Unjust Enrichment: Standing Up For Privacy Rights

Bernard Chao[*]

ABSTRACT: In TransUnion LLC v. Ramirez*, one of the country's largest credit reporting agencies violated the Fair Credit Reporting Act ("FCRA") by "fail[ing] to follow reasonable procedures to assure maximum possible accuracy . . . ." As a result, thousands of credit reports incorrectly said that consumers were "potential terrorists, drug traffickers, or serious criminals." The case wound its way to the Supreme Court on the issue of Article III standing. For plaintiffs that had their reports disseminated, the Court found standing. For victims that did not have their reports disseminated, the Supreme Court concluded that they had not suffered a "concrete injury." Accordingly, these victims did not have standing and could not recover the statutory damages provided by the FCRA.*

TransUnion *has the potential to impact several types of modern data privacy rights. While the European Union ("EU") has led the way in recognizing several new rights, this country has followed, and federal and state laws are beginning to adopt their own versions of these rights. Specifically, privacy statutes are now giving individuals the right to: (1) not have their personal data collected; (2) access their data; (3) rectify inaccurate data; and (4) have their data deleted. But after* TransUnion*, the Supreme Court may have eliminated the ability of Congress to use statutory damages to enforce such rights. This Essay suggests an approach that will restore this option to Congress.*

Earlier work (by myself and others) has already explained why unjust enrichment can help overcome issues of harm, causation and standing in privacy law. This Essay builds on that work by addressing TransUnion *and arguing that restitution and unjust enrichment can provide standing to plaintiffs that sue under emerging privacy statutes. Because unjust enrichment is based on the defendant's gain instead of the plaintiff's injury, plaintiffs can surmount standing's "concrete injury" requirement. Moreover, plaintiffs have pursued various unjust enrichment claims in courts for*

* Bernard Chao is a Professor at the University of Denver Sturm College of Law. I would like to thank Matthew Kugler Tiffany Li, Viva Moffat, Christopher Mortenson, Christopher Robertson, Jay Stanley, Zahra Takhshid, Felix Wu and the participants of the 2022 Privacy Law Scholars Conference and 2021 SMU Dedman School of Law Faculty Forum for their helpful comments.

centuries. Therefore, it is precisely the kind of historically rooted theory endorsed by TransUnion. *Finally, both Congress and state legislatures should consider expressly including a disgorgement remedy in their privacy statutes to allow victims to recover the money companies wrongly receive (or wrongfully save) for violating these laws. Such carefully drafted laws will prevent courts from limiting the availability of the unjust enrichment remedy.*

INTRODUCTION

In *TransUnion LLC v. Ramirez*,[1] a class of aggrieved individuals sued TransUnion for improperly classifying them "as potential terrorists, drug traffickers, or serious criminals" on TransUnions' credit reports.[2] Along the way, TransUnion committed several violations of the Fair Credit Reporting Act ("FCRA").[3] Most importantly, it failed to "follow reasonable procedures to assure maximum possible accuracy."[4] The case wound its way to the Supreme Court on the issue of Article III standing. For 1,853 people that had their reports disseminated, the Court found standing.[5] But for another 6,332 people that did not have their reports disseminated, the Supreme Court said that these people had "not suffer[ed] a concrete harm."[6] Therefore, they did not have standing and could not recover the statutory damages authorized by the FCRA.

Critics have been quick to decry the *TransUnion* decision. Erwin Chemerinsky says that *TransUnion* "changes the law" and "places in doubt the

1. TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021).
2. *Id.* at 2201–02, 2209.
3. *Id.* at 2214 (Thomas, J., dissenting).
4. *Id.* at 2200 (quoting 15 U.S.C. § 1681e(b) (2020)).
5. *Id.* at 2209.
6. *Id.* at 2211–12.

ability to sue to enforce countless federal laws."[7] This Essay focuses on one important context: emerging privacy rights. Daniel Solove and Danielle Citron explain that the case "arguably strikes a major blow to the enforcement of privacy laws in the federal courts."[8] Peter Ormerod said that "the [Supreme] Court's restrictive interpretation of Article III suggests that abusive informational practices are incapable of individual enforcement."[9] Perhaps not coincidentally, *TransUnion* was decided just as modern privacy statutes are beginning to recognize several new data types of privacy rights that target risk privacy practices. In fact, Congress just introduced a draft of the American Data Privacy and Protection Act ("ADPPA") this summer.[10] While the details of the ADDPA are still being worked out, new privacy statutes often include the right for individuals to: (1) not have their personal data collected; (2) access their own data; (3) rectify inaccurate data; and (4) have their data deleted. After *TransUnion*, it appears unlikely that individuals will have standing to recover statutory damages for violations of these and other emerging statutory rights unless there are also specific kinds of downstream harms.

But there may be a way to surmount the Supreme Court's standing hurdle. Prior work—including the author's—has explained why unjust enrichment can supply standing in privacy cases.[11] This Essay builds on that work and argues that the theory of restitution and unjust enrichment can provide standing to plaintiffs that sue under these emerging privacy statutes. Because unjust enrichment is based on the defendant's gain rather than the plaintiff's injury, plaintiffs can sidestep standing's "concrete injury" requirement. Moreover, plaintiffs have pursued various unjust enrichment claims in courts for centuries. Therefore, it is precisely the kind of historically rooted theory that the Supreme Court has endorsed in its standing cases.

To reinforce this argument, both Congress and state legislatures should add the unjust enrichment remedy to their private causes of action. This remedy would force companies to pay aggrieved victims by disgorging money the companies wrongly received—or wrongfully saved—for violating privacy laws. Additionally, standard statutory damage provisions should be revised

---

7. Erwin Chemerinsky, *What's Standing After* TransUnion LLC v. Ramirez, 96 N.Y.U. L. REV. ONLINE 269, 270 (2021).

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

9. Peter Ormerod, *Making Privacy Injuries Concrete*, 79 WASH. & LEE L. REV. 101, 107 (2022).

10. American Data Privacy and Protection Act, H.R. 8152, 117th Congress (2022); Müge Fazlioglu, *Distilling the Essence of the American Data Privacy and Protection Act Discussion Draft*, IAPP (June 3, 2022), https://iapp.org/news/a/distilling-the-essence-of-the-american-data-privacy-and-protection-act-discussion-draft [https://perma.cc/GVQ4-UEHS].

11. Bernard Chao, *Privacy Losses as Wrongful Gains*, 106 IOWA L. REV. 555, 557 (2021); *see also* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 658 (2019); Brief of Restitution and Remedies Scholars as Amici Curiae in Support of Respondent at 4–7, 18–19, Spokeo, Inc. v. Robins, 578 U.S. 330 (2016) (No. 13-1339), 2015 WL 5302537, at *4–7, 18–19 [hereinafter Restitution and Remedies Scholars' Brief].

and couched in language that permits statutory damages when the unjust enrichment is difficult to calculate. In such cases, statutory damages will be based on an underlying unjust enrichment injury. Presumably, this should overcome the standing obstacle and allow legislatures to reclaim their role in shaping data privacy policy with private causes of action.

I. *TRANSUNION LLC V. RAMIREZ*

TransUnion is one of the three largest credit reporting agencies in the United States.[12] It "compiles personal and financial information . . . to create consumer reports."[13] These reports are sold to various entities including banks, car dealers, landlords, and employers as they investigate applications for loans, housing, and jobs among other purposes.[14] "Beginning in 2002, TransUnion introduced an add-on product called [the] OFAC Name Screen Alert" ("Name Screen").[15] This product was based on the so-called "OFAC list," which is "maintained by the U.S. Treasury Department's Office of Foreign Assets Control."[16] Individuals on the OFAC list include "terrorists, drug traffickers, and other serious criminals" who are determined to threaten national security.[17]

When companies requested Name Screen, TransUnion would check whether the individual's name appeared on the OFAC list.[18] If it did, "TransUnion would place an alert on the credit report indicating that the consumer's name was a 'potential match.'"[19] TransUnion did nothing to determine whether the individuals were the same people as those named on the OFAC list.[20] Not surprisingly, many people share the same names as the individuals on the OFAC list, and TransUnion wrongly placed an alert on 8,185 individuals' credit reports in TransUnion's files.[21]

The FCRA contains numerous safeguards to ensure that consumer reporting agencies do not make the kinds of mistakes TransUnion did. In *TransUnion*, the plaintiffs alleged that TransUnion committed three violations: (1) failing to "'follow reasonable procedures to assure maximum possible accuracy' in consumer reports;" (2) failing to provide copies of the

12. *See Nation's Big Three Consumer Reporting Agencies Agree To Pay $2.5 Million To Settle FTC Charges of Violating Fair Credit Reporting Act*, FED. TRADE COMM'N (Jan. 13 2000), https://www.ftc.gov/news-events/news/press-releases/2000/01/nations-big-three-consumer-reporting-agencies-agree-pay-25-million-settle-ftc-charges-violating-fair [https://perma.cc/KWZ5-UHWD].

13. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2201 (2021); *see also Understanding Your Credit*, FED. TRADE COMM'N (Dec. 2021), https://consumer.ftc.gov/articles/understanding-your-credit [https://perma.cc/4Q3T-D9TN].

14. *See Understanding Your Credit, supra* note 13.

15. *TransUnion*, 141 S. Ct. at 2201.

16. *Id.* at 2197.

17. *Id.* at 2201.

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.* at 2202.

consumers' reports; and (3) failing to provide a written summary of the consumers' rights.[22] Aggrieved consumers can recover actual damages, attorney's fees, and costs.[23] Moreover, if the violations are willful, individuals may recover statutory damages—ranging from $100 to $1,000—and punitive damages.[24] At trial, the *TransUnion* jury returned a verdict for the plaintiffs and "awarded each class member $948.22 in statutory damages and $6,353.08 in punitive damages for a total award of $60 million."[25] TransUnion appealed, and the case eventually made its way to the Supreme Court on the single issue of whether the plaintiffs had Article III standing.[26]

Standing jurisprudence is rooted in the Case or Controversy Clause of the U.S. Constitution.[27] Accordingly, the jurisdiction of Article III courts is limited to deciding "cases" or "controversies."[28] In concrete terms, federal courts may not issue advisory opinions. As Justice Gorsuch put it, federal courts may only resolve "a real controversy with real impact on real persons."[29] Under modern standing jurisprudence, a three-part test for standing has emerged. To establish standing, a plaintiff must show: (1) that he or she "suffered an injury in fact" that is "concrete and particularized, [and] actual or imminent;" (2) that the injury was likely caused by the defendant; and (3) that the injury would likely be redressed by judicial relief.[30] Importantly, standing is decided separately for each claim plaintiffs bring and each form of relief they seek.[31] The question presented in *TransUnion* focused on the first prong of the standing test: whether the plaintiffs' injuries were sufficiently "'concrete' – that is, 'real, and not abstract.'"[32]

The Supreme Court first considered the "claim that TransUnion failed to 'follow reasonable procedures to assure maximum possible accuracy'" as required by 15 U.S.C. § 1681e(b).[33] The analysis divided the plaintiffs into two groups: 1,853 people whose reports had been disseminated to various businesses; and 6,332 people whose inaccurate reports had not been disseminated.[34] To determine whether the first set of plaintiffs had suffered concrete injuries, the Supreme Court looked to whether the injuries bore "a

22. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2202, 2207 (2021); *see* 15 U.S.C. § 1681e(b); *Id.* § 1681(a)(1); *Id.* § 1681g(c)(2).

23. 15 U.S.C. § 16810.

24. *Id.* § 1681n.

25. *TransUnion*, 141 S. Ct. at 2202.

26. *Id.* at 2203.

27. *Id.*

28. U.S. CONST. art. III, § 2, cl. 1.

29. Am. Legion v. Am. Humanist Ass'n, 139 S. Ct. 2067, 2103 (2019) (Gorsuch, J., concurring).

30. Lujan v. Defs. of Wildlife, 504 U.S. 555, 555, 560–561 (1992).

31. *TransUnion*, 141 S. Ct. at 2208 (citing Davis v. Fed. Election Comm'n, 554 U.S. 724, 734 (2008)).

32. *Id.* at 2204 (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016)).

33. *Id.* at 2208; 15 U.S.C. § 1681e(b).

34. *Id.* at 2200.

close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts."[35] The Court found that "[t]he harm from being labeled a 'potential terrorist' . . . bears a sufficiently close relationship to the harm from a false and defamatory statement," a traditional common law privacy tort.[36] As a result, the Supreme Court held that the 1,853 people had suffered a concrete injury and, therefore, had standing.[37]

The Supreme Court looked at the 6,332 people whose inaccurate reports had not been disseminated differently.[38] It noted that "[p]ublication is 'essential'" to the common law defamation tort.[39] Moreover, there were no other common law analogs. As a result, the Court concluded that, "The mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm."[40]

The plaintiffs argued that their risk of future injury was concrete.[41] But the Supreme Court rejected this argument on several different grounds. First, the Court said that there was no injury until the harm materialized.[42] Perhaps conceding that a high probability of future harm might be sufficiently concrete, the Court went on to say that the 6,332 "plaintiffs did not demonstrate a sufficient likelihood that their" reports would be sent to requesting businesses.[43] Finally, the Court concluded that, "It is difficult to see how a risk of future harm could supply the basis for a plaintiff's standing" when most plaintiffs "did not even know . . . that there were OFAC alerts in their internal TransUnion credit files."[44] In sum, the Supreme Court found that 6,332 class members did not have standing to claim that TransUnion violated the FCRA by failing to follow reasonable procedures to ensure data accuracy because their credit files were not disseminated.[45]

The Supreme Court then turned to the two claims alleging that TransUnion had failed to properly provide access to Ramirez's credit file.[46] When Ramirez "requested a copy of his credit file[,] TransUnion sent Ramirez [a copy and a] summary of his rights," but it failed "to mention the OFAC alert."[47] "The following day, TransUnion sent Ramirez a second mailing . . . [indicating] that his name was a . . . match to names on the OFAC

35. *Id.* at 2213 (citing *Spokeo*, 578 U.S. at 341).
36. *Id.* at 2209.
37. *Id.*
38. *See id.*
39. *Id.*
40. *Id.* at 2210.
41. *Id.*
42. *Id.* at 2211.
43. *Id.* at 2212; *see also* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 431 (2013) (Breyer, J., dissenting) ("But, as the majority appears to concede . . . *certainty* is not, and never has been, the touchstone of standing." (emphasis added)).
44. *TransUnion*, 141 S. Ct. at 2212.
45. *Id.* at 2212.
46. *See id.* at 2213.
47. *Id.* at 2201, 2213.

list . . . [but] [t]he second mailing did not include a[] . . . summary of rights."[48] Based on these facts, the plaintiffs alleged that the first mailing violated the FCRA because it failed to provide plaintiffs with a complete copy of their report (the disclosure claim) as required by 15 U.S.C. § 1681g(a)(1).[49] Moreover, the second mailing failed to provide plaintiffs with a summary of their rights (the summary-of-rights claim) as required by 15 U.S.C. § 1681g(c)(2).[50] In short, each mailing was arguably deficient, but the combination of the two mailings provided the information required by the FCRA.

The Supreme Court found that the plaintiffs lacked standing to bring these two claims. The Court first explained that "the plaintiffs have not demonstrated that the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts."[51] Moreover, the Court pointed out that the plaintiffs had presented no evidence that anyone other than Ramirez had opened the mailing or "were confused, distressed, or relied on the information in any way."[52] Thus, while the earlier analysis in *TransUnion* focused on the lack of dissemination to deny standing, this analysis used lack of causation as another basis to deny standing.

Relying on dissemination and causation reveals a fundamental difference in the way that Congress and the Supreme Court think about privacy. The FCRA seeks to deter conduct that increases the chances of subsequent privacy injuries by: (1) insisting that companies take precautions to ensure data accuracy; and (2) giving individuals a right to access their data.[53] But the Supreme Court does not recognize risky conduct as creating a "concrete injury" justifying standing. It looks for downstream injuries further along the causal chain. This is true even when the conduct violates a statute that provides a private cause of action with statutory damages. But the FCRA is not the only privacy statute that seeks to nip problems in the bud. Many of the emerging privacy rights also operate on privacy risks as opposed to the ultimate injury.

As a result, the Supreme Court has limited the ability for Congress (and—to a lesser extent—state legislatures) to enact privacy laws with private causes of action.[54] Ironically, the Supreme Court has often justified standing doctrine as a way for the courts to defer to the legislature.[55] Presumably, when

48. *Id.* at 2201–02, 2213.

49. *Id.* at 2213; *see* 15 U.S.C. § 1681g(a)(1).

50. *TransUnion*, 141 S. Ct. at 2213; *see* 15 U.S.C. § 1681g(c)(2).

51. *TransUnion*, 141 S. Ct. at 2213 (citing Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016)).

52. *Id.* (quoting Ramirez v. TransUnion, 951 F.3d 1008, 1039 (2020) (McKeown, J., concurring in part and dissenting in part), *overruled by* TransUnion LLC, 141 S. Ct. 2190 (2021)).

53. 15 U.S.C. §§ 1681, 1681g.

54. *TransUnion*, 141 S. Ct. at 2221 (Thomas, J., dissenting) ("[T]his Court has relieved the legislature of its power to create and define rights.").

55. F. Andrew Hessick, *The Separation-of-Powers Theory of Standing*, 95 N.C. L. REV. 673, 685 (2017) (noting that one justification the Supreme Court has given is that the "standing doctrine

courts fail to take a plaintiff's case for lack of standing, that leaves more room for Congress to make the important policy decision. But after *TransUnion*—and *Spokeo*[56] before it—the doctrine has grown to the point where standing is limiting the policy choices Congress can make. This is true even though there may be entirely legitimate reasons for Congress to choose to punish risky conduct (i.e., conduct that creates the *risk* of privacy injuries) vs. injurious conduct (i.e., conduct that has been shown to *actually cause* privacy injuries). In its current form, standing doctrine limits the ability of Congress to target risky conduct with private causes of action.

At the same time, modern privacy law is moving in the opposite direction. As shown in Part II below, emerging privacy laws often target practices that increase the risk of later privacy injuries.[57] Thus, the Supreme Court's standing jurisprudence creates a problem for these new privacy statutes.

My critique of *TransUnion* is not unique. Many other commentators have already denounced *TransUnion*. Daniel Solove and Danielle Citron come straight out and say that the Supreme Court is "wrong in how it conceives of privacy harms" and that the case "essentially nullified a key enforcement component of many privacy laws—private rights of action."[58] Moreover, numerous commentators have complained that the Supreme Court's standing jurisprudence allows courts to usurp the legislature's role.[59]

Yet another problem is that the Supreme Court's guidance is muddled, making it difficult to determine what informational injuries have standing.[60] To address this problem, Peter Ormerod has suggested that the law should rely on Helen Nissenbaum's contextual integrity framework to determine informational norms.[61] The courts would then use these norms to determine what injuries have standing.[62] Ignacio Cofone takes a different tact and offers a three-step framework that involves: (1) identifying if there is a privacy loss; (2) looking to see whether such losses produce privacy harms; and

---

ensures that the federal judiciary does not decide matters more appropriately addressed to the other branches of government"); Heather Elliott, *The Functions of Standing*, 61 STAN. L. REV. 459, 462 (2008) ("[T]he Court has said, standing doctrine allows the courts to refuse cases better suited to the political process . . . .").

56. *See Spokeo*, 578 U.S. at 341 ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.").

57. *See infra* Part II.

58. Solove & Citron, *supra* note 8, at 68, 62.

59. *Id.* at 69–70; Chemerinsky, *supra* note 7, at 290 ("Congress should be able to create rights whose infringement is an injury sufficient to confer standing."); Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 458 (2017); Ormerod, *supra* note 9, at 131–36.

60. Ormerod, *supra* note 9, at 128 (arguing that the Supreme Court has "fail[ed] to supply a principle for discerning when an informational injury is concrete, particularized, and actual or imminent"); Ignacio Cofone, *Privacy Standing*, 2022 U. ILL. L. REV. 1367, 1370 ("[J]udges struggle with how to constitute a privacy injury.")

61. Ormerod, *supra* note 9, at 107–08; *see* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 127 (2009).

62. Ormerod, *supra* note 9, at 146–182.

(3) identifying "whether the privacy harm is actionable" by looking at whether it fits into a common law tort or statutory breach.[63]

While I am sympathetic to Ormerod's and Cofone's efforts, they work within the Supreme Court's current injury-based framework. Therefore, their proposals can only work at the margins. If adopted, these theories may lead to more predictable outcomes. Ormerod and Cofone's proposals may result in giving standing to a few more privacy plaintiffs, but most victims will still be unable to have their day in court.[64] The basic problem is that *Spokeo* and *TransUnion* have a very narrow view of "concrete harm." Moreover, attempts to expand the meaning of that term (e.g., Citron's and Solove's proposals) fly directly into the teeth of these decisions and are unlikely to succeed.

This Essay describes an alternative path to standing. Building on prior work of both mine and others, I argue that the doctrine of unjust enrichment and restitution can provide standing to privacy plaintiffs seeking statutory damages.[65] Part II describes several emerging privacy rights and how these rights are designed to decrease the risk of privacy injuries. It also explains how the Supreme Court's standing jurisprudence has limited the ability of such laws to use a private right of action to enforce such rights. Part III then proceeds to describe the theory of restitution and unjust enrichment. It briefly describes how well rooted the doctrine is in U.S. history and English common law. As a result, this doctrine should satisfy the Supreme Court's standing test, as discussed in Part IV. Part IV also recommends that legislatures include specific statutory language to provide for an unjust enrichment remedy. This should allow legislatures to once again use the private cause of action to enforce privacy rights. Following Part IV, I briefly conclude.

II. MODERN DATA RIGHTS

For a variety of reasons, traditional common law privacy torts are ill-suited for today's information society.[66] The result has been the emergence of statutes that give individuals specific rights in their data. The European Union ("EU") has led the way, and many of these data privacy rights can now be found in the EU's General Data Protection Regulation ("GDPR").[67] This Essay considers four of these rights: (1) the right against having personal data collected; (2) the right to access personal data when third parties have this data; (3) the right to rectify (i.e., to correct) inaccurate data possessed by others; and (4) the right to have data deleted by third parties (also known as

63. Cofone, *supra* note 61, at 1369.

64. Ormerod only seeks to "cabin[] the doctrine's most extreme implications." Ormerod, *supra* note 9, at 109.

65. Chao, *supra* note 11, at 591–600; Scholz, *supra* note 11, at 670–71.

66. *See e.g.*, Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1809 (2010).

67. Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 773 (2019) ("The EU has taken an essential role in shaping how the world thinks about data privacy.").

"the right to be forgotten").[68] There are certainly other emerging data rights, but these four are among the most prominent, and should suffice to illustrate the standing issues discussed in this Essay.

While *TransUnion* only controls standing law in federal court, it has the potential to limit these new data privacy rights in three ways. First, *TransUnion* is already limiting the ability of individuals to sue on violations of existing federal statutory data rights. Indeed, one of the violations that the *TransUnion* plaintiffs raised involved the right for a consumer to access their own data under the FCRA.[69] Second, data privacy lawsuits often cross state borders and find their way into federal court through diversity jurisdiction. Thus, *TransUnion* will impact how victims can enforce data rights provided by state law. For example, several lawsuits alleging violations of the Illinois Biometric Information Privacy Act ("BIPA") in federal court have been challenged on Article III standing grounds.[70] Finally, and perhaps most importantly, the federal government is likely to eventually pass general data privacy legislation. In fact, Congress is currently working on a draft of the ADPPA.[71] In its current form, the legislation gives consumers many of the data rights discussed below.[72] Moreover, the legislation presently includes the hotly contested private right of action.[73] But after *TransUnion*, it is unclear whether privacy victims will have constitutional standing and be able to take advantage of such a provision.

A. THE RIGHT AGAINST COLLECTION

The United States has followed Europe's lead and begun passing statutes that include some variation of each of these data privacy rights.[74] Consider the right against collection. This right allows individuals to refuse to have their personal information collected.[75] At its core, the right against collection targets privacy risk. The ultimate privacy injury occurs when a party does

68. *See* Council Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation, arts. 21, 15–17, 2016 O.J. (L 119) 45–46, 43–44 (EU).

69. *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2213 (2021).

70. *See e.g.*, Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1159–61 (7th Cir. 2021); Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1148 (7th Cir. 2020). BIPA is discussed in more detail below. *See infra* Section II.A.

71. *See generally* U.S. SENATE COMM. ON COMMERCE, SCI., & TRANSP., AMERICAN DATA PRIVACY AND PROTECTION ACT DRAFT LEGISLATION SECTION BY SECTION SUMMARY (2022), https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50 [https://perma.cc/5JVB-CVD4] (providing information about current draft of legislation).

72. *See id.*

73. *See* Lauren Feiner, *Bipartisan Privacy Proposal is 'Unworkable and Should be Rejected,' Chamber of Commerce Says*, CNBC (June 9, 2022, 11:13 PM), https://www.cnbc.com/2022/06/09/bipartisan-privacy-proposal-is-unworkable-chamber-of-commerce-says.html [https://perma.cc/98C2-4P2G].

74. *See generally* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021) (discussing how emerging U.S. privacy law follows and departs from GDPR).

75. *See id.* at 1747–48.

something with data that they should not have collected. As a result, the Supreme Court's standing jurisprudence presents a significant obstacle for private plaintiffs that seek to enforce the right against collection.

There are existing federal and state statutes that include a right not to have your data collected. The Children's Online Privacy Protection Act ("COPPA") contains one variation of this right.[76] COPPA requires operators of websites "directed at children" to "obtain verifiable parental consent prior to any collection . . . of" a child's personably identifiable data.[77] Similarly, BIPA prohibits private entities from collecting a person's biometric identifier or information without the person's written consent.[78]

While COPPA does not provide a private right of action, BIPA does allow for private lawsuits with statutory damages.[79] Some violations of BIPA may not result in the kind of concrete harms that the Supreme Court has recognized. For example, consider a situation where an employer collects its employees' retinal scans without their consent. Under *TransUnion*, this violation, without additional downstream harm, will probably not have standing. But if the scans are later used—perhaps to track the employee's location—or are inadvertently disclosed in a hack, standing should exist. In fact, disputes over BIPA standing have been frequent and a pre-*TransUnion* split arose regarding these disputes.[80] *TransUnion* seems likely to quash even more BIPA lawsuits. However, there is some possibility that courts will treat biometric privacy violations more seriously than other types of privacy violations because of the sensitive nature of the underlying data.[81] But more generally, *TransUnion* will clearly limit the ability of legislatures to enforce the right against collection with private lawsuits.

B. THE RIGHTS TO ACCESS AND CORRECT

Statutes are increasingly giving individuals the right to access their data. In many cases, the right to access is accompanied by a companion right to correct inaccurate information. According to the International Association of Privacy Professionals ("IAPP"), California, Colorado, Virginia, and Utah currently give consumers the right to access their data.[82] All four states also

76. Children's Online Privacy Protection Rule, 16 C.F.R § 312.3(b) (2022).

77. *Id.* "[V]erifiable parental consent" is also required for "use and/or disclosure of" children's data. *Id.*

78. 740 ILL. COMP. STAT. ANN. 14/15 (West 2022).

79. *Id.* 14/20.

80. Michael McMahon, *Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts*, 65 ST. LOUIS U. L.J. 897, 911–15 (2021) (discussing the circuit split in BIPA standing cases).

81. *See e.g.*, Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 141 (2019) (suggesting that people "take a broad view of possible biometric privacy harms").

82. IAPP, US STATE PRIVACY LEGISLATION TRACKER: COMPREHENSIVE CONSUMER PRIVACY BILLS 2022 1 (Oct. 7, 2022), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/W3JD-2ZZH].

give consumers the right to correct inaccurate data.[83] There is pending legislation in many other states that gives consumers the right to access their data—some of which also give the right to correct.[84] But the four states with existing laws do not provide a private cause of action for either of these rights.[85] In contrast, the FCRA provides both a private cause of action and statutory damages.[86] Thus, consumers can sue companies if they do not permit individuals to obtain all the information in their credit file and/or fail to correct inaccurate information when requested to do so.[87]

However, *TransUnion* has taught us that violating the rights to access and correct data by itself will not create the type of injury recognized by standing jurisprudence. The Supreme Court found there was no standing for inaccurate data that had not been disseminated.[88] Moreover, by focusing on the lack of causation, the Court also denied standing for violations of the FCRA's disclosure requirements.[89] Specifically, the Court said that there was no evidence that the defendant's technical failures caused the plaintiff any harm.[90]

But the Supreme Court's causation analysis highlights a problem in its standing jurisprudence in privacy law. One reason why punishing conduct that creates privacy risks can be good policy is because it avoids privacy's "causation" problem.[91] For many privacy problems, causation can be particularly difficult to prove even when wrongdoing is undisputed. Consider the ultimate types of harm that the rights to access and correct are intended to prevent. In the case of the FCRA, these rights help individuals correct errors on their credit report. Such errors can lead to the denial of a loan or even cause individuals to lose out on employment opportunities. But causation chains for such harms are long and difficult to prove. It is not easy to show that someone did not get an apartment because a credit agency wrongly handled a request to get access to the person's data. The defendant credit agency could show the apartment building did not use the credit report or that there were prospective renters with better credit.

Fortunately, not even *TransUnion* suggests that plaintiffs must prove their ultimate injuries. Instead, the Supreme Court found that dissemination of the inaccurate OFAC information was enough.[92] However, the Supreme Court is

83. *Id.* The IAPP does not list California among the states that have a right to correct, but the California Privacy Right Act has added that right effective January 1, 2023. CAL. CIV. CODE § 1798.106 (West 2023).

84. *See* IAPP, *supra* note 83, at 1.

85. *Id.*

86. 15 U.S.C. §§ 1681g, 1681i.

87. *Id.* §§ 1681g, 1681i.

88. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2211–12 (2021).

89. *Id.* at 2213.

90. *Id.*

91. Chao, *supra* note 11, at 562 (describing how credit card fraud victims cannot prove which data breach led to their injury).

92. *See TransUnion*, 141 S. Ct. at 2209.

just selecting a later point on the risk continuum. Having inaccurate information in a person's credit file and having that information disseminated are not the ultimate injuries. Rather, both problems increase the *risk* of an ultimate injury. The rights of access and correction simply focus on an earlier point on the risk continuum than dissemination—the Supreme Court's apparent choice. Of course, legislatures may believe that the best way to prevent downstream injuries is to nip the problem in the bud. For privacy injuries that means giving individuals the right to access and correct their personal data. While such rights could still be enforced by regulatory agencies, the Supreme Court's standing jurisprudence clearly frustrates this kind of legislative choice by neutering private causes of action. Indeed, the Supreme Court has clearly limited the ability of private plaintiffs to enforce the right to access and the right to correct in the FCRA.

C. THE RIGHT OF DELETION

Another right that many privacy statutes have granted is the right of deletion. One variation of this right has been called "the right to be forgotten" because it allows individuals to request that personal information on the internet be deleted.[93] But the right to deletion is broader. It can apply to any kind of business. For example, in California, a business must delete personal data upon a verified request.[94] Other variations of the right to delete require automatic deletion. For example, both COPPA and the Cable Communications Privacy Act require that personal information be deleted after the information is no longer necessary to fulfill the purpose for which the information was collected.[95] Variations of the right of deletion are found in every existing state privacy law and most pending state bills.[96]

Like the other rights discussed previously, the right to delete seeks to decrease the risk of later privacy injury. The ultimate associated harm occurs when the data that should have been deleted is improperly used. As a result, plaintiffs suing for a violation of the right to delete need some form of later injury to have standing. Even before *TransUnion*, courts have denied standing to plaintiffs because they could not allege a later injury. For example, in *Gubala v. Time Warner Cable* and *Braitberg v. Charter Communications*, the Seventh and Eighth Circuits denied standing to plaintiffs alleging that the defendant cable companies retained data in violation of the Cable

93. *See e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Proteccíon de Datos, ECLI:EU:C:2014:317, ¶¶ 2, 20, 100 (May 13, 2014) (ordering Google to remove information about a Spanish man's insolvency from its website databases).

94. CAL. CIV. CODE § 1798.105.

95. 16 C.F.R. § 312.10 (2022) (COPPA); 47 U.S.C. § 551(e) (2022) (Cable Communications Privacy Act).

96. IAPP, *supra* note 83, at 1. However, most state laws do not provide a private cause of action. *See id.*

Communications Privacy Act when there were no allegations of dissemination.[97]

Unfortunately, the result is that plaintiffs may not be able to enforce their right to delete even if they had suffered injury. In many cases, consumers will want their credit card information deleted. Indeed, that is precisely the kind of information that the cable company defendants in *Gubala v. Time Warner Cable* and *Braitberg v. Charter Communications* wrongfully retained.[98] But companies often do not report when they have been hacked.[99] In such cases, plaintiffs will never learn that they are injured. Moreover, even when a person's credit card is compromised, it is almost impossible to trace it to a particular source.[100] That is because cybersecurity incidents are so commonplace. However, when statutes give individuals the right to delete, plaintiffs do not have to prove downstream harms and trace those harms to a particular privacy violation. But according to the Supreme Court's standing jurisprudence, that privacy "feature" is really a standing "bug." The upshot is that the Supreme Court has also limited the ability to enforce the right to delete through private lawsuits.

In Part IV, I offer a solution that may avoid the injury-based framework required by *Spokeo* and *TransUnion*. Part IV argues that the theory of restitution and unjust enrichment can provide standing to plaintiffs that sue under these emerging privacy statutes. But to be certain, statutes should include specific language that provides private plaintiffs with the unjust enrichment remedy.

III. UNJUST ENRICHMENT AND STANDING

In *Privacy Losses as Wrongful Gains*, I explain how privacy victims can seek to disgorge the wrongful gains that companies earn when they break their privacy promises.[101] Thus, even though a plaintiff may not be able to show that she was harmed when a company wrongfully sold her buying history, that plaintiff should be able to recover the money the company earned from the sale.[102] Unjust enrichment also allows plaintiffs to recover wrongful savings.[103] That may occur when a company breaks a promise to use reasonable

97. Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 912–13 (7th Cir. 2017); Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 930 (8th Cir. 2016). *But see* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013)) (finding standing because of "an 'objectively reasonable likelihood'" that hackers would use data breach victims' stolen credit card information.)

98. *See Gubala*, 846 F.3d at 910; *Braitberg*, 836 F.3d at 927.

99. Dan Swinhoe, *Why Businesses Don't Report Cybercrimes to Law Enforcement*, CSO (May 30, 2019, 3:00 AM), https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html [https://perma.cc/QT84-A98U].

100. Chao, *supra* note 11 at 562 (discussing the problem of showing causation in cybersecurity incidents that steal credit card numbers).

101. *See generally id.*

102. *Id.* at 574.

103. *Id.* at 585.

cybersecurity. Unjust enrichment allows plaintiffs to recover money the company saved by failing to provide the promised level of service.[104]

Besides providing a different approach for calculating recoveries, unjust enrichment has the additional benefit of changing the standing analysis. That is because unjust enrichment does not have to worry about characterizing a *plaintiff's injury*. Instead, unjust enrichment focuses on the *defendant's wrongful gain*.[105] Indeed, unjust enrichment does not require that the plaintiff suffer any harm at all. Moreover, unjust enrichment has centuries-old roots—a critical part of both *Spokeo* and *TransUnion's* standing analyses.[106] Consequently, privacy plaintiffs that pursue these claims will be relying on the analysis the Supreme Court favors (i.e., historically recognized claims) instead of struggling against its cramped view of harm.

Although most unjust enrichment cases do not expressly mention standing, there is no doubt that plaintiffs have historically brought these claims in courts. A group of leading restitution and remedies scholars discuss numerous examples in an amicus brief in *Spokeo*.[107] Their brief described ten different types of unjust enrichment claims: (1) commercial bribes and kickbacks; (2) business opportunities; (3) other conflicts of interest; (4) misuse of confidential information; (5) forfeiture of fees; (6) intellectual property infringement; (7) trespass; (8) conversion; (9) rescission; and (10) the slayer rule.[108] These examples "span tort, contract, property, and agency law."[109] They are found in state courts, federal courts (including the U.S. Supreme Court), and English courts, and have been decided in each of the last four centuries.[110]

Notably, these claims did not require proof of injury to the plaintiff. Indeed, the *Restatement (Third) of Restitution & Unjust Enrichment* specifically notes that, "The taking of a bribe or 'secret commission' is condemned, *without regard to economic injury*, because it poses a risk of divided loyalty."[111] The U.S. Supreme Court has also recognized that unjust enrichment does not require a plaintiff to have suffered any injury. In *Jackson v. Smith*, the receiver for the plaintiff arranged to sell the plaintiff's land at auction.[112] A group of individuals— including the receiver—was the highest bidder and later resold

104. *Id.* at 584–85.

105. *See* DAN B. DOBBS & CAPRICE L. ROBERTS, LAW OF REMEDIES: DAMAGES, EQUITY, RESTITUTION § 1.1 (3d ed. 2018) ("[R]estitution is measured by defendant's gains, not by plaintiff's losses.")

106. *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 340–41 (2016); TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2204 (2021).

107. Restitution and Remedies Scholars' Brief, *supra* note 11, at *1–3. The brief was written by notable remedies scholars, Douglas Laycock, Mark Gergen, and Doug Rendleman, and numerous other remedies luminaries signed onto the brief.

108. *Id.* at *7–18.

109. Chao, *supra* note 11, at 598.

110. *Id.*

111. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 43 cmt. d, illus. 17–18 (AM. L. INST. 2011) (emphasis added).

112. Jackson v. Smith, 254 U.S. 586, 587 (1921).

the land for a profit.[113] Even though the Supreme Court recognized "that the sale was fairly conducted" and "the estate *may not have been injured*[,]" the Court awarded the plaintiff the defendants' entire profits based on breach of fiduciary duty.[114]

Historical examples like these have become an important factor in deciding standing. According to *Spokeo*, courts should assess whether the alleged injury to the plaintiff "has a close relationship to a harm . . . traditionally [recognized] as providing a basis for a lawsuit in . . . American courts."[115] *TransUnion* went on to explain that this "inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury."[116] When privacy plaintiffs advance unjust enrichment claims, they will be able to point to the many examples from the Restitution and Remedies Scholars' Brief as the "close historical or common-law analogues."

Promisingly, in 2020, one federal Court of Appeals decision did find standing based on unjust enrichment. In *In re Facebook, Inc. Internet Tracking*, the plaintiffs alleged that Facebook impermissibly "sold user data to advertisers."[117] Facebook contended "that unjust enrichment is not sufficient to confer standing" and that the plaintiffs must demonstrate some harm to themselves.[118] The Ninth Circuit rejected this argument, stating that the "[p]laintiffs sufficiently alleged a state law interest [namely, unjust enrichment] whose violation constitutes an injury sufficient to establish standing to bring their [state statutory and common law] claims."[119] While *In re Facebook* was decided prior to *TransUnion*, *TransUnion* did not address, let alone mention, the theory of unjust enrichment. In short, unjust enrichment claims have both very old and recent history on their side. Therefore, they are well suited for surviving standing challenges under the legal test set forth in *Spokeo* and *TransUnion*.

IV. STATUTES & UNJUST ENRICHMENT

The previous Part establishes that claims for unjust enrichment have standing. In this Part, I explain how statutory privacy violations can provide a basis for such a claim. Unjust enrichment can be based on different kinds of "wrongful acts."[120] This includes the "interference with legally protected interests."[121] Section 44 of the *Restatement (Third) of Restitution & Unjust Enrichment* states that "interference with legally protected interests includes

113. *Id.* at 587–88.
114. *Id.* at 587, 589 (emphasis added).
115. Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016).
116. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2204 (2021).
117. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 600 (9th Cir. 2020).
118. *Id.* at 599.
119. *Id.* at 601.
120. *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT §§ 40–44 (AM. L. INST. 2011) (listing various predicate wrongs that can serve as a basis for unjust enrichment).
121. *Id.* § 44.

conduct . . . that violates another legal duty or prohibition."[122] This can include statutory violations. For example, comment b specifically notes that "competitive practices prohibited by law, such as deceptive marketing, support a claim in restitution by the rule of this section."[123] Additionally, illustration 10 discusses how a pharmacy is liable for unjust enrichment when it sells customers' prescription records in violation of local law.[124]

To be sure, the viability of an unjust enrichment claim depends on the statute. As Andrew Kull and Ward Farnsworth put it, "the statute has to be examined carefully to see whether it allows restitution by its terms, and if not, whether it leaves room for a common-law restitution claim in the event of a violation."[125] Presumably, this means that unjust enrichment is not permitted when the legislature intentionally did not provide for private causes of action in the statute. But including or omitting a private cause of action in a privacy statute is typically hotly contested; it is doubtful that legislatures even consider whether to permit unjust enrichment as a remedy. That leads to an important question: Does a statute with a private cause of action permit a claim of unjust enrichment when it does not specifically mention that remedy?

At last, for federal law, the Supreme Court has provided some guidance. For years, the rule stated in *Mitchell v. Robert DeMario Jewelry* appeared to be settled law: "Unless otherwise provided by statute, all the inherent equitable powers of the District Court are available for the proper and complete exercise of that jurisdiction."[126] Proof that the statute excluded these powers had to be clear. The Supreme Court said that unless a statute by words or "inescapable inference" restricts the full scope of a court's equitable jurisdiction, those powers are available.[127] That includes providing equitable relief like restitution.[128]

But in 2021, the Supreme Court appeared to weaken this rule. In *AMG Capital Management v. Federal Trade Commission*, the Supreme Court was asked to decide whether the Federal Trade Commission Act ("FTC Act") authorized the Federal Trade Commission ("FTC") to seek equitable monetary relief—such as restitution—when it sued defendants in federal court.[129] The FTC Act allows the FTC to pursue entities that engage in unfair or deceptive trade

122. *Id.*

123. *Id.* § 44 cmt. b. ("[C]ompetitive practices prohibited by law, such as deceptive marketing, support a claim in restitution by the rule of this section.").

124. *Id.* § 44 cmt. b, illus. 10.

125. ANDREW KULL & WARD FARNSWORTH, RESTITUTION AND UNJUST ENRICHMENT: CASES AND NOTES 308 (2018); *see also* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT §§ 44(3)(d) (AM. L. INST. 2011).

126. Mitchell v. Robert DeMario Jewelry, Inc., 361 U.S. 288, 291 (1960) (quoting Porter v. Warner Holding Co., 328 U.S. 395, 398 (1946)).

127. *Id.* at 291.

128. *See* Caprice Roberts, *Statutory Interpretation and Agency Disgorgement Powers*, 96 ST. JOHN'S L. REV. (forthcoming 2023) (manuscript at 30–31), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4279007# [https://perma.cc/WEW2-L8TS].

129. AMG Cap. Mgmt., LLC v. FTC, 141 S. Ct. 1341, 1344 (2021).

practices in either federal court or through administrative proceedings.[130] When the FTC selects federal court, section 13(b) of the FTC Act explicitly authorizes the FTC to seek "permanent injunctions."[131] The FTC had relied on section 13(b) to "seek and win restitution and other forms of equitable monetary relief."[132]

However, the defendant in *AMG Capital* argued that section 13(b) does not authorize restitution.[133] A unanimous Supreme Court agreed with the defendant.[134] The Court first pointed out that section 13(b) only refers to injunction and said that "[a]n 'injunction' is not the same as an award of equitable monetary relief."[135] Second, the Court pointed to language suggesting that the provision focuses upon prospective—not retrospective—relief.[136] Finally, the Court noted that when the FTC chose to pursue defendants in administrative proceedings, other provisions of the FTC Act specifically allowed the imposition of monetary penalties and other forms of relief including types of restitution.[137] Thus, the Court held that restitution and disgorgement were not available when the FTC chose the federal court option.

In short, *AMG Capital* signals a shift in how the Supreme Court determines whether a specific statute authorizes a court to issue equitable remedies. Earlier decisions like *Mitchell v. Robert DeMario Jewelry* and *Porter v. Warner Holding* start with the assumption that a statute gives equitable jurisdiction to the courts and only rejects that assumption when there is an "inescapable inference" to the contrary. In contrast, *AMG Capital* looks at the statute holistically. When equitable jurisdiction was expressly made available in other provisions, the Court inferred that the legislature did not intend to provide that same authority elsewhere. One might interpret *AMG Capital* to simply suggest that the inference was inescapable in the FTC Act because the statute did not authorize a court to provide restitution and disgorgement. But that is certainly a relaxed interpretation of what "inescapable inference" means.

To the extent that legislatures wish to use unjust enrichment to give standing to privacy victims, they should be aware of *AMG Capital*. Out of an abundance of caution, new privacy statutes should explicitly allow plaintiffs to recover monies based on unjust enrichment. While common law unjust

130. Federal Trade Commission Act § 5, 15 U.S.C. § 45(a)(1)–(2).

131. *Id.* § 13(b), 15 U.S.C. § 53(b).

132. *AMG Cap. Mgmt., LLC*, 141 S. Ct. at 1346.

133. *Id.* at 1345.

134. *Id.* at 1344, 1352.

135. *Id.* at 1347.

136. *Id.* at 1348.

137. *Id.* at 1348–49. The FTC may also pursue defendants through administration proceedings. If the FTC obtains a cease-and-desist order through this avenue, section 5(l) specifically discusses "mandatory injunctions and such other and further equitable relief" as appropriate. Federal Trade Commission Act § 5(l), 15 U.S.C. § 45(l). Similarly, section 19 mentions a number of monetary forms of equitable relief including "the refund of money or return of property." *Id.* § 19, 15 U.S.C. § 57b(b).

enrichment claims have certainly proceeded without such statutory language, defendants are likely to argue that specific statutes have somehow opted out of unjust enrichment claims. Statutory language expressly recognizing unjust enrichment claims will avoid such needless disputes.

Of course, calculating unjust enrichment for a privacy violation can be difficult.[138] Consider the problem in *TransUnion*. TransUnion failed to take reasonable steps to ensure that customers with names that matched those on the OFAC list were the same people.[139] It may be difficult to ascertain how much money TransUnion wrongfully saved by failing to take reasonable measures to ensure accuracy. Similarly, if a company violates a statute that requires the deletion of personal identifiable information after one year, it may be unclear how much money the company wrongfully saved by failing to adopt a compliant program. These problems are compounded as the parties try to calculate the wrongful savings owed to specific individuals.

When monetary damages are difficult to calculate, legislatures have often allowed statutory damages as an alternative. Consider copyright remedies. The copyright statute allows a copyright owner to recover "actual damages and profits."[140] But a copyright owner may elect to recover statutory damages instead.[141] Legislatures enacting privacy statutes can do the same for restitution and unjust enrichment. Statutes could allow privacy victims to recover money based on restitution and unjust enrichment. But they could also allow victims to elect to recover statutory damages of a given dollar amount. Of course, a significant benefit would be to provide standing to plaintiffs.[142] Consequently, including this language in new privacy statutes would allow legislatures to reclaim their ability to shape privacy policy by using private causes of action.

CONCLUSION

By taking a narrow view on what constitutes a cognizable injury, the Supreme Court's recent standing jurisprudence appears to have limited the ability for laws to target risky privacy conduct using private causes of action. This occurs just as a new generation of privacy statutes are granting rights that focus on conduct that increases the risk of downstream privacy injuries. These new data rights include the right against collection of data, the right to access one's data, the right to correct inaccurate data, and the right to delete data. However, courts have long recognized suits based on unjust enrichment even

138. *See generally* Mark P. Gergen, *Causation in Disgorgement*, 92 B.U. L. REV. 827 (2012) (discussing difficulties in showing the amount of unjust enrichment caused by a particular wrongful act).

139. *See supra* Part I.

140. 17 U.S.C. § 504(b) (2020).

141. *Id.* § 504(c).

142. However, the omission of the restitution is not fatal. After all, plaintiffs can still rely on *Mitchell v. Robert DeMario Jewelry* and *Porter v. Warner Holding* to argue that a specific statutory framework does not exclude equitable remedies. But these arguments are less likely to be successful after *AMG Capital*. The safer course is to expressly provide for restitution in the privacy statute.

in the absence of injury. Thus, privacy victims should be able to use this old theory to exercise their new data rights.

Both Congress and state legislatures interested in passing privacy laws that recognize these new privacy rights should explicitly allow plaintiffs to recover based on the theory of restitution and unjust enrichment. While such language has not been historically necessary to provide a claim for unjust enrichment, it may be prudent for legislatures to include unjust enrichment language. The Supreme Court appears to disfavor many privacy claims and the existence of statutory language should maximize the chances that the Court will recognize unjust enrichment claims in each case. Hopefully, this guidance will enable legislatures to reclaim their role in shaping privacy policy using private causes of action.