THERE'S NO UNDERSTANDING STANDING FOR PRIVACY: AN ANALYSIS OF *TRANSUNION V. RAMIREZ*

Summer Elliot[†]

I. INTRODUCTION

What happens when enforcing privacy rights becomes entirely subject to Supreme Court beliefs about harm? *TransUnion LLC v. Ramirez*[1] ensures we will soon find out. Litigation of modern privacy rights faces two challenges: (1) privacy rights are difficult to define, and (2) the Supreme Court has narrowed the doctrine of standing, keeping privacy cases from entering a court room. Both of these issues make it difficult for privacy law to evolve, either by statute or common law, and make it difficult to advance the protection of privacy rights. The *TransUnion* Court has implicated and worsened both issues.

Privacy rights and harms are challenging to define for courts in the United States, even outside of TransUnion's confused ruling. First, common law privacy harms were ossified in the 1960s when William Prosser, a giant of torts law, created his four "privacy torts."[2] Modern privacy law tries to fill the gaps in the common law by relying heavily on statutes and legislation.[3] This means privacy law must constantly evolve and adapt to an ever-changing technology landscape by defining new privacy harms and creating new statutes. Defining these harms is difficult as privacy encompasses many types of abstract harms that are often disaggregated across many individuals.

Second, the Supreme Court's narrowed standing doctrine also limits effective protection of privacy rights. In the last 50 years, the Supreme Court has shifted its standing doctrine from a determination of whether a plaintiff has a connection to a harm to an inquiry of whether the harm itself suffices

DOI: https://doi.org/10.15779/Z38GH9BB0K

† J.D., 2023, University of California, Berkeley School of Law.

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

2. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1889-90 (2010) In the early 1960s, Prosser collected all cases that related to upholding privacy law and retrospectively categorized these cases into four torts: Intrusion Upon Seclusion, Public Disclosure of Private Facts, Appropriation of Name or Likeness, and False Light.

3. *See e.g.,* The Fair Credit Reporting Act, 15 U.S.C. § 1681 (attempting to protect individuals' information that is collected and stored by credit reporting agencies, and which the four Prosser Torts do not specifically address).

for standing. The Court has narrowed its definition of harm for standing to such an extent that it can run explicitly counter to a Congressional statute.

The *TransUnion* decision continues to arbitrarily restrict standing by defining an intangible injury, which unlike harm to property or a person is a more abstract injury, as those harms only with a "traditional common law analogue." Because violations of privacy rights create nearly exclusively intangible harms, and are often new rights that do not have a traditional common law anchor, the Court's ruling substantively limits current privacy statutes that purposefully go beyond the common law. Further, more than any other standing case or contemporary Supreme Court decision, *TransUnion* questions and places limits on Congress's abilities to create new rights and define new privacy harms that would be recognized under Article III. This limitation will severely hamper the ability for privacy rights not just to be enforced now, but to evolve in a rapidly changing digital landscape.

The Court couches its decision in judicial restraint and postures a policy agenda of keeping frivolous lawsuits out of federal courts. However, the Court's decision usurps power from the legislature with a bootstrapped Constitutional analysis that has no clear place in privacy law. In doing so, the *TransUnion* Court prevents plaintiffs with real injuries from reaching the court, lets bad actors evade punishment, and hinders privacy law from becoming more equitable and effective.

Part II of this Note moves through a brief history of the flawed modern standing jurisprudence. Then it summarizes the origin of privacy law (as well as the limitations of privacy law) and provides an overview of why privacy harms are difficult for courts to manage even without a restrictive standing doctrine. Part III summarizes the *TransUnion* decision and its key problems. Part IV will analyze how the *TransUnion* decision narrows standing and the ability to define privacy harms, thereby encouraging the rigidity of privacy law and limiting recourse for violations.

II. BACKGROUND: STANDING, PRIVACY LAW, AND DEFINING PRIVACY HARMS

Even before the *TransUnion* decision, both the history of standing jurisprudence and the origins and development of privacy law created a difficult landscape to litigate privacy rights. Access to federal courts under Article III standing has been narrowed over the last 50 years. Common law privacy was ossified into four distinct torts in the 1960s, which are difficult to apply common law privacy to modern technology.[4] But even as privacy

4. *See supra* note 2 (Williams Prosser's four privacy torts).

statutes filled these gaps in the common law, privacy harms remain challenging for legislatures to define and courts to navigate.

A. A BRIEF HISTORY OF STANDING

Standing is defined as the required connection a plaintiff has to the harm they allege in court.[5] In *Marbury v. Madison*, the Court held for the first time that Article III of the Constitution gave the Supreme Court its judicial power to review and rule on "cases and controversies."[6] Chief Justice John Marshall stated "for every legal right there is a remedy."[7] Therefore, the Court would review allegation of harms to legal rights provided that Article III would deem the alleged harm proper for federal court.[8] Deeming what was "proper" for federal court is understood as "justiciability" analysis, and part of that analysis is the doctrine of standing. During World War II and up and through the 1960s, plaintiffs were broadly able to demonstrate a connection to an alleged harm in court even if they were alleging harms for community interests rather than their own individual injuries.[9] But in the last 50 years, the legal doctrine of standing has been used by the Court to constrict the ability for plaintiffs to enter federal courtrooms. *TransUnion v. Ramirez* is a continuation of this trend, as the Court again heightened the standing requirement to a restricted form of harm rather than restricting who has a connection to that harm.

1. Standing for the Public Evolves into Requiring an Individualized Injury

During World War II, standing jurisprudence was broad enough to allow a legal practice called the "Right to Stand for the Public."[10] In cases such as *FCC v. Sander Brother Radio Station*[11] and *Scripps Howard Radio v. FCC*,[12] the Court expanded access to the courts by allowing plaintiffs to assert rights for general public interests, even if they were merely an indirect party to the harm asserted, and seek remedies for those rights. During this era, the Court held that unless Congress had explicitly limited court access via statute, the reviewing power of the federal courts to save the public interest from injury or destruction should remain intact.[13] The ability to stand for public interests

5. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 n.1 (1992).
6. Marbury v. Madison 5 U.S. 137, 147 (1803).
7. *Id.*
8. *Id.*
9. *Id.*
10. Elizabeth Magill, *Standing for the Public: A Lost History*, 95 VA. L. REV. 1131, 1131 (2009).
11. FCC v. Sanders Bros. Radio Station, 309 U.S. 470, 477 (1940).
12. Scripps-Howard Radio, Inc. v. FCC, 316 U.S. 4, 8 (1942).
13. *Sanders Brothers*, 309 U.S. at 477.

continued through the 1960s Warren Court, especially as applied to cases of racial discrimination.[14]

However, in 1970, the ability for a plaintiff to stand for the interests of the public, particularly under a private right of action from a statute, became much more limited. In *Association of Data Processing Service Organizations v. Camp*,[15] the Court determined that even when the plaintiff was in court based on statutory authorization from Congress, they must still assert that they themselves have been injured. The Court held that this injury must be to one of the plaintiff's interests, and these interests must arguably be "within the zone of interests" that were sought to be protected or regulated by the statute or constitutional guarantee in question.[16] The Court called this requirement an "injury in fact."[17] In other words, an "injury at law," which was a community interest stemming from a statute, could not suffice by itself to allow a plaintiff with no personal "injury in fact" to have standing. However, the Court later clarified in a separate case that if Congress, by statute, had specifically provided for a private right to judicial review, rather than a generalized community legal interest, standing could be fulfilled by the violation of the rights created in that Congressional statute.[18] So long as an individual person had suffered a "legal wrong" within the meaning of the private right of action statute, they had standing in federal court.[19]

Only five years after *Association of Data Processing Service Organizations*, the Court decided a pair of cases, *Warth v. Seldin*[20] and *Simon v. Eastern Kentucky.*[21] The Court held that the injury in fact test not only applied to cases and controversies from Congressional statutes, but was required by Article III for all Constitutional cases.[22] However, even though plaintiffs were now required to allege a personal injury for all cases and controversies, the Court during this era meant for the injury in fact test to broaden the "categories of injuries that may be alleged in support of standing,"[23] by allowing plaintiffs to allege a personal injury outside of a Congressional statute or Constitutional challenge.

14. Elizabeth Magill, *Standing for the Public: A Lost History*, 95 VA. L. REV. 1131, 1131 (2009).

15. Ass'n of Data Processing Serv. Orgs. v. Camp 397 U.S. 150 (1970).

16. *Id.* at 153.

17. *Id.* at 152 (emphasis added).

18. Sierra Club v. Morton, 405 U.S. 727, 732 (1972).

19. *Ass'n of Data Processing*, 397 U.S. at 152 (emphasis added).

20. Warth v. Seldin, 422 U.S. 490, 501 (1975).

21. Simon v. E. Ky. Welfare Rights Org. 426 U.S. 26, 28 (1976).

22. *Warth,* 422 U.S at 501 ("Of course, Art. III' s requirement remains: the plaintiff still must allege a distinct and palpable injury to himself, even if it is an injury shared by a large class of other possible litigants.").

23. *Simon*, 426 U.S. at 39.

The injury in fact test was therefore supposed to expand plaintiffs' access to federal courts by expanding standing for new types of personal injuries.

2. *Lujan's Definition of Injury in Fact, Clapper's Avoidance of Risk of Harm*

Despite the Court's wishes to expand categories of injuries, in 1976, it held in Lujan v. Defenders of Wildlife[24] that "injury in fact" was a minimum high bar for Article III standing, particularly for public interest suits.[25] The Lujan Court took the injury in fact analysis and broke it up into two components. An injury in fact must first bet "concrete and particularized," and second, be an "actual or imminent harm" rather than a hypothetical or abstract harm.[26] This was a significant step in the jurisprudence of standing because the Court decided not only whether the plaintiffs had a connection to an alleged harm, but also whether the Court was willing to recognize the harm itself.

The Court then applied the Lujan definition of injury in fact in Clapper v. Amnesty International USA. [27] In 2008, Congress passed the FISA Amendments Act (FAA). The Amendment revised the procedures for foreign government surveillance to allow surveillance of persons outside of the United States without requiring specific descriptions of those persons. U.S. citizens of human rights organizations filed an action as soon as the amendment was enacted, claiming it was unconstitutional. The plaintiffs alleged that because they worked with clients overseas which the United States "believed to be associated with terrorist organizations," they were likely to be imminently harmed by the government monitoring their communications."[28]

The Court held that imminent harm could not be "speculative," but instead must be "certainly impending" to constitute an injury in fact.[29] The Court further held that the law of Article III standing was built on separation of powers principles, preventing the judicial process form usurping the powers

24. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992). In *Lujan*, a group of plaintiffs from conservation organizations wanted to sue the Secretary of the Interior for a change to the Endangered Species Act. The Court held the plaintiffs could not allege a real, individualized current harm or imminent injury to their or the public's interests simply because some citizens might want to visit foreign countries with endangered species.

25. *Id.* at 560–61.

26. *Id.* at 560. Standing would further require the injury to be "fairly traceable to the defendant's conduct" and redressed by the remedies requested.

27. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408–09 (2013).

28. *Id.*

29. *Id.* Only 5 years after *Clapper*, Edward Snowden's revelations about the NSA's spying tactics went public and confirmed the NSA was gathering information on non-U.S. persons outside the United States.

of the political branches, like the Executive Branch conducting surveillance.[30] The Court decided the human rights associations' alleged harms were not imminent and were based on mere speculation that they might be surveilled sometime in the future.

To summarize, the Court went from allowing plaintiffs to stand for community rights with only an indirect connection to an injury, to requiring plaintiffs in court under a statutory right of action to show a personal "injury in fact." The Court then grafted the injury in fact/personal injury requirement onto all Constitutional Article III standing, not just cases arising under federal statute. Then, the Court narrowly defined what an injury in fact is and what harms would meet its test. Lastly, the Court limited ability for plaintiffs to assert significant risk of harm as an "imminent harm" under the injury in fact test.

3. Spokeo's Privacy Surgery

The next and most significant step before TransUnion v. Ramirez in standing's evolution occurred in Spokeo v. Robbins.[31] Spokeo involved statutory violations of the Fair Credit Reporting Act, a privacy statute. Robbins, the named plaintiff, found his information on Spokeo's "people search" website, but the information was extremely inaccurate. Robbins alleged that because potential employers used Spokeo for background checks, this inaccurate information made it difficult for him to gain employment because the site's information made him appear overqualified. He brought a class action with other plaintiffs who also had inaccuracies in their reports. In assessing his complaint, the Court re-emphasized the definition given in Lujan for "injury in fact"—that in order to have standing, the harm asserted had to be "concrete and particularized." However, they emphasized that while the lower courts had adequately determined the injury alleged was "particular" to Robbins, they had not assessed whether it was "concrete," and that the two requirements were separate.[32]

The Court held that a concrete harm now required a "close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American Courts."[33] This requirement of concreteness would further be applied to the entire class in a class action.[34] The only other guidance the Court provided was that a "bare procedural violation divorced from any concrete harm" could not

30. *Id.*
31. Spokeo, Inc. v. Robins, 578 U. S. 330, 340 (2016).
32. *Id.* at 340.
33. *Id.* at 341.
34. *Id.* at 342.

satisfy the injury in fact test.[35] The case was remanded to the Ninth Circuit to determine if the alleged harm met the Court's requirements for a "concrete harm."

Spokeo therefore left unclear what might specifically constitute a "concrete harm" in the Court's injury in fact analysis. Courts in some Circuits assumed that an alleged federal statutory violation itself constituted a concrete injury sufficient for Article III standing.[36] Other courts treated the concrete injury test as a separate requirement from a statutory violation.[37]

4. Evolution of the Deference to Congress's Authority

Before Spokeo, despite narrowing the injury test that plaintiffs must meet, the Court went to great lengths in standing cases to acknowledge Congress's power to create rights via statute. After Association Data Processing created the injury in fact test, the Court held that Congress could create standing by statute through a private right of action.[38] In Lujan, the Court reaffirmed that "Congress has the power to define injuries and articulate chain of causation that will gives rise to a case or controversy were none existed before."[39] The Court in Spokeo, however, took a small step away from this previous Congressional deference. The Spokeo Court held that Congress is "well positioned to identify intangible harms that meet minimum Article III requirements," and that Congress's judgement is instructive and important.[40] However, according to the Spokeo Court, Congressionally defined harm via statute does not automatically satisfy the injury in fact requirement, because Article III standing still requires a concrete injury.[41] TransUnion v. Ramirez is a continuation of Spokeo's limited deference to Congress's abilities to create standing through statute.

B. ORIGINS OF PRIVACY LAW: FROM RIGHTS TO OSSIFICATION

The idea of privacy as a legal right grew out of Samuel Warren and Louis Brandeis's famous 1890 article entitled The Right to Privacy.[42] They argued that individuals' ability to keep their "inviolate personalities" free from "unwanted interference" should be deemed a right. Brandeis and Warren saw

35. *Id.*
36. *See* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1204 (Ill. 2019).
37. *See* Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 930 (8th Cir. 2016).
38. Sierra Club v. Morton, 405 U.S. 727, 732 (1972).
39. *Spokeo*, 578 U.S. at 340 (quoting *Lujan*).
40. *Id.* at 342.
41. *Id.*
42. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

privacy law as a "right to be let alone."[43] Their article was published in reaction to the proliferation of the "instant" photograph, and the media's focus on selling publications using gossip.[44] Brandeis and Warren's article led to state courts adopting generalized privacy torts in the common law.[45]

1. Prosser Limits Privacy to a Compensatory Structure, and Limits Recognized Harms in Privacy Law

In the early 1960s, William Prosser took privacy law in a different direction. Prosser looked back at all the common law cases that had stemmed from Warren and Brandeis's article and distilled them down into four types of torts: "(1) unreasonable intrusion upon a person's seclusion, (2) appropriation of someone's name or likeness, (3) unreasonably giving publicity to a person's private life, and (4) publicizing someone in a false light."[46] But by doing so, Prosser inevitably made privacy law a harms-focused tort system, because each tort was directly related to the injury it addressed, rather than the simple right to be left alone and violations of that right.[47] By creating a harms-focused mode of law, Prosser created a mode of privacy law that focused on the compensatory function of addressing torts rather than the rights function of addressing a violation of a privacy right. As leading privacy legal scholar Danielle Citron argues, a compensatory approach to privacy law forces a focus only on those harms that can be redressed monetarily, and privacy is notoriously difficult to measure in monetary value.[48]

Further, Prosser ossified privacy law so that only a narrow range of harms that fell within his four distinct categories would be recognized.[49] These categories do not account for the different ways privacy can be violated in the modern world. Hence, Prosser's engineered categories limited the ability to flesh "out the contours of 'the right to be let alone' protected by tort privacy."[50]

---

43. *Id.*

44. *Id.* at 196.

45. *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. LAW. REV. 1805, 1821 (2010) (noting a prominent example of state adoption of privacy as a right occurred in a 1905 Georgia case which found that a nonconsensual use of a plaintiff's picture in a newspaper was a "direct invasion" of the legal right to privacy).

46. *Id.* at 1823.

47. *Id.* at 1821; *see also* Richards & Solove, *supra* note 2 at 1888 (stating that for all the legitimacy Prosser gave privacy law, he stunted its development and limited its ability to adapt to the current digital information age. Prosser stripped privacy law of "any guiding concept to shape its future development").

48. *Id.* at 1823 (citing Craig Joyce, *Keepers of the Flame: Prosser and Keeton on the Law of Torts (Fifth Edition) and the Prosser Legacy*, 39 VAND. L. REV. 851, 892 (1986).

49. Citron, *supra* note 45, at 1821.

50. *Id.* at 1825.

In other words: "Prosser conceived of torts to redress harms, Brandeis and Warren cared about creating privacy rights."[51]

2. Legislatures Have Attempted to Evolve or Clarify Privacy Law Outside of the Prosser Torts

Due to the limits of Prosser's common law privacy torts to account for contemporary privacy harms, legislatures have instead created modern privacy statutes. However, statutory privacy law in the United States is based on a sectorial model, meaning different and separate privacy statutes relate to different specific economic sectors like education, video production, telecommunications, and other industries. Unlike the European Union, the United States does not have an all-encompassing, or "omnibus," privacy statute.

To give a non-exhaustive list of the United States sectoral privacy statutes, besides the Fair Credit Reporting Act (FCRA),[52] Congress has passed the following:[53] Fair and Accurate Credit Transactions Act (FACTA),[54] Cable Communications Policy Act (Cable CPA),[55] Video Privacy Protection Act (VPPA),[56] Telephone Consumer Protection Act (TCPA),[57] Privacy Act of 1974 (amended by the Computer Matching and Privacy Protection Act of 1988),[58] Right to Financial Privacy Act,[59] and the Electronic Communications Privacy Act of 1986 (ECPA).[60] Statutes like these address: (1) who can collect data or information; (2) what purposes the data can be used for; and (3) the procedural processes for using said data. Some of the statutes also grant a private right of action if the provisions of the statute are violated. But each statute only addresses a limited range of industry-specific privacy harms, and liability often hinges on whether a party has violated the express statutory language.[61]

51. *Id.* at 1823.

52. Fair Credit Reporting Act, 15 U.S.C. § 1681.

53. Brief for Electronic Privacy Information Center as Amici Curiae Supporting Respondents, TransUnion LLC, v. Ramirez 141 S.Ct. 2190, 4 (2021) (No. 20-297) [hereinafter EPIC Amicus Brief].

54. 15 U.S.C. § 1601.

55. 47 U.S.C. § 551.

56. 18 U.S.C. § 2710.

57. 47 U.S.C. § 227.

58. 5 U.S.C. § 552(a).

59. 12 U.S.C. §§ 3401–22.

60. 18 U.S.C. §§ 2510–23.

61. Mathew S. DeLuca, *The Hunt for Privacy Harms after* Spokeo, 86 FORDHAM L. REV. 2493, 2448 (2018); *see also* Facebook v. Duguid, 141 S.Ct. 1163 (2021) (holding that Facebook

The United States' sectoral approach to privacy laws underscores the need for U.S. privacy statutes to continually update as new technologies and industries emerge. In the last two years alone, Congressional representatives proposed multiple privacy bills to address privacy concerns with social media and Big Data collection.[62] Though none have been enacted, the many types of bills are a signal that privacy protection is a crucial topic of legislative concern.

C. WHY PRIVACY HARMS ARE DIFFICULT FOR COURTS, EVEN WITHOUT A CONFUSED STANDING DOCTRINE

Even without a narrowed standing doctrine or an ossified privacy common law, privacy harms are inherently difficult for courts to address. First and foremost, privacy harms are often intangible which makes them difficult to quantify for compensatory purposes. Moreover, privacy harms often comprise of many small, disaggregated instances of undetectable violations which only appear harmful in aggregation. Finally, privacy harms do not affect all populations equally, with marginalized populations more likely than the general population to have their privacy violated. Each of these aspects of privacy harms make it difficult for courts to match the harm with an appropriate compensatory remedy.

1. Privacy Harms are Intangible and Difficult to Conceptualize and Compensate

Privacy harms are inherently intangible. Some privacy harms can be emotional, like the anxiety that stems from identity theft, some might be categorized as reputational harms, and others involve risk of future harm created by an initial privacy violation.[63] With these varied categories, courts have particularly struggled to identify harms they can compensate, and have

---

could not be held liable for violation the Telephone Consumer Protection Act because it did not use an "automated dialing system" within the meaning of the statute.).

62. In 2020 alone, legislators have proposed multiple privacy bills such as the Data Protection Act by Sen. Kirsten Gillibrand (D-N.Y.), the Data Accountability and Transparency Act from Sen. Sherrod Brown (D-Ohio), the Consumer Online Privacy Rights Act from Sen. Maria Cantwell (D-Wash.), and the SAFE DATA Act and the House Energy and Commerce "bipartisan staff draft" from Sen. Roger Wicker (R-Miss.). Camerson F. Kerry & John B. Moris, *Framing a Privacy Right Legislative Findings for Federal Privacy Legislation*, BROOKINGS (Dec. 8, 2020), https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/.

63. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 810 (2022) [hereinafter Citron & Solove, *Privacy Harms*]; *see also* Daniel Solove & Danielle Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018) [hereinafter Citron & Solove, *Risk and Anxiety*].

either dismissed cases prematurely, or focused on harms that are not at the heart of a controversy, leading to "absurd results."[64]

The intangibility of privacy harms has not only baffled the courts, but also led to disagreements among privacy experts on how to classify privacy harms. Warren and Brandeis have stated the easiest way to capture privacy harms is to say that a subjective violation of privacy alone is the harm.[65] Other scholars, like Ryan Calo, view privacy harms as requiring two tests: a subjective inquiry, and an objective one.[66] In their latest article, Daniel Solove and Danielle Citron have created an entire typology of privacy harms, with fourteen distinct categories, including: reputational harms, control harms, emotional harms, and risk harms.[67] Each of Solove and Citron's harms can pose difficulties in litigation, particularly when courts try to apply a compensatory function to them.[68] For example, how should one be compensated for a loss of control over their data? Ignacio Cofone and Adriana Robertson, view privacy harms not as distinct categories, but as a spectrum of harms determined by how much other people know about a person.[69] However, even this approach has its own flaws as it only captures reputational interests in privacy, and even their model notes that privacy and reputation can be mutually exclusive at times.[70]

The intangibility of privacy harms has led to confusion among courts not just in how to frame the privacy right, but how or when to recognize a privacy harm.[71] For example, some courts have concluded that certain privacy violations, such as thwarted expectations, improper uses of data, and the wrongful transfer of data to other organizations are not recognized as harms.[72] Other courts have focused on downstream consequences, or the risk of future harms to plaintiffs from an original violation.[73] In other cases, courts have focused on narrow meanings of plain text in statutes, to the point where they have missed the key privacy rights that are at issue.[74] Courts also tend to focus on harms they are comfortable compensating, which forces plaintiffs to allege

64. EPIC Amicus Brief, *supra* note 53, at 6.

65. *See generally* ALAN F. WESTIN, PRIVACY & FREEDOM (1967).

66. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011).

67. Citron & Solove, *Privacy Harms*, *supra* note 63, at 18.

68. *Id.* at 4.

69. Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1039 (2018).

70. *Id.* at 1056.

71. EPIC Amicus Brief, *supra* note 53 at 7.

72. Daniel Solove, *Privacy Harms, Privacy and Security Blog*, TEACH PRIV. (Feb. 9, 2021), https://teachprivacy.com/privacy-harms/.

73. *Id.*

74. EPIC Amicus Brief, *supra* note 53, at 11.

compensatory or judicially cognizable harms, even if they do not go to the heart of the controversy.[75]

Given the abstractness of and courts' varying approaches to privacy rights and harms, it is not surprising that courts have struggled. This is what makes Congressional statutes necessary: they provide guidance to the courts.

2. Privacy Harms are Typically Disaggregated

Another issue with privacy litigation is that privacy harms are often disaggregated, or small harms that occur to many people or multiple times against one person.[76] The disaggregated nature of privacy harms can make them difficult to detect, even while they are profitable for bad actors to perpetuate. Disaggregation also makes designing a compensatory structure to remedy plaintiffs' individual claims more challenging.

Despite individual privacy harms being mostly small, these harms can add up to more than just minor inconveniences.[77] Citron and Solove argue that spread out over millions of people, disaggregated harms become aggregated harm from the standpoint of society.[78] Further, it can be difficult for individuals to find out about violations to their own privacy, and even "if they do, third parties ignore requests to correct them without real risk of litigation costs."[79]

One significant way that the disaggregation is addressed is by aggregating harms via class actions. However, class actions can create other problems, like putting companies with data of millions of people out of business for violations.[80] Courts are left trying to thread a needle. On the one hand, courts want to acknowledge and prevent companies from profiting off privacy violations; on the other hand, courts want to avoid causing company shakedowns or complete bankruptcy.[81]

---

75. Citron & Solove, *Privacy Harms*, *supra* note 63, at 43.

76. Daniel Solove, *Introduction: Privacy Self Management and the Consent Dilemma* 126 HARV. L. REV. 1880, 1881 (2013). For example, when many people receive the same unwanted email or one person receives hundreds of unwanted emails. "[M]any privacy harms are the result of an aggregation of pieces of data over a period of time by different entities. It is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer."

77. Citron & Solove, *Privacy Harms*, *supra* note 63, at 44.

78. *Id.*

79. Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*, 101 B.U. L. REV. ONLINE 62 (2021).

80. Eric Goldman, *The Irony of Class Action Privacy Litigation*, 10 J. TELECOMM. & HIGH TECH. L. 309, 314 (2012).

81. *Id.*

3. Privacy Harms Affect Marginalized Populations More, but Less Visibly

Finally, and not least importantly, privacy violations do not affect all populations equally. Privacy rights of those at the margins of society are most often violated. Harms committed against these populations are often neglected and unseen.[82]

The discriminatory effects of privacy harms are well documented. From over policing of black and brown neighborhoods and bodies (dating back to slavery)[83] to "the color of surveillance"[84] that uses national security as a preface to target privacy in Islamic communities,[85] racial and religious minorities' privacy rights are violated by the state at disproportionate levels. Policing also targets those of minority gender identities. In many states trans-people are constantly required to present private medical documentation about their transgender status when their gender markers do not match their government identification.[86] Welfare and government services also perpetuate disproportionate privacy harms by requiring low-income mothers to give up their privacy rights to receive Medicaid benefits and other state aid.[87]

These privacy impacts are not only propagated by the state, but also by individuals and companies. Women and minorities are subjected to online harassment, doxing, and other internet mob harms at disproportionate rates.[88] These are difficult cases to litigate because the harm is perpetuated by

82. Citron & Solove, *Privacy Harms*, *supra* note 63, at 29.

83. Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 442 (2017).

84. Alvaro M. Bedoya, *Privacy as Civil Right*, 50 N.M. L. REV. 301, 306 (2020); *see also* Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 21, 2016), https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html.

85. Saher Khan & Vignesh Ramachandra, *Post 9/11 surveillance has left a generation of Muslim Americans in a shadow of distrust and Fear*, PBS NEWSHOUR (Sept. 16, 2021), https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear; *see also* Fazaga v. FBI, 916 F. 3d. 1202 (9th Cir. 2019) (describing a mass dragnet surveillance effort by the FBI targeting multiple Southern California Islamic communities).

86. Scott Skinner-Thompson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673, 1710 (2017).

87. Khiara M. Bridges, *Privacy Rights and Public Families*, 34 HARV. J.L. & GENDER 113, 168 (2011); *see also* Hareem Mannan, *Data Privacy is a Human Right*, MODUS (May 16, 2019), https://modus.medium.com/data-privacy-is-a-human-right-cf36e1b45859 stating "Today, states subject single mothers who draw public assistance to drug tests, DNA testing of children, fingerprinting, extreme verification requirements, and intrusive questioning about intimate relationships."

88. Citron & Solove, *Privacy Harms*, at 28; *see also* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1870 (2019).

members or individuals who are "unable to pay enough in monetary damages to incentivize lawyers to litigate."[89] Further, companies using biased algorithms sell and use women and minority personal information that violates privacy and perpetuates stereotypes.[90] Moreover, marginalized communities are less likely to have access to "tech equity" than higher-income families, and are therefore less likely to be notified of privacy violations and take preventative or restorative measures.[91]

Addressing privacy violations is difficult enough without also having to also prove that algorithms are discriminatory and perpetuating biased harms.[92] Prosser's common law privacy torts do not address these disparate impacts. Marginalized communities instead must rely on evolving privacy statutes to increase their privacy equity.[93]

III. *TRANSUNION V. RAMIREZ*: A SUMMARY

This Section argues that *TransUnion v. Ramirez* worsens both the already problematic application of standing in federal courts, and the difficulties in addressing privacy harms.

Spokeo left an open question of what qualifies as a "concrete harm", in federal standing, but *TransUnion* only further confused the concrete harm definition. *Spokeo* also held that standing requires an intangible right to be a "traditionally recognized" right, but *TransUnion* specifically stated that "traditionally recognized rights" are only those rights with a common law analogue. Further, although *Spokeo* did not emphatically defer to Congress' judgement, *TransUnion* more clearly called into question whether Congress can create private rights of action or define new injuries at all in privacy.[94] Each of these holdings will limit the protection of privacy rights.

A. THE FACTS

Like Spokeo, TransUnion v. Ramirez involved a question of standing for a class action under the Fair Credit Reporting Act (FCRA).[95] The FCRA grants

89. Citron & Solove, *Privacy Harms*, *supra* note 63, at 29.

90. *Id.* at 30.

91. Mannan, *supra* note 87.

92. Citron & Solove, *Privacy Harms*, *supra* note 63, at 30. For a topical application of this problem, see also Theodore F. Claypoole, *COVID – 19 Privacy Protection and Persecuted Minorities*, X NAT'L L. REV. 142 (2020), https://www.natlawreview.com/article/covid-19-privacy-protection-and-persecuted-minorities.

93. Citron & Solove, *Privacy Harms*, *supra* note 63, at 30.

94. *See* Erwin Chemerinsky, *What's Standing After* TransUnion LLC v. Ramirez, 26 N.Y.U. L. REV. ONLINE 269, 279 (2021).

95. Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970).

plaintiffs a right of action to sue for violations.[96] TransUnion, as a credit reporting agency, is strictly regulated by the FCRA.[97]

In 2002, TransUnion created an add-on product called the OFAC Name Screen Alert. OFAC stands for Office of Foreign Assets Control. The OFAC is a subdivision of the U.S. Treasury Department that maintains a list of suspected terrorists, drug traffickers, and other serious criminals. TransUnion utilized a third-party software to search this OFAC list and placed an "OFAC alert" on any individual's credit report whose name was found on the list.[98] TransUnion did not use any other verification (such as birthdays or social security numbers) besides cross checking names.

Sergio Ramirez, the named plaintiff in *TransUnion*, attempted to buy a car when he was told by the dealership that they couldn't complete the transaction because he was on a suspected "terrorist list."[99] Ramirez immediately requested a copy of his credit file from TransUnion. However, the file TransUnion sent did not mention either the OFAC alert, or lay out his rights and the process to fix the faulty information.[100] The OFAC information eventually came in a separate standalone mailing.[101] Ramirez sued TransUnion and alleged three violations of the Fair Credit Reporting Act: (1) TransUnion did not follow reasonable procedures to ensure the accuracy of information in his file; (2) they failed to provide him with all the information in his file upon request; and (3) they violated their obligation to provide him with a summary of his rights.[102]

After learning that TransUnion had been previously sued for their OFAC product and hadn't altered their business practices, Ramirez brought a class action suit against the company. Each plaintiff had an inaccurate OFAC alert on their report and had not received any notice of this alert from TransUnion mailings. Before the trial, the parties stipulated that the class contained 8,185 members, and that 1,853 of those members had their credit reports disseminated to creditors during the seven-month stipulated time.[103]

A district court jury found that TransUnion had willfully violated the FCRA and awarded each class member $984 in compensatory damages and

96. *Id.* at § 1681n(a) ("Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer.").

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

98. *Id.*

99. *Id.* at 2202.

100. *Id.*

101. *Id.* at 2201.

102. *Id.*

103. *Id.*

$6,353 in punitive damages.[104] TransUnion appealed, stating the plaintiffs did not have standing. The Ninth Circuit, which decided *Spokeo* four years previously, affirmed the jury verdict and found that the class had Article III standing. The Supreme Court granted certiorari to address whether the entire class had standing.

B. THE HOLDINGS

The Supreme Court ultimately ruled that only those plaintiffs in the class that had their information sent to third parties had suffered a "concrete harm" sufficient for Article III standing.[105] The Court also explicitly held that Congress is limited in its ability to create new rights.[106]

1. "A Nonconcrete 'Concrete Harm' Definition"

The Court attempted to address the open question from *Spokeo*—to define what makes an injury "concrete."

The Court first stated that concreteness is a separate inquiry from whether a statute has been violated because "an injury in law is not an injury in fact."[107] The Court then reiterated its holding in *Spokeo* that both intangible and tangible injuries could be deemed concrete. However, for intangible harms to be "concrete," they had to bear a "close relationship with the harm traditionally recognized at common law."[108] The Court then used Prosser's four privacy torts as examples of "traditionally recognized" intangible harms.[109] Finally, the Court reiterated its holding in *Spokeo* that a "bare procedural violation" would not alone satisfy the definition of concrete harm, even if it was attached to a statute.[110]

2. Risk of Harm is Limited to Injunctive Relief

The *Spokeo* Court had held that the "risk of real harm" can sometimes "satisfy the requirement of concreteness."[111] However, allegation of risk of harm may only provide standing for injunctive relief, rather than for damages.[112] This is true even if Congress has directly prescribed statutory damages for procedural privacy violations that increase the risk of privacy

104. *Id.*
105. *Id.* at 2203.
106. *Id.* at 2205.
107. *Id.*
108. *Id.*
109. *Id.* This is despite the fact that Prosser had only created the categories in the 1960's and trickled into state common law in the following decades.
110. *Id.*
111. *Id.* at 2210.
112. *Id.*

harm.[113] The Court used an example of a woman getting safely home after being nearly hit by a reckless driver, stating that the near miss would be a cause for celebration, not a suit, because the harm did not occur.[114]

3. Usurpation of Powers vs. Separation of Powers

In an even more concerning turn, the *TransUnion* opinion placed direct limits on Congress's power to create new rights and injuries, contrary to nearly every other previous standing case. The *TransUnion* Court reasoned that though Congress may elevate injuries that exist in the "real world" to actionable legal status, Congress could simply enact an injury into existence, transforming something "that is not remotely harmful into something that is" using lawmaking power.[115] In other words, even if Congress had defined a harm in a statute, a plaintiff who alleges that harm would not have standing unless the harm still meet the Court's definition of concreteness.[116] The Court couched this statement in the idea that federal courts should only redress real harms rather than hold defendants accountable for "legal infractions."[117]

The opinion continued to state that allowing Congress the power to grant private citizens standing to enforce their privacy rights would infringe on the Executive Branch's Article II authority.[118] According to the Court, only the Executive Branch can choose how to prioritize and how aggressively to pursue legal actions against defendants who violate federal statutes.[119] Private plaintiffs, the court reasoned, are not accountable to the public and are not charged with pursuing the public interest in enforcing compliance with regulatory law.[120]

Even defining minimum statutory damages would not make a statutory violation a recognizable harm by the Court.[121] The court explained that if a

113. *Id.*
114. *Id.* at 2211.
115. *Id.* at 2205.
116. *Id.*
117. *Id.*
118. *Id.* at 2207.
119. *Id.*
120. *Id.*
121. Molly McGinnis Stine, Tara L. Trifon & Lindsey E. Kress, *Facts Matter*- TransUnion's *Impact on Privacy Cybersecurity Litigation*, BLOOMBERG L. (July 19, 2021), https://news.bloomberglaw.com/us-law-week/facts-matter-transunions-impact-on-privacy-cybersecurity-litigation. This Note does not address here the other jurisdictional impacts of this standing law (standing is in essence a jurisdictional decision) "[m]oreover, as Justice Clarence Thomas points out in his dissent, the court has "ensured that state courts will exercise exclusive jurisdiction over these sorts of class actions" by finding that the federal courts lack jurisdiction."

private plaintiff were permitted to rely solely on statutory damages, the holding could authorize "virtually any citizen to bring a statutory damages suit against virtually any defendant who violated virtually any federal law."[122] Arguably, however, this is exactly what Congress has always had the power to do.

4. Applying the Holdings to the Case

The Court assumed the plaintiffs were correct and that TransUnion did violate its obligations under the Fair Credit Reporting Act.[123] However, the Court stated that despite these violations, only the plaintiffs who had their faulty information sent to third parties had suffered a concrete harm.[124]

Because the Court's previous definition of standing in *Spokeo* required intangible harms to be analogous to a traditionally recognized harm, the plaintiffs had alleged that their harms were analogous to defamation.[125] Defamation, however, requires false information to be published to a third party, and only 1,853 plaintiffs' information was distributed outside of TransUnion.[126] According to the Court, "the mere presence of an inaccuracy in an internal credit file, if not disclosed, causes no concrete harm."[127]

Lastly, the Court ruled that only Ramirez had standing for the failure of TransUnion to provide the OFAC alert on his credit report with his credit report summary and a summary of his rights.[128] The other plaintiffs did not adequately prove that they either had not received the OFAC alert or that it came separately from their full credit report, both of which would have violated the procedural requirements of the FCRA.[129] The United States, as amicus curiae, asserted that the plaintiffs suffered a concrete "informational injury." But the Court held that these were "bare procedural violations" divorced from any concrete harm.[130]

Even if the other plaintiffs had proven the existence of these procedural violations, the Court reasoned that having "information disseminated in the improper format" was not a harm traditionally recognized at common law and that the plaintiffs did not demonstrate how the improperly-formatted information hindered correcting their files.[131] Plaintiffs understandably argued

122. *TransUnion*, 141 S.Ct. at 2207.
123. *Id.* at 2208.
124. *Id.* at 2209.
125. *Id.* at 2208.
126. *Id.* at 2209.
127. *Id.* at 2209.
128. *Id.* at 2213.
129. *Id.*
130. *Id.*
131. *Id.* at 2214.

these "formatting violations" created a risk of harm that their inaccurate information would be disseminated, because they would have had no way to correct the faulty OFAC alert if they had not received information that it was attached to their report.[132] However, the Court countered, reasoning that the plaintiffs did not prove they would have tried to correct their files even if they had received the information.[133] Lastly, even if each plaintiff had sufficiently alleged a risk of harm, this risk only constituted an injunctive claim and not one for damages.[134]

C. JUSTICE THOMAS'S DISSENT

Justice Thomas wrote a particularly sharp dissent against the majority opinion.[135] The liberal Justices Sotomayor, Kagan, and Breyer wrote a separate dissent while joining Justice Thomas in most of his.

Justice Thomas first pointed to the odd evolution of the Court's standing doctrine, and its application in this case to individual rights. He acknowledged the history of standing, and that "injury in fact" was coined by the Court in *Association of Data Processing*.[136] He stated that even after the injury in fact requirement was grafted onto a Constitutional analysis in *Warth v. Seldin*, the test was still an additional way to get into federal court when the plaintiff could not point to a violation of a statutorily created personal right or constitutional right.[137] The injury in fact test instead broadened the different types of harms plaintiffs could allege to achieve standing as long as they still alleged personal harm.[138]

Justice Thomas then distinguished *Lujan* as a public interest case rather than a case about individual rights. He reasoned that historically, when an individual sought redress for a private right, a violation of that right alone would suffice for standing. Trespass, for example, requires no proof that an individual's property is harmed. The act of trespass itself constitutes a sufficient violation of a right.[139] Copyright provides another example where individuals could sue for infringement of their rights without proving monetary loss.[140] On the other hand, if a plaintiff sued based on the violation of a duty owed to a community, then the courts required a legal injury AND

132. *Id.* at 2212.
133. *Id.*
134. *Id.*
135. *Id.* at 2215 (Thomas, J., dissenting).
136. *Id.* at 2219.
137. *Id.*
138. *Id.* at 2215.
139. *Id.*
140. *Id.*

provable damages, which has come to be known as an "injury in fact." This distinction mattered for both common law public rights and new statutory rights.[141] The majority opinion rejected standing's history of Congressional deference. Justice Thomas then suggested that the test should be clear: for an individual harm "so long as a statute fixes a minimum recovery there would seem to be no doubt of the right of one who establishes a technical ground of action to recover this minimum sum without any specific showing of loss."[142] Here, all three duties in the FCRA were owed to individuals, not communities, and Congress fixed a minimum sum of statutory damages.[143]

Justice Thomas then reprimanded the majority for its treatment of separations of powers. He cautioned that if the majority opinion were taken to its logical conclusion:

> [n]o matter if the right is personal or if the legislature deems the right worthy of legal protection, legislatures are [now] constitutionally unable to offer the protection of the federal courts for anything other than money, bodily integrity, and anything else that this Court thinks looks close enough to rights existing at common law. The 1970s injury-in-fact theory has now displaced the traditional gateway into federal courts.[144]

The Court had never before declared that a legal injury is inherently insufficient, or that legislatures are constitutionally precluded from creating legal rights if they deviate too far from their common law roots.[145] "In the name of protecting the separation of powers, . . . [the] Court has relieved the legislature of its power to create and define rights."[146] Justice Thomas then reasoned that by applying their rule to the facts of this case, the majority skipped over much of its own precedent on what constituted an injury.[147]

IV. ANALYSIS: HOW TRANSUNION WORSENS THE PROBLEMS WITH PRIVACY RIGHTS AND LITIGATION.

TransUnion v. Ramirez made the Supreme Court's narrowing of standing and the enforcement of privacy rights more difficult, more extreme, and more permanent. The decision will both limit privacy rights now and make it less likely that privacy rights can be adequately protected in the future.

141. *Id.*
142. *Id.*
143. *Id.* at 2218 (quoting FCRA).
144. *Id.* at 2221 (citations omitted).
145. *Id.*
146. *Id.*
147. *Id.*

First, by holding that "the right kind of harm" for intangible injuries are only those with a common law analogue, the Court blatantly overstepped its boundaries as the judiciary and limited the legislative powers of Congress to create new rights by statute. Second, the Court did not provide an adequate definition of "concrete harm." This inadequacy will alter the purpose of privacy law and will continue to confuse lower courts in privacy cases. Third, the decision disincentivizes enforcement of privacy rights by allowing privacy violators to "pay to play" and by disregarding risk as a harm. Finally, the *TransUnion* decision limits privacy rights from evolving to regulate new technologies and recognize new harms.

A. TRANSUNION RESTRICTS CONGRESS'S POWER TO DEFINE PRIVACY HARMS AND REMEDIES IN A SEPARATION OF POWERS FAKEOUT

If *Spokeo* danced around a limitation of legislative powers,[148] the Court in *TransUnion* went further and held that Congress cannot enact an injury that, according to the Court, did not already "exist in the real-world."[149] But this is a usurpation of Congress's powers. As Erwin Chemerinsky contends, "[i]f one starts with the premise that Congress has the constitutional power to create legally enforceable rights—which seems unassailable—then the Supreme Court's refusing to enforce them greatly undermines, not advances, separation of powers."[150] The *TransUnion* decision prevents Congress from using their constitutional power to define harms and remedies. The Court questions Congress's ability to (1) define substantive rights; (2) promote the importance of procedural rights to mitigate future risk of harm; and (3) outline remedies for hard to compensate harms.

In *TransUnion*, the Court first questioned Congress's ability to define substantive harms, and in the process, usurped that power for itself. The Court held that the inaccurate OFAC alerts on reports that *TransUnion* recklessly created were not substantive harms, and would only become substantive if disseminated to third parties.[151] Yet, when Congress created the FCRA, they specifically looked to *discourage* dissemination of inaccurate data, not just redress dissemination after it occurred. As Felix Wu argues, "[w]hen courts deny standing . . . on the basis of the injuries being "insufficiently concrete they . . . are deciding the substantive content of those rights. Far from supporting an appropriate separation of powers, this move amounts to a

148. *Id.*
149. *Id.*
150. Chemerinsky, *supra* note 94, at 123.
151. *TransUnion*, 141 S.Ct. at 2212.

usurpation of legislative power by the federal judiciary."[152] The Court usurped Congress's ability to define a substantive injury under the FCRA, thereby "shift[ing] locus of control over development of the law."[153]

Second, the Court limited Congress's ability to define procedural harms, through its holding that TransUnion's failure to send proper notice of a consumer's OFAC alert or their summary of rights was a "bare procedural violation" and not a concrete harm.[154] The FCRA requires consumer reporting agencies to (1) provide consumers with information in their file; (2) give consumers access to their rights and a process to fix mistakes; and (3) provide the methods they use to maintain reports' accuracy. These procedural provisions ensure better protection against the more substantive harm of a company disseminating a consumer's inaccurate information. They also give consumers information about how their data is used, something that is often unknowable for data privacy violations.[155] Without procedural rights, plaintiffs are not informed, and their risk of substantive harm increases, counter to Congress's goals.

Finally, Congress often defines remedies in statutes, including how remedies can be sought and by whom. This can include statutory damages and private rights of action. The *TransUnion* Court explicitly limited Congress's choices by holding that statutory damages are not enough to allow plaintiffs standing because that could authorize "virtually any citizen to bring a statutory damages suit against virtually any defendant."[156] Yet, for cases that do not involve statutes "with statutory damages, harm can become quite a speculative matter."[157] Judges sometimes refuse to recognize harms in a statute when compensation is uncertain for fear of bankrupting a company.[158] Statutory damages allow Congress to provide guidance to courts where, like privacy violations, the harms are hard to quantify. Statutory damages can also encourage risk reduction by violators but also cap damages to avoid potential bankruptcy. Statutory damages also help courts account for risk of future harms[159] Instead of recognizing Congress's choice to use statutory damages

152. Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DE PAUL L. REV. 439, 458 (2017); *see also* Daniel Townsend, *Who Should Define Injuries for Article III Standing?*, 68 STAN. L. REV. ONLINE 76, 81 (2015).

153. Wu, *supra* note 152, at 451.

154. *Id.* at 2211.

155. Citron & Solove, *supra* note 79.

156. *TransUnion*, 141 S.Ct. at 2212.

157. Citron & Solove, *Privacy Harms*, *supra* note 63, at 45.

158. *Id.* at 44.

159. *Id.* at 47.

provisions to allow plaintiffs better redress and access to "forcing tired old judicial concepts of harm into the enforcement of . . . statutes."[160]

B. TRANSUNION DISINCENTIVIZES ENFORCEMENT OF PRIVACY RIGHTS

A law is only good if it is enforced.[161] Society has a stake in protecting privacy and personal information. These protections promote rules of civility, guard individuals and communities in their ability to be creative, and are essential to democracy and free expression.[162] The *TransUnion* decision limits enforcement of privacy rights and therefore limits the effectiveness of privacy law. First, the Court limits plaintiffs' use of private rights of action as an enforcement tool. Second, the Court limits the recognition of risk of future harm as a prophylactic enforcement mechanism against future privacy risks, particularly in the world of Big Data.[163] These limitations make it more likely that bad actors will find it more profitable to commit privacy violations than be punished for said violations.

1. TransUnion Binds Congress's Use of Private Rights of Action as an Enforcement Mechanism

The Court's decision limits the ability for plaintiffs to be their own enforcers against companies, aggregating their harms together and holding entities accountable through private rights of action.

Private rights of action are used by Congress as an enforcement mechanism for privacy statutes.[164] Private rights of action also alleviate reliance on regulatory agencies, which is often necessary as "[n]early all regulatory agencies are significantly . . . under-resourced, and they cannot enforce in every case."[165] The bounty created by private right of actions, in the form of statutory damages, further disincentivizes harm by entities and provide redress for consumer rights. Congress also carefully considers the impacts of private rights

160. *Id.* at 45.

161. EPIC Amicus Brief, *supra* note 53, at 5 ("Privacy rights and their corresponding obligations are only effective if they are enforceable.").

162. Citron & Solove, *Privacy Harms*, *supra* note 63, at 46.

163. Big Data is defined as data that has more "volume," "velocity," and "variety," than normal data sets, allowing for greater value, visualization of data, and more information that can be pulled and analyzed in greater accuracy. *See* U. WIS. EXTENDED CAMPUS, WHAT IS BIG DATA? (2015), https://uwex.wisconsin.edu/stories-news/what-is-big-data/.

164. EPIC Amicus Brief, *supra* note 53, at 8; *see also* Citron & Solove, *supra* note 79, at 35 (citing Spencer Weber Waller, Daniel B. Heidtke & Jessica Stewart, The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology, 26 LOY. CONSUMER L. REV. 343, 375 (2014)).

165. *Id.*

of action before placing them in a statute.[166] Private actions are often the most hotly contested part of any statute—that is, they are seldom granted and only after serious debate.[167] This care and deliberate decision-making by Congress deserves more judicial deference.[168]

Instead of relying on how common private rights of actions are for privacy rights, the benefits they create for enforcement, or the care Congress takes in granting them, the Court in *TransUnion* held that only plaintiffs who had their faulty information disseminated could allege a private action.[169] To provide an example of their policy concerns, the Court reasoned that they did not want a person in Hawaii filing a federal lawsuit against a company for damaging someone else's property in Maine.[170] However, this example is particularly illogical in the context of privacy rights, because privacy rights are individualized.[171] Unlike environmental suits, in which the harm against one part of the planet may cause downstream harm in another part of the planet, most people are unlikely to sue on behalf of another's violated privacy rights. Justice Thomas's dissent noted that historically, when plaintiffs seek enforcement of an individual right, the violation of that right alone was enough for standing.[172] Further, the example given by the Court could still be resolved by analyzing whether a plaintiff has a connection to a harm, rather than whether the Court wants to recognize the harm itself.

Finally, given that privacy harms are often small harms disaggregated across many individuals, it is more likely that privacy violators will be held to account if a larger group of plaintiffs is able to bring small claims together in one suit. Otherwise, bad actors will do exactly what TransUnion did when it

166. Citron & Solove, *Privacy Harms*, *supra* note 63, at 49. Elucidating an example of a "professional plaintiff" enforcing TCPA actions in *Stoops v. Wells Fargo Bank* "Stoops may have been opportunistic, but her motives does not negate the harm-inflicted upon her. Trying to catch a wrongdoer does not mean that one is unharmed by the wrongdoer's actions in the process. Ultimately, however, harm should not be relevant to the Stoops case. Congress wrote the private right of action under the TCPA without a requirement of harm. Deterrence is the goal, not compensation."

167. *Id.* at 51.

168. *Id.*

169. TransUnion LLC v. Ramirez, 141 S.Ct. 2190, 2207 (2021).

170. *Id.* at 2205.

171. *See* Wu, *supra* note 152, at 458 ("The vast majority of privacy and security cases, though, are indeed ones involving individual rights, not merely broad questions of public interest. Almost invariably, privacy plaintiffs are specific individuals who claim that their own personal information has been mishandled in some way. That mishandling then provides the factual basis for their legal claims under statutory or common law.").

172. *TransUnion,* 141 S.Ct. at 2217 (Thomas J., dissenting) (comparing public and community interest suits versus suits over individual rights).

was originally sued for its OFAC alerts in 2005; pay off individual lawsuits rather than change business practices because it's more profitable.

The Court's decision keeps plaintiffs that Congress specifically sought to protect out of the federal court system. This limits the ability for plaintiffs to be their own enforcement mechanism against privacy violators.

2. *The TransUnion Court Severely Restricts Risk of Harm as a Harm, Limiting Prophylactic Privacy Enforcement*

Another inherent challenge with enforcing privacy rights is that an initial privacy violation creates a significant risk of future harms. Such risk is particularly present for privacy violations that qualify as "data breach harms" and "data quality harms."[173] This is because the full scope of the harm stemming from a data breach depends on how the data is used and with whom the data is shared.[174] Privacy statutes like the FCRA try to mitigate this risk by discouraging wrongful dissemination of data before it happens.

Despite holding in *Spokeo* that the risk of harm could meet the definitional test of a "concrete harm,"[175] the Court in *TransUnion* limited using the risk of harm to enforce privacy rights. At any given point, TransUnion could have sold the credit report of a consumer with a mistaken OFAC alert.[176] As Justice Thomas said in his dissent, 25% of the plaintiffs in the TransUnion class already had their information disseminated in only the seven-month time period stipulated for the case.[177] The Court still held that there was not a sufficient risk that TransUnion was likely to release plaintiffs' inaccurate information intentionally or accidentally.[178] The Court did not clarify what would constitute enough risk for standing.[179]

Even before *TransUnion's* lack of a conception of risk, cases dealing with risk as a privacy harm have been decided arbitrarily with different plaintiffs receiving different decisions about their ability to litigate the same claims.[180]

---

173. Citron & Solove, *Risk and Anxiety*, *supra* note 63, at 744.

174. Citron & Solove, *Privacy Harms*, *supra* note 63, at 45. Company A may sell stolen or inaccurate data to Company B, who might sell pieces of that data to Companies C and D (and so on).

175. Spokeo, Inc. v. Robins, 578 U. S. 330, 341–42 (2016).

176. *TransUnion*, 141 S.Ct. at 2210.

177. *Id.* at 2214.

178. *Id.* at 2212 (stating "no evidence establishes a serious likelihood of disclosure").

179. *Id.* at 2210.

180. DeLuca, *supra* note 61, at 2453, n.111. *Compare* Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (concluding that the plaintiffs had not established standing), *with* Remises v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696–97 (7th Cir. 2015) (holding that standing had been properly established regarding future risk of identity theft); *see also* Citron & Solove, *supra*

This arbitrariness between cases will likely only increase after the Court limited the use of risk without defining how much risk of future data harm would constitute standing. At worst, plaintiffs may be unlikely to allege risk of harm as a cognizable harm at all, preventing their ability to halt privacy harms before they happen.

Not only did the Court not clarify what would be enough risk, but they also did not specify what would be enough proof of this risk, only holding that the plaintiffs had not provided enough evidence.[181] Plaintiffs claimed that TransUnion's failure to provide all information about their credit reports or a summary of their rights increased their risk that their inaccurate data would be disseminated.[182] However, the Court reasoned that plaintiffs provided no proof that plaintiffs had even opened mailings about their credit reports, or would have acted on the information.[183] The Court did not explain how plaintiffs could have proven they would have read mailings that had never been sent to them. Unnecessary assumptions aside, requiring proof to some non-specified standard before plaintiffs can enter the courtroom will simply keep many plaintiffs outside of it.

The Court's misconception also disregarded the fact that risk can be a privacy harm on its own. The Court wanted plaintiffs to show that the harms are "visceral" or easy to see, measured, and "vested" in the here and now.[184] Because of the disaggregated and often undetectable nature of data harms, showing that future harms are "easy to see" is inherently difficult. Plaintiffs are unlikely to know or be able to control what happens with their information until it is too late.[185] The Court's very odd example of an averted car crash as cause for celebration misapprehends how law holds people accountable for reckless driving and other risk creating behaviors. Privacy law should not be any different.

C. THE TRANSUNION COURT LIMITS THE EVOLUTION OF PRIVACY RIGHTS

The Court's decision also matters because privacy needs to be able to evolve. For decades, the Supreme Court had upheld Congress's ability to create

note 79 (stating that Courts recognized many types of privacy harm but have consistently struggled in privacy and data breach context over other types of harms).

181. *Id.*

182. *Id.*

183. *Id.*

184. Citron & Solove, *Risk and Anxiety*, *supra* note 63, at 754 (quoting Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011)) (emphasizing that a quantifiable [rather than speculative] risk of damage" is necessary to establish data harm).

185. Citron & Solove, *supra* note 79, at 32.

new rights via statute.[186] That ability to create new rights is especially important for privacy because, as stated previously in this Note,[187] the common law does not accommodate modern privacy harms.

1. *The Court's Focus on Concrete Harms and Common Law Analogues Further Confuses and Ossifies Privacy Law*

The Court in TransUnion reiterated that to have standing, a plaintiff must have been "concretely harmed." Then, the Court stated that intangible concrete harms, as oxymoronic as that phrase is, will only create standing if they have a traditionally recognized common law analogue. However, modern privacy issues, such as for biometric privacy, data breaches, and others, all lead to intangible harms, and none have a common law analogue.[188] The Court's definition of harm is illogical, unnecessary, and stunts privacy law's evolution, instead ossifying privacy law.

First, even though the Court held that both tangible and intangible harms could meet the Court's concreteness standard,[189] there is an "obvious linguistic contradiction" with this definition of harm.[190] As an amicus brief filed by the Electronic Privacy Information Center (EPIC) pointed out, any cursory glance in a dictionary would note that intangibility is the opposite of concrete.[191] The majority tried to work around this contradiction by saying that intangible harms could be concrete if they closely matched a traditional harm at common law.[192] However, even this definition of "traditionally recognized harm" is inappropriately limited. Harms outside of the common law such as Constitutional rights violations, statutory rights, and inherent natural rights have all been previously traditionally recognized in American courts, and these rights are necessary to compliment or gap-fill common law.

While the Court specifically points to Prosser's four privacy torts as examples of concrete intangible harms at common law, the Court does not give any reason why something created in the 1960's is old enough to be "traditionally recognized." Nor does the court even recognize that these four common law privacy torts, and many others, are state law torts, with differing

186. Chemerinsky, *supra* note 94 at 101.

187. *See supra* Part II.C.1.

188. Kerry & John B. Moris, *Framing a Privacy Right Legislative Findings for Federal Privacy Legislation*, BROOKINGS (Dec. 8, 2020). https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/ Brookings.

189. *Spokeo*, 578 U.S. at 340.

190. *See In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 637 (3d Cir. 2017).

191. EPIC Amicus Brief, *supra* note 53, at 6.

192. *TransUnion,* 141 S.Ct. at 2204.

interpretations in any given state. The Court cannot and did not explain which states' version of Prosser's torts Congress would be allowed to legislate under. Further, Congress has designed many modern privacy statutes to specifically meet needs not addressed by Prosser's four torts – a fact that was made more stark when the Court itself did not apply one of Prosser's torts to the harm alleged by Ramirez and the class, and instead looked to defamation as a rough fit.[193]

The Court further does not address the fact that the common law is supposed to change and evolve.[194] When Warren and Brandeis wrote their original article on the right to privacy, they aimed to generate new causes of action, viewing the common law as "progressive, not regressive"[195] The *TransUnion* decision does not account for Warren and Brandeis's view of privacy or at what point evolutions of the common law will become "traditionally recognized." By keeping privacy law as it was conceived sixty years ago, the Court all but ensures privacy will remain ossified, creates broad confusion in future litigation and disserves the public whose privacy rights will be violated in new and changing ways.[196]

2. *TransUnion's Holdings are Functionally Inapposite to Modern Privacy Needs*

Privacy law in the United States is already limited in its ability to address future privacy threats because privacy is regulated by specific statutes connected to specific economic sectors.[197] It is unknown what privacy issues will exist in the future. Yet, the Court in *TransUnion* said that Congress cannot "simply enact an injury into existence."[198] This language limits Congress's ability to regulate new industries or potential privacy harms that have yet to be conceived.[199] It also prevents Congress from better defining privacy harms and making privacy protection more equitable.

Privacy is a salient issue for Congress. In the last few years, multiple members of Congress have proposed a wide variety of privacy bills to address

193. EPIC Amicus, *supra* note 53, at 11.

194. Citron & Solove, *supra* note 79.

195. Citron & Solove, *Privacy Harms*, *supra* note 63, at 51.

196. Citron & Solove, *supra* note 79; *see also* DeLuca, *supra* note 61, at 2452; Solove & Citron *Risk and Anxiety*, *supra* note 63, at 744 (referring to data breach harms as "akin to attempting to tap dance on quicksand").

197. Citron, *supra* note 45, at 1825.

198. *TransUnion*, 141 S.Ct. at 2215.

199. *See supra* Part IV.A (discussing the Court's overstep of Congress's legislative powers).

modern privacy issues such as biometrics, Big Data, and deep fakes and other misinformation stemming from privacy harms.[200]

These issues are not theoretical. For example, scholars like Kate Crawford have posited that Big Data harms resulting from inaccurate aggregation of data evade current privacy regulations and "may create additional harms by rendering inaccurate profiles that nonetheless impact an individual's life and livelihood."[201] Privacy laws need to be able to adapt to these harms as data collection becomes more sophisticated. Attitudes and legislation aimed on biometric privacy are also currently nuanced and evolving.[202] State courts have already confronted procedural issues with biometric privacy such as notice and consent under state biometric privacy statutes[203] Federal legislation needs to evolve to provide clear guidance and avoid inconsistent litigation between state and federal courts.

Finally, privacy needs to be able to evolve to better protect those that are most likely to be impacted. Right now, there is no common law analog for privacy protection under a federal cyber-harassment law. There is no current protection for the bias in using surveillance and facial recognition against people of color and religious minorities. The law is not yet evolved to mitigate the disproportionate impact of privacy harms, and it needs to be able to do so if privacy is to be equitable.

The TransUnion decision prevents privacy law from making necessary changes right when it most needs to evolve to regulate new industries and violations, as well as to better protect vulnerable communities.

D. LOWER COURTS NEED GUIDANCE IN PRIVACY CASES BUT TRANSUNION DOES NOT PROVIDE THAT GUIDANCE

After *Spokeo*, lower courts have already struggled to determine which intangible injuries would be concrete, leading to inconsistent and absurd results.[204] The *TransUnion* decision does not provide any more clarity for lower courts in their privacy standing analysis, and might have even made the analysis more confused.

---

200. *See* Kerry & Morris, *supra* note 62.

201. Kate Crawford & Jason Schultz, *Big Data and Due Process: Towards a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014).

202. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107 (2019).

203. *Id.* at 143; *see also* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186 (holding there had been no sufficient harm alleged because harm needed to be more than a violation of the statute). *But see* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019) (holding that the violation of the statute alone was enough to constitute harm).

204. EPIC Amicus Brief, *supra* note 53, at 6.

1. Because TransUnion Did Not Clarify Specific Definitions of Harm, Privacy Cases in Lower Courts Will Continue to be Inconsistent

After *Spokeo*, the Court's lack of guidance for what counts as a traditionally recognized harm "led some courts to shift the goalposts for concreteness away from the violation of the data protection right and toward a consequential harm standard."[205] A consequential harm standard requires either proof of specific damages from the violation of privacy or proof of a separate tangible injury outside of the privacy violation. But this has led to courts focusing on issues that are not at the heart of the privacy matter.

To illustrate, after *Spokeo*, in *In re iPhone Application Litigation*,[206] plaintiffs alleged that Apple breached its privacy policy by engaging in unauthorized transmission of information. The Court held that the plaintiffs had sufficiently alleged a harm by stating that the unauthorized data transmission taxed their phone's battery and used up phone storage.[207] A taxed battery is a very separate harm from unauthorized data transmission. In another case, *Mey v. Got Warranty Inc.*,[208] the Court held that unwanted calls violating the Telephone Consumer Protection Act caused concrete injury by depleting consumer's cell phone limits and battery life.[209] Again, this had nothing to do with the heart of the privacy violations.

In even other post-*Spokeo* cases, lower courts questioned whether the extent of the violation alleged was enough to merit standing and concluded with different answers.[210] For example, the Eleventh Circuit held in *Salcedo v. Hanna* that the receipt of a single text was not enough to constitute harm,[211] but the Eighth Circuit, in *Golan v. FreeEats.com*, Inc.[212] held that "it does not matter that the harm from an unsolicited call was minimal; in the standing analysis, we consider the type of the harm, not its extent."[213]

Lower courts are in the same position they were after *Spokeo*, with no clear guidance. *TransUnion* did not clarify what makes an intangible harm concrete. It did not clarify how much intangible harm is concrete. The only definitional information lower courts have now that they didn't have before *TransUnion* is that "traditional harms" are harms recognized at common law. The Court did

205. *Id.* at 8; *see also* Chemerinsky, *supra* note 94, at 279.

206. Citron & Solove, *Privacy Harms*, *supra* note 63, at 43.

207. *Id.*

208. Mey v. Got Warranty, Inc., 193 F. Supp. 3d 641 (N.D.W. Va. 2016); *see also* Citron & Solove, *Privacy Harms*, *supra* note 63, at 43.

209. Citron & Solove, *Privacy Harms*, *supra* note 63, at 43.

210. EPIC Amicus Brief, *supra* note 53, at 4.

211. Salcedo v. Hanna, 936 F.3d 1162, 1172 (11th Cir. 2019).

212. Golan v. FreeEats.com, Inc., 930 F.3d 950, 959 (8th Cir. 2019).

213. EPIC Amicus Brief, *supra* note 53, at 7.

not explain what is enough of an analogy between a privacy harm and the common law to constitute standing, or whether intangible harms can be compensated. The only example the Court gave was Prosser four common law torts, which modern privacy statutes do not fit neatly under. Therefore, inconsistencies in privacy cases, and lower courts' focus on the wrong harms are only likely to continue.

2. TransUnion Puts Courts in an Untenable Tug of War to Override the Court or Override Congress's Judgment

Even if Congress had explicitly granted a private right of action, defined the harms that allow for that action, and provided express minimum statutory damages, the *TransUnion* decision could still require a lower federal court to override Congress.[214] The Court believes it is its duty to make sure that federal courts mind their own business.[215] But as Erwin Chemerinsky notes, this "requires defining what their business is."[216] The Court seems to forget that "the federal courts are not [entirely] common law courts. Under the Constitution, Congress gets to decide whether to flood the federal courts. For the federal courts to make this decision is to upend the constitutional order."[217]

Because the Court has questioned Congress's powers under Article III standing, which is a jurisdictional question entirely under the purview of the Court, the decision means Congressionally defined harms that do not meets the Court's definition fail on constitutional grounds rather than the merits of case.[218] Plaintiffs would therefore be unable to change a decision through the federal legislature. Lower federal courts would have to determine whether the constitutional power of Article III as defined by the Supreme Court triumphs over Congress's Article II powers. This battle removes the proper focus on a case or controversy, placing lower courts in an untenable position and hindering any ability to allow case law to progress privacy law.

V. CONCLUSION

The original policy goal of the Supreme Court in the evolution of its standing doctrine was to require plaintiffs to assert an actual harm that they themselves had suffered, rather than harms that only applied to a

214. Wu, *supra* note 152, at 440.

215. TransUnion LLC v. Ramirez, 141 S.Ct. 2190, 2203 (2021).

216. Chemerinsky, *supra* note 94, at 123.

217. Wu, *supra* note 152, at 459 (citing Toby J. Stern, *Federal Judges and Fearing the "Floodgates of Litigation,"* 6 U. PA. J. CONST. L. 377, 399 (2003).

218. *Id.* at 451.

community.[219] The Supreme Court took this analysis of standing—one that was supposed to only apply to claims that asserted public statutory rights—and slowly grafted that analysis onto all constitutional Article III standing analyses.[220] In *Spokeo*, the Court took this bootstrapped constitutional definition to an illogical extreme by applying it to an individual privacy right under the FCRA.[221]

TransUnion was a strange case for the Court to enact an even more narrowed definition of standing. The company was previously sued in 2005 for the exact same harm, and yet, it had not changed any of its business practices, finding it more profitable to continue selling the faulty OFAC reports.[222] The case also contained a class of people who, under the definition of the FCRA, were unambiguously individually harmed.[223] Finally, the Court had a unanimous jury verdict, and the very rare jury note admonishing TransUnion directly.[224]

Nonetheless, *TransUnion* accelerated the Court's illogical evolution of standing by holding that intangible harms must be concrete and relate to a common law analogue, and Congress cannot enact new harms outside of this definition. This Note argues that this narrow definition of harm and unsound limitation on Congress's powers cements power within the Court to refuse to recognize any harms it does not deem worthy of being in court.[225]

The Court's use of this bootstrapped constitutional test in a privacy case matters. Not only does the test usurp Congressional powers, but it will limit privacy law enforcement and evolution, and continue to confuse lower courts. Privacy harms that are recognized at common law came to a standstill in the mid-twentieth century under Prosser's torts. Much of modern privacy law depends on statutes to fill in the common law gaps that cannot cover modern privacy harms. *TransUnion* disregards the gap filling needs of new privacy statutes, instead holding that Congress cannot legislate injuries into existence.

Because the Court essentially will not recognize new privacy harms in current statutes, and limits Congress's ability to create new statutes for future privacy harms, the *TransUnion* decision has stunted the progress privacy law has made and needs to make in the future. The Court's restrictive definition of harm prevents current enforcement of privacy rights, as bad actors can skirt

219. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).
220. *See Lujan,* 504 U.S. at 560.
221. Fair Credit Reporting Act 15 U.S.C. § 1681 (1970).
222. TransUnion LLC v. Ramirez, 141 S.Ct. 2190, 2215 (2021) (Thomas J., dissenting).
223. *Id.*
224. *Id.*
225. *See generally* Chemerinsky, *supra* note 94.

privacy provisions by resting assured plaintiffs won't be able to meet standing requirements to sue. The Court's limitation on Congress's abilities will keep privacy from evolving right at the time it needs to the most. New and more challenging privacy questions are coming, and U.S. citizens deserve a legal framework to protect themselves and enforce their rights. Finally, the *TransUnion* Court did nothing to aid lower courts in navigating complicated privacy issues, guidance lower courts desperately needed after Spokeo. Instead, privacy litigation, if it occurs at all will continue to be arbitrarily and inconsistently decided. The impacts of the Court's arbitrary limitations will likely be felt for years to come.