Westlaw Today
powered by Reuters

TransUnion and the 'no harm no foul' effect on data privacy

By Cynthia Cole, Esq., and Nick Palmieri, Esq., Baker Botts LLP

JANUARY 10, 2022

Who is aptly placed to judge harm in data privacy? The recent *TransUnion* decision, its dissent by Justice Clarence Thomas and its effects on lower courts would suggest that the Supreme Court may not be it.

The *TransUnion* decision

On June 25, 2021, the Supreme Court issued its decision in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), finding that more than six thousand individuals whose credit files contained misleading information did not allege a sufficiently "concrete" harm to merit standing within federal courts.

The reasoning, according to the Court's majority opinion, is that merely *violating* the Fair Credit Reporting Act ("FCRA") is not enough to warrant legal redress. Rather, by the logic of this opinion, federal courts may only act when a plaintiff can show the precise, measurable harm that a corporation has done with its ill-collected, incorrect information.

In the opinion, Justice Kavanaugh outlines three factors which a plaintiff must show in order to establish standing:

(1) that they suffered an injury that is "concrete 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.

Factor 1, ultimately, is what excluded the class members in this case, since Justice Kavanaugh could find no "concrete" harm that was done by classifying these members as a "potential match" for the OFAC's database of potential terrorists/drug-dealers/other restricted individuals. But the reasoning behind the decision is tenuous, at best, and as Justice Thomas explains in his dissent, goes against the historical context of the "injury in fact" doctrine which he relies upon.

Justice Kavanaugh's opinion relies heavily upon the concept of an "injury in fact" to determine whether the plaintiffs had Article III standing. He begins by noting that various intangible harms can be concrete "with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts."[1]

Justice Kavanaugh next turns to the plaintiff's alternative argument, that the incorrect information stored by TransUnion posed a "risk of harm" due to its possible dissemination to third parties. As admitted with respect to *some* of the plaintiffs, the dissemination of this incorrect information does qualify as a concrete harm for the purposes of standing.

And yet, Justice Kavanaugh does not go so far as to recognize that the *risk* of dissemination of that information is enough to qualify as a harm ... despite the fact that dissemination of this information is exactly what TransUnion does.

Companies could take this case as a signal that they need not conform with statutory requirements, so long as they just happen not to (directly) harm consumers in the process.

Here, Justice Kavanaugh sidesteps the issue of risk of future harm by differentiating between different types of relief requested. Since the plaintiffs are not requesting injunctive relief, but rather damages, that risk has not manifested into a harm.

Pointedly, in his dissent, Justice Thomas notes, this isn't TransUnion's first run-in regarding its OFAC alert features. The report was under fire in 2005, when the courts determined that its procedures weren't adequate to ensure accuracy of providing a "match" notification. It would appear that TransUnion did not change its procedures.

Despite Justice Kavanaugh's arguments surrounding injuries in fact and dismissing the risk of harm of TransUnion's actions, the Court's opinion comes down to essentially one maxim "no harm, no foul."

Companies *could* take this case as a signal that they need not conform with statutory requirements, so long as they just happen not to (directly) harm consumers in the process; because according to Kavanaugh's opinion, mere statutory violations are not enough to provide standing in this context.

Beyond *TransUnion* — data privacy implications

While courts are still grappling with the application of *TransUnion*, parties have begun to bring these arguments at the district court (and higher) level. These principles still have significant room for further development, and court opinions in applying these principles are still in their infancy, but reviewing how many parties are applying the principles can be illustrative in how the "injury-in-fact" standard of *TransUnion* might be applied moving forward.

In Re: Blackbaud, Inc. Customer Data Security Breach Litigation, No.: 3:20-mn-02972 (D.S.C., filed April 2, 2021)

While the original filing of the *Blackbaud* case, which relates to a multi-district litigation involving the alleged breach of data privacy laws across the country, pre-dates the *TransUnion* decision, on June 28, 2021, Blackbaud filed a notice of supplemental authority citing the decision. In its notice, the Defendant noted the *TransUnion* court's determination that "the risk of future harm on its own" failed to provide standing under Article III.[2]

What these cases make clear (or rather, what they highlight is unclear) is that TransUnion's *attempt to delineate what qualifies as a harm for Article III standing is far from settled doctrine.*

While they have not submitted supplemental briefing supporting this view, based on its previous motion to dismiss, Blackbaud seems to suggest that the plaintiffs in its own case similarly lack standing to sue, as they have not alleged adequate standing under Article III, as required by *TransUnion*.

The Plaintiffs, though, in their own response,[3] emphasize that the Defendant has not (until the *TransUnion* decision came down) challenged whether a "concrete injury" has been alleged for the purpose of standing.

Even assuming that Blackbaud *can* bring the challenge, Plaintiffs further argue that they more closely resemble those class members from *TransUnion* whose credit reports were disseminated, and thus did show a concrete harm sufficient to confer Article III standing. Since the Plaintiffs' data *was breached* and thus their personal data was disseminated to various parties beyond Blackbaud.

Mastel v. Miniclip SA, No.2:21-cv-00124 (E.D. Cal., filed July 15, 2021)

While not directly related to California's data privacy laws, the *Mastel* case relates to (alleged) breaches of privacy under the California Constitution and other laws, including the California Invasion of Privacy Act. The Defendant, Miniclip, alleged that the Plaintiff failed to allege that the information was *shared* with anyone, and thus failed under *TransUnion* to allege standing under Article III.

The court, though, did not find this argument convincing.[4] In explicitly distinguishing this case from *TransUnion*, the court narrowly construed that decision as related only to the specific type of injury relevant to those class members' claims: the common law tort of defamation.

In contrast, though, here the Plaintiff's claims were more closely related to "invasion of privacy" torts. As such, mere collection of personal information without a plaintiff's consent, according to the court, provides a sufficiently "concrete" harm for purposes of Article III.

Although this case ultimately was dismissed, it provides a narrow reading of *TransUnion* which may provide a sufficient distinction for many Federal courts to distinguish from the Supreme Court's ruling. In particular, it may provide an alternative basis for the assertion of data privacy laws, which function more similarly to invasion of privacy torts than defamation. The question remains, though, as to whether other courts will find this reasoning convincing, or, even if they agree with the type of harm, will find that sufficient to distinguish from *TransUnion*

In re FDCPA Mailing Vendor Cases, Nos: 21-2312, 21-2587, 21-3002, 21-3383, 21-3434 & 21-3462 (E.D.N.Y., filed July 23, 2021)

In another case which was dismissed for a lack of standing,[5] Plaintiffs brought a class action under the Fair Debt Collection Practices Act ("FDCPA") alleging that the use of outside mailing vendors to mail debt collection letters (for sums under $500) caused harm, since certain plaintiffs did not owe any debt.

After discussing the *TransUnion* decision, the court ultimately found that the plaintiffs here had alleged even *less* harm than the class members of *TransUnion*. In particular, the court emphasizes that the information disclosed in *TransUnion* held the potential for significantly more reputational damage, since it implied that the class members there were either funding terrorists, or worse, were terrorists themselves.

In contrast, here, the "erroneous" information circulated was, at worst, the disclosure of potential debts ranging from $25 to $482.28. These amounts, even if false, were, in the court's opinion, untenable to claims of defamation that would cause hatred, contempt, or ridicule to the plaintiffs. The disclosure would still fail even other common-law torts, such as intentional infliction of emotional distress, since improper disclosure of these debts was not "extreme and outrageous conduct."

This case demonstrates an application of the *TransUnion*, in contrast to *Mastel*, in which the court used the *TransUnion* standard as a bar to plaintiffs, requiring them to show a heightened standard of damages, and denying the alleged damages even at the pleadings stage.

A major facet of these cases, though, is the emphasis on the type of damage (and thus the underlying tort/harm which would qualify

the plaintiffs for Article III standing) alleged by the plaintiffs. The differing outcomes in these cases can be attributed, at least in part, to the underlying "tort" to which the damages are analogized, as was done by the Supreme Court.

By tailoring a specific injury, with a comparable underlying tort that may not require as high a burden of showing harm, plaintiffs, in data privacy or other cases, may be able to fashion claims which would hold up even in Federal courts.

Conclusion

What these cases make clear (or rather, what they highlight is unclear) is that *TransUnion*'s attempt to delineate what qualifies as a harm for Article III standing is far from settled doctrine. Even under the Supreme Court's guidance, parties in Federal courts struggle to define adequate harms, and are left to struggle with proposed theories until they can find more definite strategies.

TransUnion analogized to the harm of defamation, while *Mastel* compares the harms to "invasions of privacy." And while on its face this might look like a win for data-consuming companies, it, in fact, will most likely promote more complex and expensive litigation over the definition of harm.

Perhaps Justice Thomas's dissent is correct, and these cases will be pushed into state courts, where state laws can more explicitly set forth harms caused by data breaches, without relying upon flimsy (or at the very least inapt) comparisons to common law torts.

Given the increasing scope and scale of data privacy laws and cases throughout the country, though, this issue is expanding beyond state-specific harms, and is quickly becoming a national concern. To that end, it is perhaps increasingly incumbent upon Congress to be the originator of new, more certain data privacy legislation.

Notes

[1] Slip Op. at 9.

[2] *In Re: Blackbaud, Inc. Customer Data Security Breach Litigation*, Case No.: 3:20-mn-02972, ECF: 118 (D.S.C., filed June 28, 2021).

[3] Plaintiffs' Response to Defendant Blackbaud, Inc's Notice of Supplemental Authority, *In Re Blackbaud*, ECF: 120 (D.S.C., filed July 1, 2021).

[4] It is important to note, though, that the Court did ultimately dismiss the claims, but explicitly distinguished from *TransUnion* in doing so.

[5] Though the judge noted that it was without prejudice to refiling in State Court, per Justice Thomas's dissent in *TransUnion*.

About the authors

Cynthia Cole (L) is a partner at **Baker Botts** and serves as the deputy department chair of the corporate section in the firm's Palo Alto, California, and San Francisco offices. Her practice focuses on corporate, strategic and technology transactions and data privacy. She can be reached at cynthia.cole@bakerbotts.com. **Nick Palmieri** (R) is an associate in the intellectual property practice of the firm's New York office. He has experience in the data privacy space, having assisted clients with data breach notification requirements and compliance with GDPR and CCPA regulations. He can be reached at nick.palmieri@bakerbotts.com.

This article was first published on Westlaw Today on January 10, 2022.