ADDING INSULT TO INJURY: HOW ARTICLE III STANDING MINIMIZES PRIVACY HARMS TO VICTIMS AND UNDERMINES LEGISLATIVE AUTHORITY

Kristin Hebert, Nicole Onderdonk, Mark A. Sayre, Deirdre Sullivan

ADDING INSULT TO INJURY: HOW ARTICLE III STANDING MINIMIZES PRIVACY HARMS TO VICTIMS AND UNDERMINES LEGISLATIVE AUTHORITY

Kristin Hebert, Nicole Onderdonk, Mark A. Sayre, Deirdre Sullivan[1]

ABSTRACT

Victims of data breaches and other privacy harms have frequently encountered significant challenges when attempting to pursue relief in the federal courts. Under Article III standing doctrine, plaintiffs must be able to show a concrete and imminent risk of injury. This standard has proved especially challenging to victims of privacy harms, for whom the harm may be more difficult to define or may not yet have occurred (for example, in the case of a data breach where the stolen data has not yet been used). The Supreme Court's recent decision in *TransUnion* appears on its fact to erect an even higher barrier for victims of privacy harms to seek relief. In this article, the authors provide a background on Article III standing doctrine and its applicability to cases involving privacy harms. Next, the recent *TransUnion* decision is discussed in detail, along with an overview of the evidence that *TransUnion* has failed to resolve the ongoing circuit splits in this area. Finally, the authors propose a test from the Second Circuit as a standard that may be able to resolve the ongoing split and support increased access to the courts for the victims of privacy harms.

INTRODUCTION

A secretive company has decided that you are potentially a terrorist. You definitely are not, but the company's rudimentary matching algorithm does not know that. And, although a court had previously characterized the company's rudimentary matching algorithm as both "reprehensible" and a violation of Federal law, the company made no meaningful changes.[2] More problematically, you know that the company shares information about you when you apply for a job, request a loan, purchase insurance, take out a credit card, or rent an apartment; while you have not done any of those recently, you certainly plan to at some point. You fear that being labeled a terrorist might cost you that next big career opportunity or prevent you from buying a new home for your growing family. Can you bring suit for damages in Federal court?

Unfortunately, no.[3] In fact, this scenario is very similar to a 2021 Supreme Court case, *TransUnion LLC v. Ramirez*, in which the Court rejected class certification for thousands of individuals whose consumer reports contained inaccurate potential terrorist flags because the reports had not yet been disclosed to any third parties and thus the individuals failed to show any

[1] All of the authors are J.D. Candidates at the University of Maine School of Law, Class of 2024. The authors would like to thank Professor Scott Bloomberg and the members of the Student Journal of Information Privacy Law team for their thoughtful review and edits.

[2] *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2215 (2021) (Thomas, J., dissenting).

[3] You may, however, bring a suit for equitable relief. *See id.* at 2210-11 (majority opinion).

concrete harm.[4] And while upsetting, in the context of privacy cases, *TransUnion* is unsurprising.[5] Rather, it is yet another example of the Court's tendency to add insult to privacy injuries by minimizing the harm to victims and preventing access to relief.

This paper begins with a history of the standing doctrine and its application within the particular context of privacy harms. Next, we discuss the Court's most recent attempt to provide clarity in *TransUnion, LLC v. Ramirez*, reactions to *TransUnion* by privacy scholars, and the ongoing circuit splits post-*TransUnion*. Finally, we suggest that courts may be able to resolve the issue by adopting a coherent, workable standard from the Second Circuit for data breach cases or, alternatively, expand and bolster the conception, asserted in *TransUnion,* that the risk of future harm can generate a separate, concrete, current harm sufficient for standing.

I. A "CASE OR CONTROVERSY": ARTICLE III STANDING AND ITS APPLICATION TO PRIVACY

Article III of the United States Constitution lays down that federal courts are limited to hearing only "cases" or "controversies."[6] For there to be a case or controversy, a plaintiff must have standing.[7] To establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.[8] If a plaintiff is unable to meet all of the requirements for standing, their case will be dismissed and they will be unable to seek a remedy in the Federal Courts.[9] The Supreme Court has focused on the "injury in fact" requirement for standing since the second half of the 20th century.[10]

A. Injury-in-Fact: *Lujan v. Defenders of Wildlife*

In *Lujan v. Defenders of Wildlife*, the Supreme Court determined that several environmental groups' alleged injuries from the geographically-limited enforcement of environmental regulations protecting endangered species was too speculative and not sufficiently imminent to constitute an injury-in-fact.[11] While recognizing that the interest in continuing to observe endangered species is cognizable for standing purposes,[12] the Court held that this interest was not sufficiently injured when the plaintiffs had no concrete plans to visit the species in question.[13] The Court required that plaintiffs show an "injury in fact," meaning an injury that is

[4] *See id.* at 2211. Counsel for TransUnion quipped at oral argument that the facts of the case should have prompted the plaintiffs to "break out the champagne, not break out a lawsuit." Oyez, Oral Argument in *TransUnion LLC v. Ramirez*, at 04:55 (Mar. 30, 2021), https://www.oyez.org/cases/2020/20-297. It seems more likely, however, that it was TransUnion who broke out the champagne after the Court's decision.

[5] Some scholars have argued that courts appear to require that plaintiffs "move mountains" to establish harms in the privacy context, even where those harms are readily accepted in other legal contexts. *See* Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 363-64 (2014). Other scholars blame privacy scholars for the failure to gain greater recognition for privacy harms, arguing that they suffer from "too much doctrine, and not enough dead bodies." Ann Bartow, *A Feeling of Unease About Privacy Law*, 154 UNIV. OF PA. L. REV. 52, 52 (2006).

[6] U.S. Const. art. III, § 2.

[7] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 800 (2021).

[8] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

[9] *Id.*

[10] *E.g.*, Friends of the Earth v. Laidlaw Env. Servs., 528 U.S. 167, 181 (2000).

[11] Lujan v. Defenders of Wildlife, 504 U.S. 555, 558-60 (1992).

[12] *Id.* at 562-63.

[13] *Id.* at 563-64.

"concrete and particularized" and "actual or imminent, not 'conjectural' or 'hypothetical.'"[14]

After *Lujan*, the "injury-in-fact" requirement, and specifically the requirement that the injury be "concrete and particularized" and "actual or imminent," became an increasingly difficult barrier for cases involving privacy rights and harms.[15]

B. Imminence: *Clapper v. Amnesty International USA*

In *Clapper v. Amnesty International USA*, the Supreme Court assessed whether a group of attorneys and human rights organizations had standing to challenge the constitutionality of the Foreign Intelligence Surveillance Act (FISA), which authorizes surveillance for foreign intelligence purposes.[16] Because the plaintiffs did not have any evidence that the government had actually surveilled their communications under FISA,[17] they presented two alternative theories of injury: (1) that there was an "objectively reasonable likelihood that their communications will be acquired" at some point and thus a substantial risk of future injury; and (2) that the costs incurred to "protect the confidentiality" of their communications constituted "present injury."[18]

The Court's analysis of the plaintiffs' first theory of harm focused on the requirement that an injury-in-fact must be "imminent," meaning that the "'threatened injury must be *certainly* impending.'"[19] After concluding that plaintiffs' fear of future surveillance was based on a "highly attenuated chain of possibilities," the Court concluded that such risk was not certainly impending.[20] The Court also rejected plaintiff's second theory, finding that the assumption of costs due to a fear of surveillance that was not certainly impending was not fairly traceable to the Act being challenged.[21]

The effect of *Clapper* on subsequent privacy cases is unclear.[22] Many courts have referenced *Clapper* when dismissing claims related to the increased risk of future identity theft after a data breach.[23] However, some scholars have vigorously challenged the applicability of *Clapper* to cases of this nature.[24] And, some circuit courts have even argued that *Clapper* reaffirms a finding of standing in such cases.[25]

C. Concreteness: *Spokeo, Inc. v. Robins*

---

[14] *Id.* at 560.
[15] Citron & Solove, *supra* note 7, at 800.
[16] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401, 406 (2013).
[17] *Id.* at 411.
[18] *Id.* at 407.
[19] *Id.* at 409 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).
[20] *Id.* at 410. *But see id.* at 440-41 ("[T]he word 'certainly' in the phrase 'certainly impending' does not refer to absolute certainty. As our case law demonstrates, what the Constitution requires is something more akin to 'reasonable probability' or 'high probability.'") (Breyer, J., dissenting).
[21] *Id.* at 416 (majority opinion).
[22] John L. Jacobus & Benjamin B. Watson, *Clapper v. Amnesty International and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?*, 21 RICH. J.L. & TECH. 3, 81 (2014); Ariel Emmanuel, *Standing in the Aftermath of a Data Breach*, 4 J.L. & CYBER WARFARE 150, 169 (2015).
[23] *See, e.g.*, *Beck v. McDonald*, 848 F.3d 262, 272 (4th Cir. 2017).
[24] *See* Emmanuel, *supra* note 22, at 181-89.
[25] *See, e.g.*, Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 692-96 (7th Cir. 2015). The Seventh Circuit in *Remijas* highlighted the double-edged sword of data breach claims: requiring plaintiffs to wait until the harm of the breach has materialized may increase the imminence of the harm, but the additional passage of time may also make it harder to show that the harm is fairly traceable to the breach. *Id.* at 693.

Only three years later, the issue of standing in privacy cases was back in front of the Court in *Spokeo, Inc. v. Robins*.[26] This time, however, the Court focused on a different injury-in-fact requirement: concreteness.[27] The plaintiff in *Spokeo* brought a class action against an online people search engine, arguing that it violated multiple provisions under the Fair Credit Reporting Act (FCRA).[28] Prior to *Spokeo*, courts often referred to the requirement that the injury be "concrete and particularized," but the *Spokeo* Court clarified that the two parts of this requirement, concreteness and particularization, require two separate inquiries.[29] Because the Ninth Circuit had only analyzed whether the injury was particularized and not whether it was concrete, the Court vacated the decision below and remanded the case back to the Ninth Circuit.[30]

Justice Alito, writing for the Court, specifically declined to determine whether the facts of the case were sufficiently concrete to establish standing,[31] but did provide a detailed discussion of the parameters and motivations of concreteness to guide the Ninth Circuit on remand. Alito indicated that while particularization focuses on whether the harm is specific to the individual plaintiff, concreteness focuses instead on whether the harm is "'real,' and not abstract."[32] Concreteness requires that "the asserted harm [have] a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts."[33] However, scholars have pointed out that the meaning of "traditional harms" is unclear and that the scope of harms recognized by courts is constantly evolving.[34]

Assessing the concreteness of intangible harms requires further analysis.[35] When determining if an intangible harm is concrete, "both history and the judgment of Congress play important roles."[36] And while Congress can, through the enactment of a statutory right, elevate previously inadequate injuries into legally cognizable harms, a violation of that right does not *per se* establish injury-in-fact.[37]

D. Circuit Splits Post-*Spokeo*

Given the jumbled nature of input from the Supreme Court, the circuit courts have varied widely in their application of standing requirements to privacy cases after *Spokeo*.[38] In the case of data breaches, the Second Circuit developed a three factor test in *McMorris v. Carlos Lopez & Associates, LLC*.[39] First, the court considers "whether the data at issue has been compromised as

[26] Spokeo, Inc. v. Robins, 578 U.S. 330 (2016).
[27] *Id.* at 339-43.
[28] *Id.* at 336. The Fair Credit Reporting Act explicitly provides for a private right of action when a company is negligent in failing to comply with any of its requirements. 15 U.S.C. § 1681(a).
[29] *Id.* at 334.
[30] *Id.*
[31] *Id.* at 343.
[32] *Id.* at 340 (quoting Webster's Third New International Dictionary 472 (1971)).
[33] *Id.* at 341.
[34] Citron & Solove, *supra* note 7, at 806.
[35] Spokeo, 578 U.S. at 340. Intangible harms have been recognized by the Court. *Id.* (citing Pleasant Grove City v. Summum, 555 U.S. 460 (2009) (free speech); Church of Lukumi Babalu Aye, Inc. v. Hialeah, 508 U.S. 520 (1993)). Even some intangible privacy harms are concrete. In re Mednax Servs., Inc., Customer Data Sec. Breach Litig., 2022 WL 1468057, at *2 (S.D. Fla. May 10, 2022) ("Concrete intangible harms may include . . . disclosure of private information, and intrusion on seclusion.").
[36] Spokeo, 578 U.S. at 340.
[37] *Id.* at 342.
[38] Citron & Solove, *supra* note 7, at 804-07.
[39] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301 (2d Cir. 2021).

the result of a targeted attack intended to obtain the plaintiff's data."[40] Second, the court requires a showing that at least some part of the compromised data set has been misused.[41] Third, the court looks to "the type of data at issue, and whether that type of data is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed."[42] In contrast, with statutory violations, the Second Circuit assesses whether a statutory provision was intended to protect concrete interests and whether those interests were at risk of harm in the case.[43]

II. *TRANSUNION LLC V. RAMIREZ*

Recognizing these circuit splits, the Supreme Court granted certiorari to hear *Transunion*, where a class of plaintiffs inaccurately labeled by a consumer reporting agency as terrorists sued the agency for violating the FCRA.[44] The FCRA provides a private right of action for noncompliance, including *inter alia* a failure to "follow reasonable procedures to assure maximum possible accuracy" in consumer credit reports.[45] *TransUnion*, one of the "big three" consumer reporting agencies,[46] certainly did not meet the procedural standard required by the statute when it matched consumers solely by name to individuals listed on the "OFAC list."[47] The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) maintains a list of individuals who may pose a threat to national security, including "terrorists, drug traffickers, or other serious criminals."[48] Unsurprisingly, when TransUnion relied exclusively on matching names–without cross-referencing any other personally identifiable data,[49] 8,185 innocent consumers were incorrectly identified as potential terrorists on their credit reports.[50] However, the court determined that only the plaintiffs whose information had been disclosed to third party businesses had suffered a concrete injury.[51] The fact that TransUnion maintained incorrect records in their internal system alone was not enough. Because TransUnion had only shared 1,853 individuals' inaccurate records with third parties, only those individuals met the standing requirement.[52] Therefore, the remaining 6,332 members of the class were foreclosed from bringing suit.[53]

A. Critics Respond to *TransUnion*

Critics challenged the legal reasoning of the Court's decision. Privacy law scholars Daniel J. Solove and Danielle Keats Citron contend that the *TransUnion* decision "is a usurpation of

[40] *Id.*
[41] *Id.*
[42] *Id.* at 302.
[43] Strubel v. Comenity Bank, 842 F.3d 181, 190 (2d Cir. 2016).
[44] Transunion LLC v. Ramirez, 141 S. Ct. 2190 (2021).
[45] *Id*. at 2200 (citing 15 U.S.C. § 1681e(b)).
[46] As a consumer reporting agency, TransUnion creates consumer reports by compiling relevant credit and financial data about individuals. TransUnion "then sells those consumer reports for use by entities such as banks, landlords, and car dealerships that request information about the creditworthiness of individual consumer." *Id* at 2201.
[47] *Id.* at 2218 (Thomas, J., dissenting).
[48] *Id*. at 2201 (majority opinion).
[49] *Id.* at 2200.
[50] *Id*. at 2201.
[51] *Id*. at 2212-13.
[52] *Id.*
[53] *Id*.

legislative power."[54] The authors assert that if Congress has determined that noncompliance with a statute constitutes a private right of action, then to hold otherwise is "akin to rewriting the law."[55] In *Clapper v. Amnesty Int'l USA*, the Court itself recognized that Article III standing is built on separation-of-powers principles.[56] Thus, applying significant additional requirements to plaintiffs in order to satisfy standing represents an interference by the Court in Congressional decision making. This reasoning was mirrored by Justice Kagan in her dissenting opinion in *TransUnion*, where she remarked that the majority decision "transforms standing law from a doctrine of judicial modesty into a tool of judicial aggrandizement."[57]

More importantly, privacy law scholars and experts have expressed concern that limiting the scope of a statutorily granted private right of action reduces protections for victims of privacy harms.[58] Private rights of action aid in holding organizations accountable for violations by complementing often under-resourced and understaffed regulatory agencies.[59] Thus, the Court's failure to recognize a statutorily defined legal injury threatens Congressional efforts to protect against current and emerging privacy harms. The Electronic Frontier Foundation wrote that the Court's decision "reflects a naïve view of the increasingly powerful role that personal data, and the private corporations that harvest and monetize it, play in everyday life."[60]

B. Leaving the Door Open for Emotional Harms Caused by Future Risk

While the Court did not mince words when it declared that the risk of future harm alone would not constitute a sufficient injury under the standing analysis, it nevertheless seemed to leave the door open for cases in which "the exposure to the risk of future harm itself causes a separate concrete harm."[61] Tucked away in a footnote, the Court writes that "a plaintiff 's knowledge that he or she is exposed to a risk of future physical, monetary, or reputational harm could cause its own current emotional or psychological harm," but stops short of affirmatively proclaiming that "such an emotional or psychological harm could suffice for [standing] purposes."[62] This potential exception is particularly relevant for data breach cases, in which victims of a breach may experience emotional or financial distress due to the threat of identity theft looming over them as their sensitive personal information remains in a purgatory-like state floating around the internet indefinitely.

C. Circuit Splits Post-*Transunion*: More Confusion than Clarity

As noted above,[63] the Supreme Court's decision in *TransUnion* appeared to significantly

---

[54] Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion LLC v. Ramirez, 101 B.U. L. REV. Online 62 (2021).
[55] *Id*. at 47.
[56] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).
[57] Transunion LLC v. Ramirez, 141 S. Ct. 2190, 2225 (2021) (Kagan, J., dissenting).
[58] *See e.g., Supreme Court Limits Standing to Sue in Credit Reporting Case*, ELECTRONIC PRIVACY INFORMATION CENTER (June 25, 2021), https://epic.org/supreme-court-limits-standing-to-sue-in-credit-reporting-case/.
[59] Solove & Citron, *supra* note 54.
[60] *Supreme Court Says You Can't Sue the Corporation that Wrongly Marked You A Terrorist*, ELECTRONIC FRONTIER FOUNDATION (June 28, 2021), https://www.eff.org/deeplinks/2021/06/supreme-court-says-you-cant-sue-corporation-wrongly-marked-you-terrorist.
[61] TransUnion, 141 S. Ct. at 2211. (majority opinion).
[62] *Id*. at 2211 n.7.
[63] *See supra* Section II.A.

restrict, if not foreclose, standing based on the risk of future harm, a particularly damaging result for victims of privacy harms.[64] However, lower court decisions since *TransUnion* reflect more confusion than clarity.[65] Similar to the aftermath of both *Clapper*[66] and *Spokeo*,[67] the application of *TransUnion* by lower courts has greatly varied, echoing the circuit splits that existed before the decision.[68] Some courts dismissed cases for lack of standing[69] while other courts found standing,[70] while both citing *TransUnion*. Additionally, some courts reached their decisions by distinguishing from *TransUnion*,[71] while others did not mention it at all.[72] Within this chaotic landscape of decisions, two potentially informative lines of cases can be observed: cases applying pre-*TransUnion* standards and cases leveraging *TransUnion's* borderline-dicta assertion that risk of future harm may be the source of a separate, concrete, current harm sufficient for standing.

In the line of cases using pre-*TransUnion* standards to evaluate standing, the most dominant standard referenced is the Second Circuit's *McMorris* factors test. To assess whether risk of future harm is concrete enough to satisfy the injury-in-fact requirement of standing, courts consider (1) whether the data has been compromised due to a targeted attack; (2) whether there has been some showing of misuse; and (3) whether the type of data is susceptible to misuse once exposed.[73] Despite *McMorris*'s uncertain fate post-*TransUnion*, courts in the Second Circuit have continued to apply it. For example, in *Cooper v. Bonobos*, the court declined to apply *TransUnion*, instead applying the *McMorris* factors.[74] The court explicitly left it to the Second Circuit to decide if *McMorris* was overturned by *TransUnion* and did not comment further on it.[75] Ultimately, the court dismissed for a lack of standing because the case failed on the third *McMorris* factor–the type of data exposed was not susceptible to misuse.[76] Moreover, *McMorris* has been favorably cited, and used to inform standing analyses, by multiple other circuits post-*TransUnion*,[77] supporting the contention that this test remains a viable framework for evaluating standing in cases

---

[64] James Dempsey, *US Courts Mixed On Letting Data Breach Suits Go Forward*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Mar. 9, 2022), https://iapp.org/news/a/u-s-courts-mixed-on-letting-data-breach-suits-go-forward/.

[65] *Id.*

[66] *See supra* Section I.B.

[67] *See supra* Section I.C-D.

[68] James Dempsey, *Chapter 4A: Standing After TransUnion*, CYBERSECURITY LAW FUNDAMENTALS (Nov. 9, 2022), https://cybersecuritylawfundamentals.com/chapter-4a.

[69] *See, e.g.*, C.C. v. Med-Data Inc., No. 21-2301-DDC-GEB, 2022 WL 970862 (D. Kan. Mar. 31, 2022); Cooper v. Bonobos, Inc., No. 21-CV-854 (JMF), 2022 WL 170622 (S.D.N.Y. Jan. 19, 2022).

[70] *See, e.g.*, Clemens v. ExecuPharm Inc., 48 F.4th 146 (3d Cir. 2022); Bohnak v. Marsh & McLennan Cos., Inc., 580 F. Supp. 3d 21 (S.D.N.Y. Jan. 17, 2022); *In re* Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig., No. CV 19-MD-2904, 2021 WL 5937742 (D.N.J. Dec. 16, 2021).

[71] *See, e.g.*, Cotter v. Checkers Drive-In Restaurants, Inc., No. 8:19-CV-1386-VMC-CPT, 2021 WL 3773414 (M.D. Fla. Aug. 25, 2021); *In re* Blackbaud, Inc., Customer Data Breach Litig., No. 3:20-MN-02972-JMC, 2021 WL 2718439 (D.S.C. July 1, 2021).

[72] *See, e.g.*, Burns v. Mammoth Media, Inc., No. CV2004855DDPSKX, 2021 WL 3500964 (C.D. Cal. Aug. 6, 2021).

[73] McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301 (2d Cir. 2021).

[74] Cooper, 2022 WL 170622, at *3.

[75] *Id.* at *3 n.1.

[76] *Id.* at *3.

[77] *See, e.g.*, Clemens v. ExecuPharm Inc., 48 F.4th 146, 153-54 (3d Cir. 2022); C.C. v. Med-Data Inc., No. 21-2301-DDC-GEB, 2022 WL 970862, at *4 (D. Kan. Mar. 31, 2022) (citing McMorris to highlight that no circuit has fully foreclosed standing for an injury based on future harm); Cotter v. Checkers Drive-In Restaurants, Inc., No. 8:19-CV-1386-VMC-CPT, 2021 WL 3773414, at *5 (M.D. Fla. Aug. 25, 2021) (citing McMorris to support the holding of an Eleventh Circuit case).

where the injury is a risk of a future harm.

In the line of cases citing *TransUnion*'s assertion, relegated to footnote, that risk of future harm may be the source of a separate, concrete, current harm sufficient for standing,[78] lower courts leveraged this "open door" as a potential avenue to find standing, an avenue that some critics feared would be completely foreclosed by the central holding of *TransUnion* itself. The Court's acknowledgement that knowledge of one's exposure to a risk of future harm "could cause…current emotional or psychological harm"[79] is what many lower courts seemed to take away from *TransUnion.* In *In re Am. Medical Collection Agency, Inc. Customer Data Security Breach Litigation*, the court found standing, explicitly citing *TransUnion,* holding that the compromise of data alone is a concrete harm in and of itself.[80] In *Clemens v. ExecPharm, Inc.*, citing *TransUnion*, the Third Circuit affirmed that, in data breach scenarios, an injury can satisfy concreteness even if intangible (as long as it has a relationship to a harm traditionally recognized); "where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff…can satisfy concreteness as long as [they] allege[] that the exposure to that substantial risk caused additional, currently felt concrete harms," such as emotional distress or money spent on fraud mitigation measures.[81]

While these initial cases provide an indication of the impacts of *TransUnion*, they leave a significant amount of uncertainty.[82] In some cases, there appears to be different interpretations of *TransUnion* within a single district.[83] Therefore, the additional impacts will not reveal themselves until these cases and others progress through the later stages of trial[84] and the appeals process.[85]

III.CIRCUIT COURT CHAOS YIELDS POTENTIAL SOLUTIONS

From *Clapper* to *TransUnion*, the Supreme Court has weighed in on the application of injury to privacy three times in less than a decade, and yet lower courts continue to reach different conclusions when applying standing to nearly identical cases involving privacy. Should the Court resign itself to the "hopeless indeterminacy"[86] of standing in privacy cases? The 212 million U.S.

---

[78] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2211. (majority opinion).

[79] *Id*. at 2211 n.7.

[80] In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig., No. CV 19-MD-2904, 2021 WL 5937742, at *7 (D.N.J. Dec. 16, 2021).

[81] *Clemens*, 48 F.4th at 154-156. For other examples of cases applying footnote 7 of *TransUnion*, *see e.g.*, Rand v. The Travelers Indemnity Co., no. 7:21-cv-10744, at *4 (S.D.N.Y. Oct. 26, 2022); Bohnak v. Marsh & McLennan Cos., Inc., 580 F. Supp. 3d 21, 29 (S.D.N.Y. 2022).

[82] The majority of privacy harm cases where standing is at issue decided since *TransUnion* are data breach cases; non-data breach cases may reveal different applications and impacts of *TransUnion* than are noted in this paper. *See e.g.*, Mastel v. Miniclip SA, 2021 U.S. Dist. LEXIS 132401 (E.D. Cal. July 15, 2021) (finding standing based on analogy to traditionally recognized harm).

[83] *Compare Bohnak*, 580 F. Supp. (applying *TransUnion* and finding standing), *with* Cooper v. Bonobos, Inc., No. 21-CV-854 (JMF), 2022 WL 170622 (S.D.N.Y. Jan. 19, 2022) (applying *McMorris* and finding no standing).

[84] *See, e.g., In re* Blackbaud, Inc., Customer Data Breach Litig., No. 3:20-MN-02972-JMC, 2021 WL 2718439, at *2 n.15 (D.S.C. July 1, 2021) (indicating that the plaintiff's allegations of concrete injury in the pleadings are sufficient to establish standing at this stage); Cotter v. Checkers Drive-In Restaurants, Inc., No. 8:19-CV-1386-VMC-CPT, 2021 WL 3773414, at *4 (M.D. Fla. Aug. 25, 2021) (deferring interpretation of *TransUnion* to the circuit court).

[85] *See e.g.*, *Cooper*, 2022 WL 170622, at *3 n.1 (S.D.N.Y. Jan. 19, 2022) (deferring to Second Circuit to decide on TransUnion implications); *Cotter*, 2021 WL 3773414, at *4 (M.D. Fla. Aug. 25, 2021).

[86] Johnson v. United States, 576 U.S. 591, 598 ("[T]his Court's repeated attempts and repeated failures to craft a principled and objective standard out of the residual clause confirm its hopeless indeterminacy.") (referring to the interpretation of a single clause within the Armed Career Criminal Act).

victims of data breaches in 2021 alone,[87] not to mention the countless other victims of other similarly challenged privacy injuries, certainly hope not. Surely the Constitution grants the Court the ability to adjudicate a harm affecting more than 60% of the country's population.[88] On this front, we are persuaded by Professors Citron and Solove's critique; the *TransUnion* Court simply got it wrong.[89]

Where Congress has defined a right in statute and provided for enforcement of such right via a private right of action, the answer should be simple: the violation of such right establishes injury-in-fact for standing purposes. Such an approach properly reflects that the Constitutional standing requirement is built on separation-of-powers principles.[90]

However, even where the Court is unable to find standing in the violation of a statutory right, there is evidence of two other avenues. The first is a clear and workable standard for defining a privacy injury that already exists: the Second Circuit's *McMorris* factors. These factors continue to be employed to evaluate standing post-*TransUnion*, both within[91] and beyond[92] the Second Circuit. Even without being adopted *yet* by the Supreme Court, the use of the test (and *McMorris* holdings in general[93]) beyond the circuit where it originated is evidence that this formulation of factors could have broad appeal, which would decrease the risk that the current circuit splits persist.

Second, and perhaps most compellingly, even without looking beyond *TransUnion*, there is an interpretation that some circuits have already adopted that provides a pathway to standing: that exposure to future risk of privacy harm may create a separate, concrete, current harm. As some courts have already done, *TransUnion's* footnoted assertion that emotional distress caused by the knowledge that your data has been exposed and may be misused in the future is an opportunity to "make lemonade out of lemons"—that is, find standing, even in spite of *TransUnion's* seemingly prohibitive holding. Through continued lower court interpretations, *TransUnion* may be used to expand and bolster, rather than minimize, the concreteness of privacy harms.

CONCLUSION

The evolution in standing jurisprudence over the past decade, from *Clapper* to *TransUnion*, has made it increasingly difficult for victims of privacy harms to pursue relief in Federal Courts. The Court's incremental erection of ever higher barriers for privacy victims stands in sharp contrast

---

[87] Jason Cohen, *United States Has the Most Data Breach Victims in the World*, P.C. MAG. (Dec. 10, 2021), https://www.pcmag.com/news/united-states-has-the-most-data-breach-victims-in-the-world.

[88] The Census Bureau projected that the population of the U.S. was 332 million on Jan. 1, 2022. Census Bureau, *Census Bureau Projects U.S. and World Populations on New Year's Day* (Dec. 30, 2021), https://www.census.gov/newsroom/press-releases/2021/news-years-day-2022.html#:~:text=DEC.,Day%20(April%201)%202020. Not accounting for timing differences between the data breaches and the Census Bureau's measurements, 212 million divided by 332 million is 63.9%.

[89] Citron & Solove, *supra* note 54, at 62.

[90] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013). Alternatively, the Court could consider whether the statute establishes injury-in-fact on a statute-by-statute basis, using a test such as the one adopted by the Second Circuit. *See* discussion *supra* Section I.D. The Second Circuit test has also been adopted by the Ninth Circuit. Citron & Solove, *supra* note 7, at 804-05. Reflecting the principle of separation of powers, the Court should be deferential to Congress when applying such a test. *See* Robins v. Spokeo, Inc., 867 F.3d 1108, 1115 (9th Cir. 2017) (citing Van Patten v. Vertical Fitness Grp., 847 F.3d 1037 (9th Cir. 2017)).

[91] *See, e.g.*, Aponte v. Northeast Radiology, P.C., 21 CV 5883 (VB) (S.D.N.Y. May 16, 2022); In re GE/CBPS Data Breach Litigation No. 1:20-cv-02903-KPF, 2021 WL 3406374 (S.D.N.Y., Aug. 4, 2021).

[92] *See, e.g.*, cases cited *supra* note 77.

[93] *See, e.g.*, Clemens v. ExecuPharm Inc., 48 F.4th 146, 153-54 (3d Cir. 2022) (citing the *McMorris* factors to support the imminence prong of its three-part injury-in-fact test).

to society's growing awareness of the risks to privacy posed by the rapid growth in data collection and increasing sophistication of cyber attackers. This disconnect between the Court's perspective and reality may explain why its decisions have failed to resolve ongoing circuit splits in this area. We believe that the test adopted by the Second Circuit provides a coherent, stable framework for analyzing the injury to victims of privacy harms, particularly in data breach cases. Such a test, given evidence of its current application, could achieve broader adoption across circuits and provide victims and companies with greater clarity. Alternatively, *TransUnion*'s assertion that the risk of future harm may constitute a separate and concrete current harm, if further expanded and bolstered by courts, can provide an even more meaningful avenue for plaintiffs to rely on for standing.