. But it does not necessarily have to be information that a lot of people already have: she could also not care if lots of strangers find out that she is married when the event just happened and no one knows yet.

Even more, under some circumstances, such as to correct a misconception, someone might even find a loss of privacy desirable.[190] Recall the problem that Robins faced in *Spokeo*, where the website displayed false information about people's education and employment history.[191] When potential employers received this misleading information (false clues), their probability distribution about Robins did not improve. The false clues either widened employers' probability distribution, making them less certain about Robin's true characteristics, or they shifted the mean of their probability distribution, leading them to believe false things about Robins (i.e. the distribution did not become tighter or it became tighter around the wrong value).[192] Robins would have been better off had Spokeo disclosed nothing about him. But, conditional on Spokeo having done it, and on courts doing nothing about it, Robins's best strategy is to tell employers more about his true characteristics, correcting the error. Doing so, technically, produces a loss of privacy (because employers know more about

187. *Id.* at 186.

188. *Id.* at 129–58 (explaining contexts, informational norms, actors, attributes, subject, and transmission principles); Nissenbaum, *Contextual Integrity Up and Down the Data Food Chain*, *supra* note 185, at 228–31 (explaining actors, types of information, and transmission principles); Helen Nissenbaum, *Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't*, in THE FUTURES OF PRIVACY 19, 23–25 (Carine Dartiguepeyrrou ed., 2019) (describing the parameters as actors, information types, and transmission principles).

189. Cofone & Robertson, *supra* note 80, at 1055.

190. Note that, for the contextual integrity framework, this is not a reduction in privacy.

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

192. It is also worth distinguishing between Arianna's preferences over privacy and her preferences over the clues. Both are preferences over her personal information, but they behave differently in that Arianna the latter affect Arianna's wellbeing only to the extent that they affect the former. Cofone & Robertson, *supra* note 80, at 1051–52 (explaining that the informativeness of clues depends on the other clues one has previously received, and some clues may not be informative).

him) but a gain in employment prospects and no privacy harm from the second disclosure.

The second factor is who is involved—the information sender, recipient, and who it is about. Beyond her interactions with Google, Arianna's wellbeing also depends on the observer's identity. Arianna might experience no loss of wellbeing from her partner learning something about her, such as the time she leaves for work every morning, but she might experience a significant loss of wellbeing if a complete stranger learned the same information about her. In some contexts, people like to share details about themselves with others. For example, someone might enjoy sharing details about their day with their spouse or friend, and it might make them happy sensing that their loved ones know them well (*i.e.*, have a clear sense of their target information).

The third factor is comprised of the conditions under which the information was collected, used, or shared. For many interactions, the condition to make an information flow appropriate is the subject's consent.[193] Data breaches, for example, are inappropriate information flows because they were not authorized.[194]

Similarly, the baseline information to which someone aggregates new collected information forms part of the relevant context: the more Google already knows about Arianna, the less effect the same clue will have on the standard deviation of its probability distribution. As a result, while the first few clues when Arianna has a lot of privacy affect the standard deviation a lot, Arianna's preferences are such that a reduction in standard deviation from a high-privacy starting point has a smaller effect on her wellbeing (i.e. not be harmful). This effect may be small because, at that point, she has a lot of privacy. In other words, even if subsequent clues are less informative than the first, they tend to be more harmful.[195]

Courts can determine reasonable expectations of privacy over information by identifying normative values.[196] The normative value assigned to the loss of one type of information, compared to other types, works as an objective standard. To build this standard, courts do and should consider context. For instance, gender is a type of information that, subject to privacy loss, could be harmful to someone who is transgender if a court considers this context (*e.g.*, the plaintiff not wanting their assigned sex at birth to be revealed). One might focus on the reduction in wellbeing that is privacy harm (rather than the privacy loss) because

193. Nissenbaum, *Contextual Integrity Up and Down the Data Food Chain*, supra note 185, at 230.

194. *See* Lior Strahilevitz & Lisa Yao Liu, *Cash Substitution and Deferred Consumption as Data Breach Harms* (forthcoming in 2022). This would be conceptualized by contextual integrity as the transmission principle requires authorization.

195. Depending on one's conception of privacy, one may have a different reading of the meaning of privacy loss and privacy harm. A proponent of the privacy as secrecy or control approach might see the concept of privacy as the reduction in the probability distribution equivalent to a privacy loss, independent of the person's wellbeing. When Google learns more about Arianna, she has less secrecy and less control over her information, even if her wellbeing does not diminish from this loss.

196. *See* Nissenbaum, *Contextual Integrity Up and Down the Data Food Chain*, *supra* note 185, at 231–34 (explaining ethical and political values together with contextual functions, purposes, and values).

this reduction indicates that, given the context, information flowed in a socially inappropriate manner. In the example above, if Arianna's friend learns more about her purchasing habits and, understanding what this means, she does not mind it, this could be taken to imply that her friend learned the information through a socially appropriate channel.[197]

This type of harm identification allows for substantive redress while it addresses the prevalent concern that recognizing federal privacy standing when nonprivacy injuries are absent may lead to overlitigation.[198] This policy concern was presented, for example, in the U.S. Chamber of Commerce amicus brief in *Spokeo*, which deceivingly argued: "There are dozens of federal laws similar to the one at issue here, all of which could be read to authorize suit against businesses by plaintiffs who have suffered no actual, concrete, or particularized injury."[199] It was also present in the amicus briefs from technology companies such as Facebook, Twitter, and Google, who falsely argued that the Ninth Circuit makes them susceptible to being sued by millions of people when there is no injury.[200] The Supreme Court echoes the concern in *TransUnion v. Ramirez*, where it compares granting standing for FCRA breaches to a hypothetical law that would allow anyone to sue polluters for unclean air or water regardless of whether they were injured by it.[201] Scholars such as Sara Spiekermann, likewise, have indicated that "[c]ommon market practices, such as the aggregation of personal data, identification, secondary use, exclusion, and decisional interference are all recognized privacy breaches according to Solove's taxonomy. This seems to be a dilemma."[202]

Doctrinally, and linked to this policy concern, the distinction can separate statutory violations that are considered "merely procedural" under *Spokeo* and those that are not.[203] *Spokeo* suggested that, while a statutory violation that is substantive may be sufficient for standing, a violation of a statute's procedural requirement may not automatically grant standing.[204] According to some, following *Spokeo*, standing may depend on the category of right Congress intended to grant when enacting the right at issue under a statute (*e.g.*, statutory enforcement right, procedural decision-making right, a right arising from the

197. The contextual integrity heuristic leads to assessing information flows' merits as a function of their meaning and significance in relation to the aims, purposes, and values of the context. *See generally* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 185.

198. Brief of the Chamber of Commerce of the United States of America and the International Association of Defense Counsel as Amici Curiae in Support of Petitioner at 6, Spokeo v. Robins, 578 U.S. 330 (2016) (No. 13-1339).

199. *Id.*

200. Brief for Amici Curiae Ebay Inc., Facebook, Inc., Google Inc., and Yahoo! Inc. Supporting Petitioner at 3, Spokeo v. Robins, 578 U.S. 330 (2016) (No. 13-1339).

201. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2207 n.3 (2021). *Cf.* discussion *infra* Section VI.B.

202. Sarah Spiekermann, Alessandro Acquisti, Rainer Bohme & Kai-Lung Hui, *The Challenges of Personal Data Markets and Privacy*, 25 ELEC. MKTS. 161, 164–65 (2015).

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

204. *Id.* at 341.

denial of a statutory procedural right, or instrumental right).[205] The distinction between privacy loss and harms resolves the indicated dilemma because it distinguishes between different market practices that are privacy-reducing for individuals.

Perhaps counterintuitively, extending federal standing in such a way will not always be detrimental to corporations. *Marquez v. Google*, where Marquez sued Google in a putative class action alleging that Google Photo's facial recognition procedure violates BIPA, illustrates this idea.[206] In the case, Google alleged Marquez's particularized injury and Article III standing to move the case from an Illinois state court to a federal court,[207] while Marquez did not plead particularized harm and moved to sever and remand his claim to state court.[208]

Identifying what harms people is crucial for finding workable redress. Courts' fear that everything is believed to be privacy harm in theory risks that nothing will be taken to be privacy harm in practice. Failing to account for these two concepts, and its consequential inclusion of everything in theory and nothing in practice, is the problem that courts face when addressing harm in privacy.

C. Intrinsic and Consequential Privacy Harms

People face privacy loss any time they share information, but their overall wellbeing might still increase due to the benefits they obtain from the social connections produced.[209] Their wellbeing will crucially depend on how the receiver uses their information.[210] How a social network uses people's information, for example, may constitute privacy harm, and there may be other harms that were enabled due to that loss in privacy.[211]

Harms that are enabled by a loss of privacy have recently been the subject of rich scholarly literature that explains the wide array of harms that privacy

205. Jon Romberg, *Trust the Process: Understanding Procedural Standing Under* Spokeo, 72 OKLA. L. REV. 517, 571 (2019) ("In other words, what makes a statutory right "procedural" in the sense advanced by Spokeo is that it is instrumental, which means it is intended to protect some distinct interest other than the denial of the right itself. Congress grants instrumental rights (mandating or forbidding certain conduct by statute) not because of the harm caused by violation of that instrumental right – violation of the instrumental right itself, with nothing more, ordinarily causes no real-world harm – but because Congress has concluded that granting the instrumental right serves to protect against risk to a distinct, real-world, target harm. That is, the instrumental right is enacted for the instrumental purpose of protecting against the concrete, target injury.").

206. Marquez v. Google LLC, No. 20C4454, 2020 WL 6287408, at *1 (N.D. Ill. Oct. 27, 2020).

207. *Id.* at *2 ("Google argues that remand of Marquez's BIPA § 15(a) claim is inappropriate because Marquez alleges that Google failed to comply with BIPA § 15(a)'s deletion requirements and thereby pleads a violation of individual privacy rights sufficient for Article III standing. (Dkt. 15 at 1).").

208. *Id.* at *2 ("Marquez moves to sever and remand his claim under BIPA § 15(a) to state court for lack of Article III standing. (Dkt. 11).").

209. *Cf.* CARISSA VELIZ, PRIVACY IS POWER (2020) (arguing that data collection is always harmful, and that it would be beneficial for individuals and for the economy to ban the practice).

210. *See* Ignacio Cofone, *Beyond Data Ownership*, 43 CARDOZO L. REV. 501, 534-8 (2021).

211. *Id.* at 1054 (explaining how privacy losses can lead to other losses that stem from the initial privacy loss).

violations can produce.[212] Ryan Calo has called the latter "objective" privacy harms.[213] In Calo's words:

> Objective privacy harm is the actual adverse consequence—the theft of identity itself or the formation of a negative opinion—that flows from the loss of control over information or sensory access. Subjective privacy harm is, by and large, the perception of loss of control that results in fear or discomfort.[214]

I refer to these as consequential harms because they are harms that are external to privacy interests but occur as a consequence of privacy violations. They fall outside what I have defined as privacy harm because they do not attack a privacy interest. Rather, they affect other important interests, such as financial or reputational.[215] They are, thus, nonprivacy harms that pertain to privacy law because they also accrue due to the collection, use, or dissemination of personal information. While recent scholarly work persuasively groups them together as privacy harms so as to explain to courts the importance of recognizing them,[216] I believe the distinction can better provide redress while navigating constitutional harm requirements.

To clarify the distinction with an analogy, recall the tort of battery. The fact that the tort of battery chiefly protects one's physical integrity does not render all harms that battery can cause 'physical harms.' An act of battery can cause emotional and psychological harms if the injury or the circumstances were severe enough; most tort law scholars would consider it imprecise to refer to those emotional and psychological harms as physical harms just because they were caused by battery. Similarly, the fact that the torts of intrusion upon seclusion and public disclosure of private facts chiefly protect a privacy interest does not mean that all the harms that an intrusion or a disclosure can cause are privacy harms: intrusions and disclosures can harm one's privacy interest as well as one's financial and reputational interests, among others.

Recognizing privacy harm also when consequential harms are absent is beneficial from a doctrinal and an enforcement perspective. From a doctrinal perspective, relying solely on consequential harms for standing will often run afoul of the de facto requirement for injuries at the federal level established by the Supreme Court, meaning that an injury must already exist for it to be concrete,[217] because they rarely arise at the moment of the privacy loss.

The enforcement benefits exist independent of the type of court involved. Because consequential harms often materialize later on, requiring consequential harm to recognize privacy harm is problematic from a policy perspective. The increased risk of consequential harms may be difficult to prove ex-ante. Once consequential harms do materialize, causality is difficult to establish. For that

212. Citron & Solove, *supra* note 14.
213. Calo, *supra* note 171, at 1143.
214. *Id.*
215. Citron & Solove, *supra* note 14.
216. Citron & Solove, *supra* note 14.
217. Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016).

reason, requiring consequential harms risks leading to injuries being frequently left unaddressed.[218] Omri Ben-Shahar, for example, famously discussed causation problems in privacy with analogies to environmental harm.[219] But these causation problems are specific to requiring consequential harms. Identifying (intrinsic) privacy harm overcomes those causation obstacles.

Therefore, courts should identify both intrinsic privacy harms and consequential harms so as to rely on both of them, and not on the latter to the exclusion of the former, to determine standing when a privacy violation is concerned.

V. STEP 3: WHEN HARM TURNS INTO ACTIONABLE PRIVACY INJURIES

A. Distinguishing Between Ordinary Privacy Harm and Actionable Privacy Injuries

The concept of privacy loss identifies when someone loses privacy; and the concept of privacy harm identifies when someone was harmed by such a loss. But adjudication requires a further normative component: evaluating which types of privacy losses harm individuals in a legally cognizable way and which ones do not.[220] The next distinction to make is thus between privacy harm and actionable privacy injuries.

Privacy injuries exist when privacy harm is coupled with a wrong, which is a question of statutory interpretation. Legally cognizable privacy harm, or actionable privacy injuries, thus, depends on normative factors. Courts undertake a normative judgment when they interpret statutes to decide which harms are actionable.[221]

William Fletcher illustrates this idea when explaining the nature of standing:

> Imagine two siblings who compare, as children will, the treatment they receive from their parents. If one child receives a new bicycle, the other child may complain if he does not also receive a new bicycle or some equivalent. A parent who has just bought a bicycle for one child is likely to say to the complaining child, 'It doesn't hurt you that I got a bicycle for your sister.' Of course, I am wrong if I say that. The child is feeling hurt. What I really mean, or should mean if I think about it, is that the child should not feel hurt; or that the child has no 'right' to feel hurt; or that I do not wish to recognize the feeling as a hurt (perhaps because if I so recognized it, I would feel some obligation to avoid doing what has caused it). The complaining child is invoking a sort of familial equal protection clause: What the parents give to one child, they must give to the other. The

218. *See supra* Section II.A.
219. Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104, 125–26 (2019).
220. *See* William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 231 (1988).
221. *See id.*

> parent, in denying that injury exists, is not denying the sense of injury but is, rather, denying the existence of such a family norm.[222]

An analogous example can take Fletcher's principle to the privacy realm. Ben and Caroline go to a club on a Saturday night and, there, they are seen by a coworker, who tells everyone at work about having seen them there. Caroline does not mind it, but Ben does. Both Ben and Caroline faced privacy loss. Unlike Caroline, because he minds it, Ben also suffered privacy harm, like Fletcher's hypothetical sibling. But Ben did not suffer an actionable privacy injury—a privacy loss that is legally cognizable. This is so not because his harm was anything less than real, but because the acquaintance, while potentially breaching a social norm, did not commit a legal wrong. Identifying this difference is significant for its policy consequences because distinguishing actions that are wrongs from those that are not resolves the fear of an overexpansive private right of action for privacy harm.[223]

The difference between ordinary privacy harm and (actionable) privacy injury cannot depend solely on the victim's interest—because the victim's interest is always affected by privacy harm. It depends on the (legal) wrongness of the act in question. Wrongness identifies whether a legally cognizable norm was breached by the pertinent harm.[224] Such legal wrongness will depend on what is normatively acceptable and what courts have previously decided to be actionable. For example, a data breach lawsuit arising from a hack has an evident wrongness from the malicious actor who hacked. But it will also have wrongness from the company, against whom the lawsuit is filed, when the company was negligent in securing its data sufficiently or failed to comply with a data breach notification mandate.[225]

What is the practical relevance of this distinction? Congress cannot do much to change how the Supreme Court interprets injury-in-fact requirements relevant to step 2, but it has wide discretion to recognize wrongness for step 3 when passing legislation. Lower federal courts, similarly, can interpret statutes in a way that recognizes a variety of harms, including privacy harm, granting redress under the Supreme Court's injury-in-fact restrictions.

B. Wrongness Recognized

The law can incorporate the social standards that define wrongness normatively through two pathways: legislatively and judicially.

The first pathway is when a statute identifies a wrong and recognizes standing to sue for such a wrong. For example, the FCRA, the FACTA, the Telephone Consumer Protection Act, the Video Privacy Protection Act, and the

222. *Id.* at 231–32 (explaining that the legal system's imposition of standards of injury by deciding which causes of action to recognize as valid legal claims is an inherently normative undertaking).

223. *See id.* at 233.

224. *See id.* at 232–33.

225. *See* John A. Fisher, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215, 218 (2013) ("[C]onsumers should have a negligence cause of action in cases of data breach.").

Driver's Privacy Protection Act all identify a wrong and grant standing to sue for such a wrong.[226] A breach of these statutes is a sufficient condition for wrongness—and, when Article III is not an obstacle, as is the case for state courts, it can be a sufficient condition for standing.

Circling back to the circuit split, such wrongness is what the Third, Sixth, Seventh, Ninth, Eleventh, and D.C. Circuits emphasize in their rulings: by granting standing in these statutes, Congress has stated that conduct in breach of them is wrong in a way that should be addressed by courts.[227] But the Second, Fourth, and Eighth Circuits are correct in pointing out that the existence of such wrongness from the defendant is different from the existence of an injury-in-fact from the plaintiff.[228]

The second pathway to incorporate these norms is when a court uses tort law to enforce a majoritarian standard embedded in a social norm or a social practice, absent a statute that explicitly adopts such norm or practice. That is, when a court decides "this privacy harm is socially significant and we will thus make it actionable."[229]

Relying on social norms in such a way is what the Supreme Court should have said in *Spokeo* instead of formulating its historical recognition requirement.[230] It is akin to applying a reasonable person standard for privacy.[231] Having statutes and courts rely on social practices means that one is not liable when one does something that, even though it produces privacy harm, a reasonable person would deem acceptable. Making all privacy harms actionable, on the other hand, would be akin to setting a strict liability standard: anyone who produces privacy harm would be liable for it. The latter—produced precisely by the lack of an intrinsic privacy harms theory—seems to produce courts' and corporations' fear of overlitigation.[232]

226. Daniel Townsend, *Who Should Define Injuries for Article III Standing?*, 68 STAN. L. REV. ONLINE 76, 79 (2015) (indicating the long list of major statutes implicated by *Spokeo*'s nonlegal harm argument); Peter C. Ormerod, *Privacy Injuries and Article III Concreteness*, 48 FLA. ST. UNIV. L. REV. 133, 142–49, 173–91 (2020) (listing the privacy statutes that identify a privacy injury which *Spokeo* undermines).

227. *See, e.g.*, *In re* Horizon Healthcare Servs., Data Breach Litig., 846 F.3d 625, 639 (3d Cir. 2017) ("[W]ith the passage of FCRA, Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm."); Church v. Accretive Health, Inc., 654 F. App'x 990, 994–95 (11th Cir. 2016) ("The FDCPA creates a private right of action, which Church seeks to enforce. . . . [T]his injury is one that Congress has elevated to the status of a legally cognizable injury through the FDCPA. Accordingly, Church has sufficiently alleged that she suffered a concrete injury, and thus, satisfies the injury-in-fact requirement.").

228. *See, e.g.*, Katz v. Donna Karan Co., LLC, 872 F.3d 114, 119 (2d Cir. 2017) ("[A] plaintiff's pleading must satisfy a two-part test for such an allegation to constitute a concrete harm: first, that 'Congress conferred the procedural right to protect a plaintiff's concrete interests' as to the harm in question, and second, that 'the procedural violation presents a "risk of real harm" to that concrete interest.'").

229. Kirsty Hughes, *A Behavioural Understanding of Privacy and Its Implications for Privacy Law*, 75 MOD. L. REV. 806, 814 (2012).

230. *Spokeo*, 578 U.S. at 340 ("whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts").

231. SCOTT SKINNER-THOMSON, PRIVACY AT THE MARGINS 8–44 (2021).

232. *See* Daniel J. Solove & Danielle Keats Citron, *Privacy Harms* (GWU Law School Public Law Research Paper No. 2021-11, 2021).

In sum, what transforms privacy harm into a privacy injury that is actionable is the behavior of the offending party—whether they committed a legal wrong. Courts can and should find those wrongs in statutory law and common law torts.

Legal wrongness is often clear in privacy cases: a breach of a privacy statute such as the FCRA, or the applicability of a recognized tort.[233] It is the privacy loss and harm elements that are most challenging for courts to identify.[234] As the cases above illustrate, it has been courts' recurrent mistake on both sides of the circuit split to answer the first question (was there a privacy loss?) and the second question (was there a privacy harm?) with the third question (would an eventual harm produced by this conduct be actionable?).[235] The result is hesitancy to recognize privacy interests and a systemic lack of remedy for people who had their protected privacy interest injured but have not faced, at least yet, a consequential injury.

This hesitancy problematically mirrors a long historical narrative in the common law. In comparison to damages for pecuniary loss or bodily harm, common law has historically and unjustifiably treated damages for non-pecuniary and non-physical harm, such as emotional harm or psychological injury, with skepticism—even when there is a clear legal wrong.[236] Like with privacy, the resistance has been that these harms "are less susceptible to a 'scientific" or itemized approach than are pecuniary losses."[237] And that "[t]ranslating pain and suffering or emotional distress into monetary terms poses tremendous problems of proof because, unlike the situation with property, no market exists to provide a standard for compensating a victim of such a loss."[238]

The causes of hesitation have tracked to privacy harm, which is also intangible and dignitary. According to Nancy Levit, for example, key reasons for this negative treatment have been fear of opening floodgates to litigation, how widespread emotional harm is in modern society, and a lack of tools and standards to evaluate the extent of the harm.[239] Damages for pain and suffering

233. *See* discussion *supra* Section IV.C.

234. *See* Ben-Shahar, *supra* note 219, at 126 ("It is the inadequate proof of harm, not of negligence, that precludes tort liability.").

235. *See* discussion *supra* Section IV.A.

236. Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 140–41 (1992). *See also* Martha Chamallas & Linda K. Kerber, *Women, Mothers, and the Law of Fright: A History*, 88 MICH. L. REV. 814, 814 ("This apparently gender-neutral hierarchy of values has privileged men, as the traditional owners and managers of property, and has burdened women.").

237. JAMIE CASSELS & ELIZABETH ADJIN-TETTEY, REMEDIES: THE LAW OF DAMAGES 193 (2000).

238. Stanley Ingber, *Rethinking Intangible Injuries: A Focus on Remedy*, 73 CALIF. L. REV. 772, 773–78 (1985).

239. Levit, *supra* note 236, at 142 ("Several concerns explain this caution: (1) emotional harm is less objectively verifiable than physical harm and therefore easier for an individual to feign, to exaggerate, or to imagine; (2) emotional harm can be widespread-a single act can affect a substantial population; (3) some degree of emotional harm is endemic to living in society, and individuals must learn to accept and cope with such harm; (4) giving legal credence to and permitting recovery for emotional harm may increase its severity; and (5) related to the prior concern, while mitigation may be important in minimizing this harm, there is little a legal system can do to encourage or enforce mitigation. These policy concerns often led courts to declare that actors had "no duty" to prevent pure emotional harm, except in some narrowly defined areas.")

in American law, however, have increasingly been recognized since the late 18th century,[240] without such policy concerns materializing. This diagnosis suggests that that courts may become more receptive to recognizing privacy harm if provided with a method, such as the one proposed here, to distinguish it.

The next step is to differentiate privacy harm from related harms with which it is usually claimed in court.[241] While these are often claimed together, the distinct nature of their interests warrants differential treatment because privacy harm can arise in the absence of others. The next Part offers such distinction.

C. Courts Should Distinguish Intrinsic Privacy Injuries and Consequential Injuries

The right to privacy is inextricably tied to values such as personal autonomy, dignity, and individuality.[242] It comes as no surprise then that the right to privacy is also inextricably tied to a host of other harms and injuries besides those that take place against a privacy interest. This relationship further increases the importance of recognizing standing for privacy injuries. As explained in the privacy law scholars' amicus brief in *Spokeo*: "Congressional authorization of statutory damages does not signal a lack of injury-in-fact. Rather, it represents congressional recognition of the difficulty of documenting that injury, given the structural characteristics of the offending conduct."[243]

Online interactions include a distinct set of harms in addition to privacy harms. Namely: reputational harm (*e.g.*, when employers find inaccurate information about a job candidate), financial harm (*e.g.*, with identity theft), discriminatory harm (*e.g.*, when a member of a nonvisible minority is "outed"), bodily harm (*e.g.*, when someone is doxxed and then harassed), and harm to autonomy (*e.g.*, when someone's personal information is used to manipulate them).[244] By distinguishing between them, courts can identify the pertinent injury to the case. Different injuries would and should have different probatory burdens for standing and compensation. Any of these injuries, not only those that are material, are and should be sufficient for conferring standing.

240. Joseph H King, *Pain and Suffering, Noneconomic Damages, and the Goals of Tort Law*, 57 SMU L. REV. 163, 170 (2004).

241. Anita L. Allen, *Privacy Torts: Unreliable Remedies for LGBT Plaintiffs*, 98 CALIF. L. REV. 1711, 1760–61 (2010) ("[T]he invasion of privacy tort and the infliction of emotional distress torts function more as friends than competitors. The intentional infliction of emotional distress tort commonly accompanies the invasion of privacy torts in lawsuits alleging wrongs of intrusion, publicity, and appropriation . . . ."); *see, e.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330, 333 (2016).

242. Solove, *supra* note 172, at 1116.

243. Brief of Information Privacy Law Scholars as Amici Curiae Supporting Respondent, p. 12, Spokeo, Inc. v. Robins, 578 U.S. 330 (2016) (No. 13-1339), 2015 WL 5261535, at *12.

244. Ignacio Cofone, *Online Harms and the Right to Be Forgotten*, *in* THE RIGHT TO BE FORGOTTEN: A CANADIAN AND COMPARATIVE PERSPECTIVE (Ignacio Cofone ed., 2020).

Online harms to reputation can be most serious when part of an effort of online abuse.[245] When women are victims, these often involve publicly accusing them of engaging in sex work or carrying sexually transmitted infections.[246] When queer people are targeted, online abuse often entails nonconsensual pornography or the victim's impersonation, for example to send people to their home or work looking for sex, as it happened in *Herrick v. Grindr*.[247] As Ari Waldman puts it, "online harassment is particularly pernicious because it is cheap, fast and permanent."[248]

The second type of related online harm is financial harm. A particularly grave example of online financial harm is identity theft enabled by stolen or leaked personal information.[249] But harms to people's finances go beyond identity theft.[250] Other examples of financial harm that people face are having their insurance premiums raised;[251] prices increased due to price discrimination;[252] and their credit score ruined, disadvantaging them when looking for a new home or a new job.[253] People subject to data breaches without identity theft switch from credit card transactions to cash payments and defer purchases, two harmful consequences.[254]

The third type is discrimination: when members of historically disadvantaged groups are unjustly treated differently due to their group membership in an online environment. The same technologies that amplify

245. Thomas E. Kadri, *Networks of Empathy*, 4 UTAH L. REV. 1075, 1081–83 (2020) (discussing the prevalence of digital abuse and recommending solutions to regulate this abuse).

246. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 35–55 (2014) (providing examples of cyber harassment against women).

247. Herrick v. Grindr LLC, 765 F. App'x 586, 588 (2d Cir. 2019) ("[Plaintiff] allege[d] that Grindr is defectively designed and manufactured because it lacks safety features to prevent impersonating profiles and other dangerous conduct . . . ."); *see also* Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 L. & SOC. INQUIRY 987, 992 (2019) (explaining that LGBTQ persons experience higher rates of nonconsensual image sharing online relative to the general population); Ari Ezra Waldman, *Queer Dating Apps Are Unsafe by Design: Privacy Is Particularly Important for L.G.B.T.Q. People*, N.Y. TIMES (June 20, 2019), https://www.nytimes.com/2019/06/20/opinion/queer-dating-apps.html [https://perma.cc/K262-TESJ] ("The frequency with which queer people using social media, generally, and mobile dating apps, in particular, amplifies the privacy concerns we face compared with the general population.").

248. Ari Ezra Waldman, *Cybermobs Multiply Online Threats and Their Danger*, N.Y. TIMES (Aug. 3, 2016, 10:06 PM), https://www.nytimes.com/roomfordebate/2016/08/03/how-to-crack-down-on-social-media-threats/cybermobs-multiply-online-threats-and-their-danger [https://perma.cc/2V47-6B65].

249. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1814–16 (2010) (explaining how financial injuries, including identity theft, have multiplied in the digital era).

250. Solove & Citron, *supra* note 12, at 764–74 (explaining the emotional harm arising from data breaches).

251. Citron, *supra* note 249, at 1815, 1834 (explaining how data leaks can determine and undermine one's insurability).

252. Vincent Conitzer, Curtis R. Taylor & Liad Wagman, *Hide and Seek: Costly Consumer Privacy in a Market with Repeat Purchases*, 31 MKTG. SCI. 277, 277–80 (2012) (providing insight into the relationship between privacy and price discrimination); Joost Poort & Frederik J. Zuiderveen Borgesius, *Does Everyone Have a Price? Understanding People's Attitude Towards Online and Offline Price Discrimination*, 8 INTERNET POL'Y REV. 1, 2 (2019) (showing how surveillance leads to personalized pricing and price discrimination); Frederik Zuiderveen Borgesius & Joost Poort, *Online Price Discrimination and EU Data Privacy Law*, 40 J. CONSUMER POL'Y 347, 358–63 (2017) (discussing how data protection law applies to price discrimination).

253. Solove & Citron, *supra* note 12, at 745 ("Data-breach victims might decline to search for a new home or employment since there is an increased chance that lenders or employers will find their credit reports marred by theft.").

254. Strahilevitz & Liu, *supra* note 194.

reputational harm can amplify discriminatory harm, for example when a platform allows its users to make decisions on the basis of race.[255] Likewise, marginalized communities often experience disproportionate surveillance—a discrimination harm that is connected to the harm of lack of privacy.[256] Indeed, regulations often block people's personal information to prevent discrimination.[257] For example, employment law forbids employers from asking female job candidates whether they intend to take a maternity leave,[258]and genetic nondiscrimination statutes prevent employers from acquiring genetic information about their employees.[259] When people's personal information is processed by decision-making algorithms, this also leads to distinct forms of algorithmic discrimination that have a larger scale than human discrimination and are often hidden behind promises of neutrality.[260]

The fourth is physical integrity. Online abuse often leads to cyber harassment or cyberstalking that includes physical harm, such as battery, or the threat of physical harm, such as threats of rape of death.[261] Online abuse often involves doxxing, which leads to subsequent abuse by others.[262] Particularly, online harms to physical integrity are disproportionately suffered by women.[263]

255. *See, e.g.*, Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1161–62 (9th Cir. 2008) (Plaintiff argued that Roommate was "effectively a housing broker doing online what it may not lawfully do offline" by asking questions to prospective subscribers regarding their sex, family status and sexual orientation, in violation of the Fair Housing Act).

256. Scott Skinner-Thomson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673, 1678 (2017) ("[P]erformative privacy helps highlight the disparate burden of surveillance on marginalized communities and identifies a collective form of political resistance.").

257. Ignacio N. Cofone, *Antidiscriminatory Privacy*, 72 SMU L. REV. 139, 140–47 (2019) (discussing the importance of regulating the acquisition of information to prevent discriminatory practices and offering a legal framework for identifying when acquiring information can lead to discrimination).

258. *Id*. at 156.

259. Jessica L. Roberts, *Protecting Privacy to Prevent Discrimination*, 56 WM. & MARY L. REV. 2097, 2101, 2146 (2015) (arguing that "[t]he Genetic Information Nondiscrimination Act (GINA) provides a useful example of the privacy/antidiscrimination symbiosis" and that violations of genetic privacy can be understood in antidiscrimination terms).

260. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677–93 (2016) (discussing how algorithms inherit and magnify the prejudices of decision-makers); Ignacio N. Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L.J. 1389, 1428 (2019) ("In algorithmic decision-making, classification schemes can be used to exacerbate inequality or disadvantage a protected category . . . .").

261. CITRON, *supra* note 246, at 5 ("In some cases, online abuse has resulted in just what victims' dread: rape and real-world stalking."); Mary Anne Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655, 655–56 (2012) (explaining that legal responses to sexual harassment in cyberspace must account for the "'multiple-setting' conception of sexual harassment that both moves beyond traditionally protected settings and explicitly acknowledges that sexual harassment in one setting can produce harms in another"); *see also* Ari Ezra Waldman, *Amplifying Abuse: The Fusion of Cyberharassment and Discrimination*, 95 B.U. L. REV. ANNEX 83, 85 (2015) ("As a means of 'outing' gay persons, cyberharassment also triggers an onslaught of potential discrimination in employment, housing, and the provision of health care. 'Outing,' or the revelation of another's identity, is a frequent element of cyberharassment targeting members of the LGBT community.").

262. Svana M. Calabro, Note, *From the Message Board to the Front Door: Addressing the Offline Consequences of Race- and Gender-Based Doxxing and Swatting*, 51 SUFFOLK UNIV. L. REV. 55, 57–60 (2018) (providing a detailed overview of the nature and history of doxxing).

263. Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1904–28 (2019) (highlighting how women throughout history have disproportionally experienced sexual-privacy invasions and how the digital era provides contemporary opportunities for sexual privacy invasions).

The fifth type of harm is online manipulation, which can be defined as the use of technology to "covertly influence another person's decision-making, by targeting and exploiting their decision-making vulnerabilities."[264] People's personal data, in particular, can be used to influence their decisions.[265] In recent years, for example, there have been reported cases of political campaigns meaningfully influencing voters' choices,[266] including the Cambridge Analytica scandal. More broadly, what Shoshana Zuboff calls "behavior modification," which relates to buying things people do not need or want,[267] has become a pervasive business model and central to the information economy.[268] For some, this online environment involves harms to autonomy of varying magnitudes.[269]

Delineating the boundaries of privacy harm as the last Part did is consequential, in part, because of its relation to other online harms. When a website makes a ghost profile with someone's name on it but that person lacks evidence of reputational harm, as it happened in *Spokeo*, courts are unsure of whether to grant her remedy.[270] The same is true when a credit bureau is hacked, as it happened in the Equifax breach,[271] when financial information was collected illegally, as it happened in *Urban Outfitters*, or when financial information is stolen, like it happened in *Bradix*, but victims lack evidence that this has caused them financial harm.[272] Likewise, that is true when women and queer people share compromising pictures that are then disseminated, as it happened in *Novak v. Simpson*,[273] where a woman's boyfriend showed naked pictures of her and a video at a fraternity and later texted them to his friends.[274] Recognizing the

264. Daniel Susser, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. 1, 1 (2019).

265. *See generally* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015) (arguing that ideas better develop away from surveillance or public exposure and privacy shelters people's ability to make their own decisions).

266. SIVA VAIDHYANATHAN, ANTISOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY 146–74 (2018) (discussing how big data influenced the 2016 U.S. presidential election); Frederik J. Zuiderveen Borgesius et al., *Online Political Microtargeting: Promises and Threats for Democracy*, 14 UTRECHT L. REV. 82, 83–92 (2018) (discussing the prevalence of online political microtargeting based on data analysis in the US and Europe).

267. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 9 (2019).

268. Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEO. INQ. IN L. 157, 172–73 (2019) (discussing the sustainability of the market-based manipulation argument); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003–18 (2014) (arguing that the future of market manipulation is one marked with corporations exploiting the limits of each consumer's ability to pursue their own self-interests).

269. Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 34–44 (2019) (discussing how a harm of online manipulation to one's autonomy is a threat to liberal democracy); *see also* Skinner-Thomson, *supra* note 256, at 1676 (arguing that privacy is also associated with freedom of speech).

270. Spokeo, Inc. v. Robins, 578 U.S. 330, 336, 349 (2016).

271. Editorial Board, *The Unfinished Business of the Equifax Hack*, BLOOMBERG OP., (Jan. 29, 2019, 7:30 AM), https://www.bloomberg.com/opinion/articles/2019-01-29/equifax-hack-remains-unfinished-business [https://perma.cc/46WM-PJT2] (discussing how the Equifax breach revealed the industry-wide flaws with consumer protection).

272. *See supra* Section III.A and *infra* Section VI.B.

273. Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 164–76 (2015) (demonstrating that privacy is especially important for marginalized communities, such as the LGBTQ community, because of its relationship with discrimination, dignity, and autonomy).

274. Novak v. Simpson, No. 6:18-CV-922, slip op. (M.D. Fla. Jun. 15, 2018).

existence of privacy harm in those situations also gives victims much needed redress for these other interests.[275]

As Lionel Smith explains, "[s]tanding in private law is usually uncomplicated inasmuch as it generally corresponds to the holding of rights."[276] This is because standing is a power to enforce rights—and the most common way to enforce them in common law.[277] No standing means unenforced rights.

VI. DOCTRINAL CONSEQUENCES FOR PRIVACY LAW

A. Expanding the Framework: Improving Tort Law

The considerations presented above have consequences for tort law as well. A reevaluation of the harm standards used in adjudicating privacy and related torts in light of the different harms presented above would improve redress. The main difference between the privacy tort and other related torts (such as libel, slander, and intentional infliction of emotional distress)[278] is that the privacy tort should not require the plaintiff to prove a separate harm other than harm to their privacy interest in order to obtain compensation.[279]

This leads to an evidentiary consideration. In cases involving the privacy tort, courts should evaluate whether privacy harm—and not necessarily another harm—is present. This question mirrors, in a different doctrinal context, the above discussion on the circuit split as to whether plaintiffs must show harm in addition to the statutory violation.[280] Should courts, in those cases, presume the existence of privacy harm, or should a plaintiff prove it like they would prove reputational or financial harm in other cases? A plaintiff must prove psychological harm in a claim of intentional infliction of emotional distress,[281]

275. CITRON, *supra* note 246, at 48; Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 359 (2014).

276. LIONEL SMITH, THE LAW OF LOYALTY (forthcoming 2022) (manuscript at 1*).

277. Timothy Liau, *Privity: Rights, Standing, and the Road Not Taken*, 41 OXFORD J. LEGAL STUD. 803, 805 (2021).

278. RESTATEMENT (SECOND) OF TORTS § 652H (AM. L. INST. 1977); Socialist Workers Party v. Att'y Gen., 642 F. Supp. 1357, 1421 (S.D.N.Y. 1986); Manville v. Borg-Warner Corp., 418 F.2d 434, 437 (10th Cir. 1969); Cason v. Baskin, 159 So. 2d 635, 638 (Fla. 1947).

279. *See, e.g.*, Eli A. Meltz, *No Harm, No Foul? "Attempted" Invasion of Privacy and the Tort of Intrusion Upon Seclusion*, 83 Fordham L. Rev 3431, 3465–66 (2015) (discussing how a claim for intrusion upon seclusion should not require an additional element, such as proof of acquisition, because to require so would mischaracterize the nature of the harm to a privacy interest, which is an unwelcome invasion of privacy); Townsend, *supra* note 226, at 80 ("Many wrongs do not lead to bodily damage, economic damage, damage to property, or other physical correlates that can be pointed to as 'real' harm outside of the violation of a legal right. Damage to a person's reputation or privacy interests can often occur without physical consequences.").

280. *See* discussion *supra* Section II.C.

281. *See e.g.*, Jenkins v. CitiFinancial, No. 10-986-(NHL), 2010 U.S. Dist. LEXIS 124744, at *13 (D.N.J. 2010) ("To establish severe emotional distress, a plaintiff must demonstrate that the emotional distress suffered was 'so severe that no reasonable man could be expected to endure it.'. . . This distress must be sufficiently substantial as to result in either physical illness or serious psychological harm."); Dammarell v. Islamic Republic of Iran, 404 F. Supp. 2d 261, 291 (D.C. Cir. 2005) ("[T]he tort of IIED, by contrast, imposes liability only for substantially egregious behavior that causes significant psychological harm (though no physical contact is required) . . . .").

and must prove reputational harm in an action for libel or slander.[282] In cases involving a privacy violation, can a court assume that privacy harm is already present? The answer most consistent with other torts is no.[283] But, if courts choose that path, it is crucial that courts do not require a different harm or they will empty the privacy tort of its content. Instead, courts must look into the normative elements of privacy, outlined above,[284] to determine whether the plaintiff's privacy loss is an injury to the privacy interest (a privacy harm).

As Danielle Citron and Daniel Solove have argued, the law has also recognized in many contexts that emotional distress is sufficient to establish harm—and it should for privacy violations.[285] Data breaches, they demonstrate, produce a significant amount of emotional distress that is analogous to the one that courts have recognized as harm in other areas.[286]

A recent case against Facebook serves as an example. In 2020, in *Davis v. Facebook*, plaintiffs sued as a class because Facebook continued to collect their personal data after they had logged off.[287] The Ninth Circuit held that the plaintiffs had adequately alleged harm to privacy interests and had therefore adequately stated claims for relief of intrusion upon seclusion.[288] The court required the plaintiff to prove the facts.[289] But once the facts were established, it did not require the plaintiff to prove reputational, financial, or discriminatory harm based on the tort because these are not elements of intrusion upon seclusion.[290] The reason why these are not elements of intrusion upon seclusion is that they are not part of the privacy interest: they are other interests that may be harmed when people's personal information is wrongfully collected, used, or disseminated.[291]

More broadly, courts have been better at perceiving this issue in torts than in statutory privacy. For example, in *In re Facebook*, a district court granting the defendant's motion to dismiss noted that intrusion upon seclusion would have been sufficient.[292] In *In re Vizio*, an intrusion upon seclusion claim was adequately pled in an order denying the motion to dismiss in part, before the case was settled.[293] Similarly, in *Opperman v. Path*, a district court held that the

282. *See, e.g.*, Schlegel v. Ottumwa Courier, 585 N.W.2d 217, 221–23 (Iowa 1998) (discussing the large body of case law requiring a reputational harm prerequisite in defamation actions); King v. Union Station Holdings, LLC, No. 4:12CV696SNLJ, 2012 U.S. Dist. LEXIS 155158, at *12 (E.D. Mo. 2012) ("Proof of actual reputational harm is an absolute prerequisite in a defamation action.").

283. *See* discussion *supra* Section II.C.

284. *See* discussion *supra* Sections IV.A–B.

285. Solove & Citron, *supra* note 12, at 777–78.

286. *Id.* at 778–81 (providing numerous examples of data breaches that produce emotional distress).

287. Davis v. Facebook, Inc. (*In re* Facebook Inc. Internet Tracking Litig.), 956 F.3d 589, 566 (9th Cir. 2020).

288. *Id.* at 603 (explaining that the plaintiffs had also sought standing to bring claims for breach of contract, breach of the implied covenant of good faith and fair dealing, in addition to statutory claims under the Wiretap Act and California Invasion of Privacy Act).

289. *Id.* at 606.

290. *Id.* at 601–03.

291. *Id.*

292. *In re* Facebook Internet Tracking Litigation, 263 F. Supp. 3d 836, 843–44 (N.D. Cal. 2017).

293. *In re* Vizio, Inc., Consumer Privacy Litig. 238 F. Supp. 3d 1204, 1217 (C.D. Cal. 2017).

plaintiffs adequately pled intrusion upon seclusion, dismissed Yelp's motion for summary judgment, and proceeded to trial, where the case was settled.[294]

As standing for statutory privacy injuries post-*Spokeo* involves demonstrating how the alleged injury is analogous to a traditional cause of action, the privacy tort has been reinvigorated as a way to demonstrate alleged injuries that stemmed from a statutory violation.[295] But this recognition is not an exclusive characteristic of the privacy tort. It is, instead, a characteristic of the privacy interest to which the privacy tort often (but not always) refers.[296]

The same probatory principle of not requiring consequential harms for redress, which courts tend to follow in tort law, should be extended to statutory violations of privacy. Like the common law privacy tort, privacy statutes that grant private rights of action protect the privacy interest by declaring wrongful a specific set of activities that harm people's privacy interests.[297] As with the privacy tort, privacy harm should exist to grant standing for a privacy statute that protects the privacy interest and contemplates private rights of action, but not a different harm. Interpreting that a different interest must be harmed in order to grant standing is to fundamentally misunderstand the very purpose of these statutes.

B. Addressing Widespread Effects Through a Robust Theory of Privacy Harm

The considerations presented in Parts IV and V can help courts distinguish interferences with privacy interests that produce individualized harm to large numbers of people and widespread privacy losses that are undifferentiated between members of the public, called generalized grievances.[298]

For injuries to be particularized, they must "affect the plaintiff in a personal and individual way."[299] Privacy-reducing actions that produce generalized grievances are a bad candidate for standing because, by definition, everyone suffers their effects in an undifferentiated way.[300] Therefore, these losses would fail to meet the particularity requirement under Supreme Court case law.[301] But not all widespread harms are generalized grievances—some have the potential

294. Opperman v Path, Inc., 87 F. Supp. 3d 1018, 1061 (N.D. Cal. 2014); Opperman v. Path, Inc., No. 13-CV-00453-JST, 2016 WL 3844326 (N.D. Cal. 2016).

295. Matthew S. DeLuca, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2458–63 (2018) ("[C]ourts have found standing, at least in part, by analogizing the plaintiff's alleged injury to one that has been historically recognized by the courts, usually in the common law, and frequently to one of the privacy torts.").

296. *Id.* at 2468.

297. *Id.* at 2463.

298. FEC v. Akins, 524 U.S. 11, 35 (1998) ("If the effect is 'undifferentiated and common to all members of the public,' the plaintiff has a 'generalized grievance' that must be pursued by political rather than judicial means.").

299. *Id.*; Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 n.1 (1992).

300. *Akins*, 524 U.S. at 35 ("What is noticeably lacking in the Court's discussion of our generalized-grievance jurisprudence is all reference to two words that have figured in it prominently: 'particularized' and 'undifferentiated.'").

301. *See* Susan Bandes, *The Idea of a Case*, 42 STAN. L. REV. 227, 273 (1990).

to meet the particularized harm requirement. The task is to differentiate mass (privacy) violations that produce several individualized privacy injuries, from undifferentiated generalized (privacy) grievances that produce generalized privacy losses.

Dismissing all widespread effects as incompatible with the particularity requirement leads to a paradox. Widespread effects are socially relevant precisely because they are pervasive.[302] From a policy perspective, widespread harms must be addressed to compensate victims of those harms and to deter harmful behavior by internalizing externalities.[303] Widespread effects are not a bad candidate for compensation; they are just challenging for lawsuits because individuals have lower than optimal incentives to sue on the basis of widespread effects.[304] But, as the cases discussed here show, people do sometimes sue; claiming that law suits are not a suitable vehicle for widespread privacy harms due to their infrequency is inconsistent with claiming that people should not be granted compensation when they sue.

The social value of deterring and compensating widespread privacy harm, coupled with its unfitness for standing under current doctrine, shows that *Spokeo* and its follow-up cases have the wrong underlying theory of privacy injuries—or they gloss over them because they have no theory of privacy injuries at all.[305]

In other areas of law, courts have recognized widespread effects as important enough to consider them in their harm and standing evaluations. In national security surveillance litigation, courts have taken privacy harms more seriously, ruling that the interception of communications and the seizing and keeping of personal information in a database can constitute by themselves an injury-in-fact—without requiring consequential harms.[306] Most notably, in environmental law, due to the enormity of the interest to quality of life in society and the difficulty in providing individual proof, courts have recognized injuries to people's environmental interests without requiring a separate physical or financial injury.[307] As Rachel Bayefsky explains, plaintiffs suing to protect the

302. *Id.* at 285 ("Rather than treating the widespread nature of constitutional injury as a disqualifying characteristic, the Court should view it as a sign of its importance.").

303. Israel Gilead, *Tort Law and Internalization: The Gap Between Private Loss and Social Cost*, 17 INT'L REV. L. & ECON. 589, 589 (1997) (explaining that tort law liability's central function is internalizing "harmful externalities [that] emerge whenever injurers fail to take into account the loss they inflict on victims").

304. Richard B. Stewart & Cass R. Sunstein, *Public Programs and Private Rights*, 95 HARV. L. REV. 1193, 1214 n.72 (1982) ("When the social benefits of eliminating an unlawful activity are widely shared, the stake of any individual is often small and each individual can enjoy a 'free ride' on the enforcement efforts of others. As a result, no individual may have sufficient incentive to bring suit.").

305. *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 812 (2019) ("We live in a legal environment in which privacy rights mobilization is already difficult; managerial privacy compliance exacerbates the problem. Standing requirements and other hurdles hamper privacy plaintiffs' use of tort law, contract law, and federal privacy statutes to vindicate their privacy rights."); Malaya Powers, *Spokeo v Robins: Standing in the Way of Gender Equality for Intangible Injuries* (2021 draft, on file with author) (demonstrating that *Spokeo* and subsequent cases contain a gendered view of injuries).

306. Margot E. Kaminsky, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. R. 413, 422–25, 429–30 (2017).

307. Jonathan R. Siegel, *Chilling Injuries as a Basis for Standing*, 98 YALE L.J. 905, 915 (1989) (explaining that courts have gradually begin to recognize injuries to environmental interests for standing purposes given the importance of environmental interests to societal quality of life).

environment are often granted standing on the basis that the harm is to an aesthetic or recreational interest that they hold.[308] Furthermore, although courts are reluctant to grant standing based on fears of future environmental harm, some courts have even found standing based on a reasonable fear, such as concerns about the effects of polluting discharges.[309]

Even the Supreme Court has noted, in *Sierra Club v. Morton*, that: "Aesthetic and environmental well-being, like economic well-being, are important ingredients of the quality of life in our society, and the fact that particular environmental interests are shared by the many rather than the few does not make them less deserving of legal protection through the judicial process."[310] What is more, the Court held in *Friends of the Earth v. Laidlaw* that, because standing in environmental cases depends on injury to the plaintiff rather than injury to the environment, it can allow standing even if plaintiff's belief in environmental degradation is factually incorrect—provided there are reasonable concerns about environmental degradation.[311]

For some scholars, this conclusion suggests that environmental cases have embraced subjective showings of harm as sufficient for federal jurisdiction.[312] These subjective showings of harm are analogous to privacy harm in their relevance to people's wellbeing. This connection was noted, for example, in *Krottner v. Starbucks*, where the court discussed whether risk of future harm may suffice for privacy claims given that it has been accepted for environmental claims, stating that "in the context of environmental claims, a plaintiff may challenge governmental action that creates 'a credible threat of harm' before the potential harm, or even a statutory violation, has occurred."[313] As Jonathan Adler explains, violating "an environmental permit requirement could produce no measurable impact, but nonetheless support standing if the citizen-suit plaintiffs claim to have modified their behavior as a result of their fears. This is sufficient for the plaintiff to claim injury."[314]

The normative question to establish this analogy is whether privacy harm affects people's wellbeing as does environmental harm, justifying considering privacy interests similarly to environmental interests. Arguably, it does.[315] Although privacy harm and environmental harm have countless relevant descriptive and normative differences, the social importance of privacy harm

308. Rachel Bayefsky, *Psychological Harm and Constitutional Standing*, 81 BROOK. L. REV. 1555, 1586 (2015); *see also* Jonathan Adler, *Stand or Deliver: Do Liberalized Standing Rules Advance Environmental Protection?*, 12 DUKE ENV'T. L. & POL'Y F. 39, 51 (2001).

309. Bayefsky, *supra* note 308, at 1628; *see, e.g.*, Cent. Delta Water Agency v. United States, 306 F.3d 938, 948–50 (9th Cir. 2002).

310. Sierra Club v. Morton, 405 U.S. 727, 734 (1972).

311. Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc., 528 U.S. 167, 181–84 (2000).

312. Gene R. Nichol Jr., *Standing for Privilege: The Failure of Injury Analysis*, 82 B.U. L. REV. 301, 312–13 (2002) ("Statutory standing cases are regularly based on widely-shared and intangible claims, despite the Court's effort in *Lujan v. Defenders of Wildlife* to restrict legislatively-crafted standing.").

313. Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010).

314. Adler, *supra* note 308, at 57 ("Thus, under *Laidlaw*, the injury in fact requirement is not a substantive hurdle, but merely a technical pleading requirement that can be satisfied with something as simple as an affidavit alleging 'fear' or 'concern' about a given legal violation in the vicinity.").

315. *See* Ben-Shahar, *supra* note 219, at 105; Cofone, *supra* note 210, at 515–16.

resembles that of environmental harm when incorporating its widespread effects commenced; they also resemble each other in the difficulty of quantifying harm and balancing values.[316] Leaving actions that produce widespread privacy harm to citizens from large corporations unaddressed by deeming it a generalized grievance is undesirable for similar reasons: harm is addressed nowhere else, victims remain uncompensated, and externalities are not internalized.

While administrative law measures exist in privacy, they are insufficient. As Citron and Solove explain: "Private lawsuits serve a function that these other tools lack. Such lawsuits allow individuals to have a say about which cases are brought. These lawsuits bring out facts and information about blameworthy security practices by organizations. They provide redress to victims, and they act as a deterrent."[317]

Doctrine and standing on harm must catch up with the social reality of the enormity of collective privacy interests and the difficulty in providing proof in a networked society. Nonprivacy injuries (such as financial and reputational) that stem from privacy loss often do not materialize until much later and, once they do materialize, causality is extremely difficult to establish.[318] As the D.C. Circuit acknowledged in *Attias v. Carefirst* when discussing information stolen in a hack: "No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already."[319] The doctrinal position of ignoring privacy interests for standing thus leads injuries frequently being left unaddressed because it introduces problems of proof of harm and causality.

Two cases may serve as examples of this. In *Bradix v. Advance Stores*, hackers allegedly obtained Advance Stores' employees' names, Social Security numbers, wages, and states where employees paid income taxes.[320] Hackers then used employees' information to attempt to secure a vehicle's financing, which appeared on the plaintiff's credit report, without authorization.[321] The court dismissed the case for lack of injury because it considered that there was no proof that fraud attempts had actually damaged the plaintiff's credit score.[322] But how could a plaintiff ever demonstrate that this contributes to a lowering of his credit score in the future, or if his credit score had already decreased, that it was actually this act that damaged his credit score and not something else? Not recognizing

316. *See* Bandes, *supra* note 301, at 289 ("A number of influential scholars have questioned the Court's assumption that [A]rticle III precludes the judicial branch from resolving claims of abstract or widely shared injury.").

317. Solove & Citron, *supra* note 12, at 782; *see generally* Sangchul Park, *Why Information Security Law Has Been Ineffective in Addressing Security Vulnerabilities: Evidence from California Data Breach Notifications and Relevant Court and Government Records*, 58 INT'L REV. L. & ECON. 132 (2019).

318. *See* Solove & Citron, *supra* note 12, at 785.

319. Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017).

320. Bradix v. Advance Stores Co., No.16-4902, 2016 U.S. Dist. LEXIS 87368, at *2 (E.D. La. July 6, 2016) (holding that the plaintiff did not have Article III standing).

321. *Id.* at *3.

322. *Id.* at *10 ("A careful review of Plaintiff's complaint makes it clear there is no certainly impending injury alleged. The two 'as yet unidentified' credit inquiries do not constitute cognizable injuries in fact. . . . Plaintiff has not even alleged that his credit score was adversely impacted . . . .").

the privacy injury introduced a proof problem and thus left two injuries unaddressed: a privacy injury and a financial one.[323]

Similarly, recall *Meyers* and *Kirchein*,[324] discussed above to illustrate the importance of aggregating information.[325] If plaintiffs in either case face credit card fraud or identity theft in the future, it will likely be because of different pieces of information that a malicious actor aggregated from different sources, not for one wrongful credit card receipt.[326] Such aggregation makes it impossible for plaintiffs to know, and let alone prove, when the credit card fraud or identity theft happens, which misuse of the information caused that harm, leaving it unaddressed.[327] If either business's illegal practice collaborated with the eventual identity theft or credit card fraud, plaintiffs will never know.[328] It seems absurd, from this perspective, to require impossible-to-trace financial harm to recognize privacy harm.[329] The dismissal of these two cases due to not recognizing the plaintiffs' privacy injury introduced a causation problem that left one injury in the present unaddressed (privacy) and will leave another injury in the future unaddressed (financial) if its risk materializes.[330] These cases show why it would be desirable, like it is for environmental harms, to recognize widespread effects in privacy standing analyses.

This is the progress that this Article's framework aims to facilitate. When applying it, not *all* privacy harms are seen as generalized grievances, thus forcing courts to remedy either all or none of them. Instead, harms such as those in these cases, but not all harms, can and should be considered particularized.

C. Re-Examining TransUnion v. Ramirez

TransUnion, one of the three large credit bureaus, mislabeled thousands of people as possible terrorists and other national security threats in credit reports that were available to potential employers and creditors.[331] The mistaken results for over 8,000 people was due to a process of matching names with the Office of Foreign Assets Control.[332] Mr. Ramirez learned about this mistaken designation, and the lack of a procedure to correct it, after finding that it was the reason he

323. *See id.* at *3.

324. Meyers v. Nicolet Rest. of De Pere, Inc., 843 F.3d 724, 725 (2016) ("Meyers was given a copy of his receipt after dining at Nicolet. . . . He noticed that Nicolet's receipt did not truncate the expiration date, as the FACTA requires."); Kirchein v. Pet Supermarket, Inc., 297 F. Supp. 3d 1354, 1356 (2018) ("Kirchein filed a putative class action alleging that the Defendant violated the Fair and Accurate Credit Transactions Act, which prohibits printing 'more than the last five digits of the credit card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction.'").

325. *See* discussion *supra* Section III.C.

326. *See* discussion *supra* Section III.C.

327. Strahilevitz & Liu, *supra* note 194, at 3–5*.

328. *See Meyers*, 843 F.3d at 725; *Kirchein*, 297 F. Supp. 3d at 1356.

329. Citron & Solove, *supra* note 12, at 777–78 (discussing a similar statement for data breach harms).

330. *Meyers*, 843 F.3d at 725; *Kirchein*, 297 F. Supp. 3d at 1360.

331. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2201 (2021).

332. *Id.* at 2197.

was unable to purchase a car.[333] He sued on behalf of a putative class arguing that TransUnion breached the FCRA in failing to secure credit reports' accuracy, to disclose reports in their entirety, and to inform consumers of their relevant rights.[334] The company argued that plaintiffs did not suffer a concrete injury and thus lacked Article III standing.[335]

After a jury ruled in favor of Ramirez, the Ninth Circuit affirmed, reasoning that all class members had a risk of harm to their privacy, reputational, and financial interests.[336] The Supreme Court vacated and remanded.[337] It held that the plaintiffs' claim that TransUnion increased their risk of harm was insufficient to be awarded standing and the plaintiffs needed an additional injury that can be regarded as concrete; plaintiffs thus lacked (federal) standing.[338] Out of the 8,185 class members, only 1,853 had their incorrect credit reports disclosed to third parties; those 1,853 suffered an injury-in-fact but the remaining 6,332 class members had only a theoretical risk of future harm that is insufficient for federal standing.[339]

TransUnion v. Ramirez, in short, confirmed the Court's reading of injuries in *Spokeo* that a statutory violation is insufficient to confer federal standing.[340] But it went beyond that in ruling that risk of future harm does not qualify as concrete under Article III.[341] Although the facts of the case pertain to the FCRA, the reasoning applies to federal standing for any statute that involves private rights of action for privacy breaches.[342]

The Supreme Court could have written the ruling, arriving at the same result, as an explicit statutory interpretation ruling about the types of injuries that Congress recognized in the FCRA, interpreting that the FCRA as written requires financial harm for standing (to fulfill the legal wrong in step 3). Congress, after all, has the power to decide whether an action constitutes a legally cognizable wrong and whether one has a right that guards against a particular loss in wellbeing, so that such a loss constitutes a legally cognizable harm.[343] Disappointingly, the majority wrote it as a standing ruling instead (hinging on step 2).[344] Doing so, at minimum, subtracts clarity about its scope. But the

333. Specifically, as a Specially Designated National, barred for national security reasons from conducting business in the United States.

334. *TransUnion LLC*, 141 S. Ct. at 2197.

335. *Id.*

336. *Id.* at 2200.

337. *Id.* at 2214.

338. *Id.* at 2205–07.

339. *Id.* at 2208–09 (discussing that the common law analog, defamation, requires publication, and mere risk of future harm meaning possible future publication, is insufficient to establish federal standing).

340. *Id.* at 2223 (Thomas, J., dissenting).

341. *Id.* at 2209 ("[T]here is 'no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury.'" (quoting Owner-Operations Independent Drivers Assn., Inc v. United States Dept. of Transp., 879 F.3d 339, 344 (D.C.C. 2018))).

342. *Id.* at 2197.

343. *See generally* Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).

344. *Ramirez*, 141 S. Ct. at 2205 ("But even though 'Congress may "elevate" harms that "exist" in the real world before Congress recognized them to actionable legal status, it may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is.'").

problem runs deeper. As Justice Thomas explains in his dissent: "in the name of protecting the separation of powers, this court has relieved the legislature of its power to create and define rights."[345] By confusing steps 2 and 3 of the analysis, the *TransUnion* ruling muddles constitutional standing with statutory interpretation and is objectionable on the very constitutional grounds that the Court uses as basis for its reasoning.

But not even Justice Thomas places enough blame on the Court. Because gutting Congress's powers to create rights is not a bug of the majority's *TransUnion* ruling; it is a feature of federal privacy standing since *Spokeo.*[346]

In *Spokeo*, the Court wrote that "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury-in-fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified."[347] That leads to a statutory interpretation exercise to determine in which cases Congress, to use the words of the Court, identified privacy harm, exempting plaintiffs from alleging any additional, consequential, harm. *Spokeo* was the first time that the Court split the "concrete and particularized" prong in two in order to deny standing.[348] A statutory violation that produces a privacy loss should therefore be sufficient to constitute a concrete injury and establish standing in *some* statutes.[349] The question is which ones.[350]

A broad reading of *TransUnion* would contradict such dicta and put the Court at odds with its own already narrow case law on federal standing. The Court (and TransUnion in its arguments) provided no standard for determining what would constitute a "concrete" injury.[351] This standardless evaluation of injuries would amount to a complete disregard of injuries.[352] Such broad reading would stand in contradiction to numerous precedents in which the Court considered that intangible harms can satisfy federal standing,[353] some of which

345. *Id.* at 2221; *see also* Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*, 101 B.U. L. REV. ONLINE 62, 69–71 (2021) (explaining how the majority ruling usurps legislative powers).

346. *Ramirez*, 141 S. Ct. at 2197.

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

348. *See id.* at 352 (Ginsburg, J., dissenting); *Justiciability—Class Action Standing*—Spokeo, Inc. v. Robins, 130 HARV. L. REV. 437, 444 n.77 (2016).

349. *See Spokeo*, 578 U.S. at 330.

350. Note that the Ginsburg-Sotomayor dissent in *Spokeo* is based on the argument that Robins did allege concrete harm by stating that Spokeo's misinformation caused him actual harm. *Id.* at 351–53 (Ginsburg, J., dissenting). This seems to indicate that majority and dissent agreed that statutory violation can be sufficient to constitute a concrete injury and to establish standing in *some* statutes; their disagreement was whether the FCRA was one of them.

351. *See Ramirez*, 141 S. Ct. at 2203–14.

352. Flast v. Cohen, 392 U.S. 83, 123 (1968) (Harlan, J., dissenting).

353. *See, e.g.*, *id.* at 95; Regents of Univ. of Cal. v. Bakke, 438 U.S. 265, 267 (1978); U.S. Parole Comm'n v. Geraghty, 445 U.S. 388, 396 (1980); Havens Realty Corp. v. Coleman, 455 U.S. 363, 378 (1982); FEC v. Akins, 524 U.S. 11, 19 (1998); Pub. Citizen v. U.S. Dep't of Justice, 491 U.S. 440, 449 (1989); Trafficante v. Metro. Life Ins. Co., 409 U.S. 205, 209–10 (1972); Hardin v. Ky. Utils. Co., 390 U.S. 1, 7 (1968); Heckler v. Mathews, 465 U.S. 728, 738 (1984); Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 211 (1995).

the majority relies on to discuss its very own concreteness requirement.[354] It would warrant the dissent's criticism that it engages in judicial activism by taking away Congress' ability to determine injuries[355]—particularly given that, from a textualist perspective, given class members' loss in wellbeing there was nothing hypothetical about the case and controversy at hand.[356]

As an alternative, courts could read *TransUnion* narrowly: the case can be construed as stating that the FCRA violation requires disclosure to third parties (but not financial harm) to constitute concrete and particularized privacy harm.[357] Risk of future financial harm is irrelevant in this case, based on the Court's precedent, because it is not concrete; but there is a present harm that fulfils the constitutional requirement: the existing, concrete, privacy harm.[358] Requiring that plaintiffs sufficiently prove some type of harm (either privacy or financial), and arguing that this is a burden that can be imposed without encroaching on congressional powers, can only work if privacy harm is also acknowledged. The majority does recognize, allowing for this narrow reading, that "[v]arious intangible harms can also be concrete."[359] It just fails in its task of identifying any of them in the case.[360]

That narrow reading, with the framework of this Article, gives lower courts some scope to provide redress. Ramirez suffered a privacy and a reputational loss, harm, and injury: the disclosure of the erroneous information and his inability to purchase a car.[361] His loss and harm were produced by TransUnion disclosing an incorrect terrorist alert, which affected other entities' belief distributions about Ramirez inappropriately. Coupled with TransUnion's FCRA violation, that harm constituted an injury. The best argument to distinguish among class members is that the injury was not shared with all members of the class because, to injure someone's privacy or reputation, the information must be shared.[362] Under this line of reasoning, the other members of the class did not suffer a privacy injury (because no true information about them was illegally collected or distributed) and did not suffer a reputational injury (because no false information about them was shared).[363] *TransUnion* is, with regards to the 6,332 class members that were implicitly cut out of the class by the Court, in a similar situation to *Urban Outfitters*, where there is a statutory violation sanctionable by the appropriate authority but no injury had yet materialized.[364]

354. *Ramirez*, 141 S. Ct. at 2200 ("[A] 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms including (as relevant here) reputational harm.").

355. *Id.* at 2225 (Kagan, J., dissenting) ("The Court here transforms standing law from a doctrine of judicial modesty into a tool of judicial aggrandizement.").

356. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (discussing the classification of hypothetical).

357. *Ramirez*, 141 S. Ct. at 2222 (Thomas, J., dissenting).

358. *Id.* at 2200.

359. *Id.*

360. Solove & Citron, *supra* note 345, at 68–69.

361. *Ramirez*, 141 S. Ct. at 2209.

362. *Id.* at 2220 n.4 (Thomas, J., dissenting).

363. *Id.* at 2215 (Kagan, J., dissenting).

364. *Id.* at 2214.

Distinguishing privacy injuries from mere privacy loss and from other injuries for standing purposes can support the conclusion that Ramirez had a privacy and reputational injury but not every member of the class did, since illegal disclosure would be necessary to constitute such injury. Such conclusion is independent to the risk of financial injuries created.[365] That narrow reading is even compatible with a hypothetical pro-Robins judgment in *Spokeo* (had the Court relied on the arguments supported in the privacy law scholars' brief on the importance of FCRA standing) because Robins and Ramirez, individually, had equivalent injuries.[366] The *TransUnion* ruling indicates that not all informational violations can confer standing.[367] But there is a way to build productive case law on this overall objectionable ruling by arguing that not all statutory violations create privacy or reputational injuries, but many do.

The worst mistake the Court made is not the outcome of distinguishing Ramirez from some other members of the class. It is the reasoning of distinguishing him from those who did not identify consequential harms (as the Court calls them, "downstream consequences"), such as financial. Instead, to be consistent with its own precedent, the Court should have distinguished him from those other members, if any, who did not suffer privacy injuries. Lower courts deciding similar cases could do exactly that.

Crucially, *TransUnion* has a lesson for the importance of identifying intrinsic privacy harm. In the majority ruling, Justice Kavanaugh shows concern that there is not enough interference with the reputational and financial interests of all members of the class to justify standing.[368] That may be correct. The issue is that it may have been the right answer to the wrong question because there was also an interference with the privacy interest.

Recognizing consequential harms would not have helped in addressing the plaintiffs' claims in *TransUnion*.[369] Those other harms did not yet materialize for many of the plaintiffs, but they will in the future, so conditioning standing on them now leads to their harms being left unaddressed.[370] But when these other harms materialize, proving their relationship with TransUnion's actions will be too burdensome for these plaintiffs, also leaving them unaddressed. Ex-ante, courts do not always know what subsequent harms will happen, so it may be ineffective to rely on subsequent consequential harms to remedy actual privacy harm. And besides these other harms to each member of the class, plaintiffs share privacy loss, harm, and injury.

365. *Id.* at 2201.
366. *Id.* at 2202.
367. *Id.* at 2209.
368. *Id.* at 2200 ("Central to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms including (as relevant here) reputational harm").
369. *Id.* at 2218 (Thomas, J., dissenting).
370. *Id.* at 2219.

VII. CONCLUSION

Supreme Court case law puts federal courts dealing with privacy claims in a straightjacket. To address privacy standing in this context without gutting privacy rights, courts should do three things. First, they need to identify whether there was privacy loss—a descriptive element—meaning a reduction in the plaintiff's level of privacy. Second, they need to identify whether such a loss produced privacy harm by looking at privacy's normative values (Did it impede autonomy? Did it impede intimacy?). Third, they need to identify whether the privacy harm is actionable by looking at whether it fits into a common law tort or a statutory breach that provides plaintiffs' standing.

The conceptual problem has been that federal courts, including the Supreme Court, have attempted to answer the first and second questions through the third. They dive directly into the third step while skipping the first and second, and thus lack a way to distinguish among plaintiffs consistently—to rule out frivolous lawsuits while providing meritorious redress. That conceptual problem has produced a doctrinal one: a federal circuit split. Courts on both sides of the disagreement blend these steps together and, what is worse, to remedy the ill one side requires instead harm to nonprivacy interests, such as financial. The doctrinal problem—that half of the circuit courts do not consider privacy interests—relates to the fear that, if privacy interests are recognized, everything will end up giving rise to privacy claims. Victims of privacy harm, as a consequence, lack a legal remedy where those who are similarly situated (with other types of harm) have one.

This Article proposes a solution to that three-level problem. Many situations produce privacy losses, but only some produce privacy harm, and fewer produce privacy harm that is actionable. Treating the three steps separately has theoretical and practical benefits. This solution would expand redress for privacy injuries by navigating restrictive Supreme Court precedent with modern views of privacy, it captures the importance of inferences for privacy harms, addresses stated policy concerns by eliminating the risk of a slippery slope, and facilitates consistency in federal case law.