ESSAY

PRIVACY STANDING[†]

PAUL M. SCHWARTZ[*]

ABSTRACT

The last decades have seen a torrent of legislative, regulatory, and judicial activity concerning data privacy around the world. Currently, some 162 countries have data privacy statutes. But the American constitutional law of standing, as shaped by the Supreme Court, has become a potent threat to data privacy. In recent decisions, the Supreme Court has constructed constitutional barriers against enforcement of Fair Information Practices (FIPs) by private parties. Yet FIPs have been the key components of data privacy legislation since the 1970s. Moreover, the Supreme Court in these cases weakens Congress' power to legislate by inventing a faux-historical constitutional law of standing that rests on private law antecedents. In inventing this new tradition, the Court requires a shift to common-law privacy baselines.

In limiting Congress' ability to legislate remedies, the Supreme Court has undercut consumer privacy protections. The Court's approach to privacy standing also forms part of its larger project to increase its power at the cost of other legal institutions. In addition to restricting congressional ability to legislate FIPs, a cornerstone of modern data privacy law, the Supreme Court's caselaw regarding privacy standing demonstrates how it manipulates doctrine to select the litigants that it wishes to favor. This paper concludes by pointing to the Court engaging in "Calvinball," a game in which players make up the rules as they go along.

[†] This Essay grows out of the *Boston University Law Review* Symposium: Information Privacy Law at the Crossroads, held at Boston University School of Law on November 3, 2023.

[*] Jefferson E. Peyser Professor of Law, University of California, Berkeley, School of Law. For their insightful comments on an earlier draft, I would like to thank Dean Erwin Chemerinsky, Danielle Citron, Daniel Solove, and Ari Waldman. Thanks as well to Caroline Grady of the *Boston University Law Review* for her excellent editorial work.

CONTENTS

INTRODUCTION

The U.S. Constitution does not make use of the word "standing." The Supreme Court has drawn on the language in Article III of the Constitution regarding "cases" or "controversies," however, to craft standing requirements that restrict the ability of plaintiffs to bring lawsuits. Article III standing requires that a party demonstrate an injury from the contested state action that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[1]

Through its standing doctrine, the Supreme Court has restricted the ability of the judiciary to intervene in certain matters because the underlying matter is not considered to be properly justiciable. In Dean Erwin Chemerinsky's critical assessment, "[t]he result of these restrictions is that governments may commit constitutional violations that no person has standing to challenge in court, in which case the Constitution goes unenforced."[2] As an example of such a standing case in the context of information privacy law, *Clapper v. Amnesty International USA*[3] raises all-but-impossible hurdles for plaintiffs seeking to contest a statute that authorizes national security surveillance.[4]

There is another dimension to the Supreme Court's standing doctrine, however, and it will have a deleterious impact on the ability of Congress to legislate in the privacy area. In *Spokeo, Inc. v. Robins* (2016),[5] and then *TransUnion LLC v. Ramirez* (2021),[6] the Court constructs constitutional barriers against enforcement of Fair Information Practices ("FIPs") by private parties.[7] Yet FIPs have been the key components of data privacy legislation since the 1970s, not only in the United States but throughout the world.[8] Moreover, the Court in these cases weakens Congress' power to legislate by inventing a faux-historical constitutional law of standing that rests on private law antecedents.

This new doctrine has destructive potential for data privacy law. It creates a new tradition for privacy standing, and represents a rearguard action, more than a half century after the rise of a modern law responding to the computerization of personal data. In the United States, this area of law is called data privacy or information privacy, and it establishes rules for the collection, use, storage, and disclosure of personal data. These rules draw on FIPs, which are the building

[1] Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010).

[2] ERWIN CHEMERINSKY, CLOSING THE COURTHOUSE DOOR: HOW YOUR CONSTITUTIONAL RIGHTS BECOME UNENFORCEABLE 98 (2017).

[3] 568 U.S. 398 (2013).

[4] *See id.* at 437 (Breyer, J., dissenting).

[5] 578 U.S. 330 (2016).

[6] 594 U.S. 413 (2021).

[7] *See Spokeo*, 578 U.S. at 342; *TransUnion*, 594 U.S. at 442.

[8] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1824 (2011). For a critical look at FIPs and an argument that additional safeguards are also needed, see Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017).

blocks of this legal field. In Europe and in the rest of the world, data protection law is the term for this area of law. Here, too, there has been a recourse to FIPs. Throughout the world, these types of statutes represent the law's best efforts to respond to the computerization of personal data by government and industry. Created during the age of mainframe computers, data privacy law has continued to develop and evolve in response to the Internet, cloud computing, and now artificial intelligence.

The last decades have seen a torrent of legislative, regulatory, and judicial activity concerning data privacy around the world. Currently, some 162 countries now have data privacy statutes.[9] But the American constitutional law of standing, as shaped by the Supreme Court, has become a potent threat to legislative attempts in the United States to safeguard data privacy. In limiting Congress' ability to legislate remedies, the Supreme Court has undercut consumer privacy protections. The Court's approach to privacy standing also forms part of its larger project of increasing its power at the cost of other legal institutions. In addition to restricting congressional ability to legislate FIPs, a cornerstone of modern data privacy law, the Supreme Court's case law regarding privacy standing demonstrates how it manipulates doctrine to select the litigants that it wishes to favor. This Essay concludes by pointing to the Court's "Calvinball," a game in which players make up the rules as they go along.

I. LETTERS NEVER SENT AND THE PUZZLE OF PRIVACY STANDING

This Part analyzes the three important Supreme Court precedents that in a mere decade have radically reshaped the law of constitutional standing. The first case of the triad, *Clapper*, sets roadblocks for litigants faced with secret surveillance.[10] It is a decision about the need for *a personally suffered injury*.[11] The operationalization of standing doctrine as a limit on *congressional action*, begins in the next case, *Spokeo*, and reaches its current high point in *TransUnion LLC v. Ramirez*. *Spokeo* somewhat disingenuously explains standing as a "doctrine developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood."[12] But in that case, it used standing not to restrict federal courts, but to announce limits on *congressional authority* to protect against certain kinds of harms to privacy interests.[13]

A. *The Road to* TransUnion

In 2021, the Supreme Court decided *TransUnion LLC v. Ramirez*, its most recent and most important standing case for information privacy law. In

[9] Graham Greenleaf, *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills*, PRIV. L. & BUS., Feb 2023, at 1, 3-4 (2023).

[10] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

[11] *See id.* at 411.

[12] *Spokeo*, 578 U.S. at 338.

[13] *See id.* at 341.

TransUnion, in an opinion written by Justice Kavanaugh, the Court's succinct mantra was, "No concrete harm, no standing."[14] To understand, the impact of *TransUnion*, we first analyze the two cases leading up to it.

1. *Clapper*: Keeping Plaintiffs from the Courthouse

In *Clapper v. Amnesty International USA*, the Supreme Court considered a standing case in the area of national security.[15] A group of journalists contended that governmental surveillance under Section 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA") violated their Fourth Amendment and statutory rights.[16] These plaintiffs could not prove, however, that the government had actually surveilled their communications using the statutory provision that they wished to contest. That is unsurprising; the existence of such surveillance is generally a secret to those whose communications are targeted. The plaintiffs could only argue that there was "an objectively reasonable likelihood that their communications will be acquired . . . at some point in the future."[17] The plaintiffs further contended that they had suffered a present injury because the threat of surveillance under Section 702 "forced them to take costly and burdensome measures to protect the confidentiality of their international communications."[18]

In an opinion by Justice Alito, the *Clapper* Court rejected both claims and held that the litigants lacked Article III standing. This five-four decision ended these litigants' attempt to determine whether the government had engaged in unauthorized activities under Section 702. In the Court's summary, the respondents "cannot demonstrate that the future injury they purportedly fear is certainly impeding and . . . they cannot manufacture standing by incurring costs in anticipation of non-imminent harm."[19]

As to the first claim regarding the impeding nature of the surveillance, FISA "at most *authorizes*—but does not *mandate* or *direct*—the surveillance that respondents fear . . . ."[20] To illustrate this point, the Court spun out a series of hypotheticals. First, the government might not target the communications of the respondents or their foreign contacts. Second, the government might target the foreign contacts of the litigants, but do so under a statute other than Section 702. Third, the FISA court might reject an attempt by the government to obtain the required Section 702 order, which would prevent the surveillance from taking place. Fourth, the government might obtain such an order, but the attempted surveillance would be unsuccessful. Finally, even if foreign contacts had been

[14] TransUnion LLC v. Ramirez, 594 U.S. 413, 417 (2021).

[15] *Clapper*, 568 U.S. at 401.

[16] *Id.*

[17] *Id.*

[18] *Id.* at 402.

[19] *Id.* at 422.

[20] *Id.* at 412.

surveilled, perhaps the government might not obtain the litigant's communications with these parties.[21]

In short, the plaintiffs had made only "conjectural" allegations and failed to demonstrate imminent harm.[22] In Justice Breyer's dissent in *Clapper*, in contrast, the plaintiffs were seen as parties who had engaged in electronic communications of the kind that the contested statute was designed to reach.[23] In addition, the government had a strong motive to listen to conversations of the kind likely to occur. Moreover, despite the majority's endless stream of hypothetical improbabilities, Justice Breyer observed simply that there was "a very strong likelihood" that the government acting under its statutory authority would have intercepted some communications of the plaintiffs.[24]

The Supreme Court issued its decision in *Clapper* on February 26, 2013.[25] A few months later, on June 6, 2013, the *Washington Post* in the United States and the *Guardian* in the United Kingdom began to publish documents about U.S. government surveillance leaked by Edward Snowden, an errant former employee and then-contractor of the National Security Agency ("NSA").[26] These publications revealed, among other matters, that the NSA had engaged in widespread surveillance under FISA Section 702.[27] Through its hitherto secret Prism and Upstream programs, the NSA had collected communications from Google, Facebook, and other large U.S. tech companies (Prism) and targeted communications sent over the Internet backbone (Upstream).[28] The Snowden documents demonstrated "that the NSA is able to search for names, emails, and other personal information through databases."[29] A 2017 summary of the

[21] *Id.* at 412-14.

[22] *Id.* at 412.

[23] *Id.* at 427 (Breyer, J., dissenting).

[24] *Id.* at 430.

[25] *Id.* at 398 (majority opinion).

[26] Barton Gellman, Aaron Blake & Greg Miller, *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST (June 9, 2013, 6:20 PM), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html; Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded [https://perma.cc/5ZEA-8ZEV].

[27] *Edward Snowden Discloses U.S. Government Operations*, HISTORY, https://www.history.com/this-day-in-history/edward-snowden-discloses-u-s-government-operations [https://perma.cc/B66D-H6WT] (last updated June 3, 2024).

[28] Matthew Guariglia, Cindy Cohn & Andrew Crocker, *10 Years After Snowden: Some Things Are Better, Some We're Still Fighting For*, ELEC. FRONTIER FOUND. (May 19, 2023), https://www.eff.org/deeplinks/2023/05/10-years-after-snowden-some-things-are-better-some-were-still-fighting [https://perma.cc/G66D-HBWG].

[29] Sneha Indrajit, Celia Louie & Jessica L. Beyer, *FISA's Section 702 & the Privacy Conundrum: Surveillance in the U.S. and Globally*, UNIV. OF WASH. (Oct. 25, 2017),

documents argued that they showed "the incidental collection of U.S. citizens' data is inevitable and a central point of controversy about 702."[30] And a 2023 analysis from the Electronic Frontier Foundation, a civil liberties nongovernmental organization, asserted "[t]hrough both upstream and downstream surveillance under Section 702—a law that relaxes constitutional and other privacy safeguards in the name of targeting foreign surveillance—the intelligence community gains access to Americans' online communications that it would regularly need a warrant to access."[31]

If the Snowden leak had come earlier, it might have played a decisive role in the *Clapper* Court's decision-making. Only one more vote was needed to transform Justice Breyer's commonsense dissent into the majority opinion. Justice Breyer's view was entirely validated by the subsequent reports of widespread NSA surveillance through Prism and Upstream. As Justice Breyer expressed in his dissent:

> One can, of course, always imagine some special circumstance that negates a virtual likelihood, no matter how strong. But the same is true about most, if not all, ordinary inferences about future events. Perhaps, despite pouring rain, the streets will remain dry (due to the presence of a special chemical). But ordinarily a party that seeks to defeat a strong natural inference must bear the burden of showing that some such special circumstance exists.[32]

The harm facing the plaintiffs proved to be far from "speculative," as the *Clapper* majority had wrongfully concluded.

Indeed, in 2021, the European Court of Human Rights ("ECHR") adopted the kind of common-sense approach that Justice Breyer proposed in *Clapper.* In *Centrum För Rättvisa v. Sweden*, the ECHR considered the application of a litigant who argued that "Swedish legislation and practice in the field of signals intelligence violated" rights protected by Article 8 of the European Convention on Human Rights.[33] Article 8 of the Convention guarantees an individual "the right to respect for his private and family life, his home and his correspondence."[34] In *Centrum För Rättvisa,* Sweden argued, similarly to the U.S. government in *Clapper*, that the lawsuit was being brought by someone who could not prove the government was targeting him in its bulk surveillance.[35]

---

https://jsis.washington.edu/news/controversy-comparisons-data-collection-fisas-section-702/ [https://perma.cc/SG2N-RC6H].

[30] *Id.*

[31] *Upstream vs. PRISM*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/upstream-prism [https://perma.cc/MN73-73ST] (last visited Oct. 21, 2024).

[32] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 431 (2013) (Breyer, J., dissenting).

[33] Centrum För Rättvisa v. Sweden, App. No. 35252/08, ¶ 3 (May 25, 2021), https://hudoc.echr.coe.int/eng?i=001-210078.

[34] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

[35] *Centrum För Rättvisa*, App. No. 35252/08, ¶¶ 155-60. For Sweden's application making this argument, see *id.* at ¶¶ 12, 152, 154, 155, 157, 160, 168.

Similar to the chain of improbabilities posed by Justice Alito in *Clapper*, Sweden even argued that "virtually no risk" existed for the litigant of having "communications being retained for further scrutiny" because the surveillance in question was always "restricted to foreign threats and circumstances."[36] The ECHR swept this argument aside even while agreeing with Sweden "that the applicant does not belong to a group of persons or entities targeted by the Swedish signal intelligence legislation and measures."[37] The ECHR pointed to the danger that requiring proof of "the applicant's victim status" would render any litigation impossible.[38] Demonstrating "that one's communications are of interest for agencies tasked with foreign intelligence [is] an almost impossible task, having regard to the secrecy inherent in foreign intelligence activities."[39]

Doctrinally, *Clapper* took a different approach than *Centrum För Rättvisa* and required that plaintiffs demonstrate that they were injured, or likely to be injured. The plaintiffs in *Clapper* included "attorneys and human rights, labor, legal and media organizations" in their ranks.[40] These litigants argued that the contested statute "compromise[d] their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[41] It caused them to cease having "certain telephone and e-mail conversations."[42] Ultimately, the core concern of the plaintiffs was how the contested surveillance statute chilled their communications and violated their protections under the First Amendment. The *Clapper* Court's rejection of these arguments as inadequate proof of impending future injury points to a theme present in the next two standing cases, which, albeit doctrinally focused elsewhere, reflects the same troubling lack of concern for privacy.

In *Clapper*, the lack of value assigned to privacy is especially striking because the Supreme Court is otherwise highly protective of First Amendment interests. Consider, for example, the Court's recent decision in *303 Creative LLC v. Elenis*.[43] There, the Court found standing for Lorie Smith, a graphic designer who wished to expand her business to include services for couples who desired a wedding website.[44] The difficulty? Colorado had enacted an anti-discrimination act; a same sex couple might ask her to design a wedding website for them; doing so would violate her "sincerely held religious conviction" that marriage was "a union between one man and one woman"; and Colorado might enforce this law against her.[45]

[36] *Id.* at ¶ 171.

[37] *Id.* at ¶ 168.

[38] *Id.* at ¶ 171.

[39] *Id.*

[40] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 406 (2013).

[41] *Id*.

[42] *Id*.

[43] 600 U.S. 570 (2023).

[44] *Id*. at 583.

[45] *Id*. at 582-83.

Like the litigants in *Clapper*, Ms. Smith had free speech concerns. As she successfully argued in *303 Creative LLC*, should Colorado use an anti-discrimination law to force her to design a website for a same-sex couple, it would be compelling her to engage in a speech act.[46] Yet, at the time of the litigation all she could point to regarding a "certainly impending future harm" was a set of concerns, or as the Court termed it, her "worries."[47] She had never designed a wedding website of any kind, and did not yet have a functioning business to do so. As the Court noted, "[w]hile Ms. Smith has laid the groundwork for her new venture, she has yet to carry out her plans."[48]

Nonetheless, Ms. Smith's worries about her fate should she enter the wedding website business were sufficient for the Supreme Court to find that she had standing. In *Clapper*, in contrast, the lawyers and human rights activists did not merely plan one day to "engage in sensitive international communications with individuals who they believe are likely targets of surveillance" under the challenged statute.[49] Rather, the litigants were actively communicating with clients who were likely to be surveilled by the government under the contested statute. Another difference between the cases is that the *Clapper* litigants tried to use the First Amendment to protect their data privacy, that is, their interest in communicating without the government listening in. The Supreme Court does not appear to have valued this interest highly, especially in contrast to *303 Creative LLC*, where it was acutely attentive to the harms from compelled speech that would violate an individual's religious beliefs.

2. *Spokeo*: Limiting Fair Information Practices

Nonetheless, post-*Clapper*, the Supreme Court doubled down on its quest to toughen standing requirements. In *Spokeo v. Robins*, in another opinion by Justice Alito, the Court returned to the matter of injury in fact.[50] In *Clapper*, the Court determined that an injury sufficient to permit federal litigation had to be an *imminent* one.[51] For the *Spokeo* Court, in a six-two decision, the injury also had to be both *particularized* and *concrete*.[52] In *Spokeo*, and for the first time in its history, the Supreme Court identified the concreteness of an injury as a separate requirement. Specifically, a *concrete* injury had to involve more than a personal interest of the plaintiff, such as a statutory violation that affected the party individually. Rather, a concrete injury had to be a "*de facto*" one; it had to "actually exist."[53]

[46] *Id*. at 588.

[47] *Id*. at 580.

[48] *Id*. For further analysis of this case, see Leah M. Litman, Melissa Murray & Katherine Shaw, *Of Might and Men*, 122 MICH. L. REV. 1081, 1096-98 (2024)

[49] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

[50] Spokeo, Inc. v. Robins, 578 U.S. 330, 334 (2016).

[51] *Clapper*, 568 U.S. at 409.

[52] *Spokeo*, 578 U.S. at 339.

[53] *Id.* at 340.

A quick review of the facts of *Spokeo* would be helpful at this juncture. *Spokeo* concerned "a people search engine" that collected aggregated data about individuals.[54] Once this company began to sell information to employers who wished to evaluate job applicants, it fell under the jurisdiction of the Fair Credit Reporting Act of 1970 ("FCRA"). Spokeo failed to comply, however, with the requirements of that venerable information privacy statute.

Clapper was a case that shut the courthouse doors before plaintiffs. Certain violations of privacy might never be discovered because no suitable plaintiff existed.[55] In *Spokeo*, fatefully, the Supreme Court began its project of turning standing law into a significant limiting factor on Congress' ability to enact legislative protections for personal information. A harm had to be more than one that the FCRA established. To comply with the requirements of Article III, this harm had to have separate and sufficient constitutional weightiness as a "concrete" injury. The Court was insistent that "Robins cannot satisfy the demands of Article III by alleging a bare procedural violation."[56] And this decision made clear that the Supreme Court would have the final word on the kinds of privacy injuries that count, not Congress.

As to the content of the required constitutionally cognizable concrete injury, Justice Alito provided only vague guidelines as he directed the case back to the Ninth Circuit. Such harms could be tangible or intangible.[57] In some instances, the violation of a procedural right might be sufficient.[58] In other cases, it would not. For example, if the personal data in a credit file were accurate and no notice was provided to the data subject, there would be no concrete harm, according to the Supreme Court.[59] Moreover, "an incorrect zip code, without more," was deemed unlikely to work concrete harm.[60]

Finally, the Supreme Court decided that a key element in evaluating a statutory interest for standing involved a turn to the past. Here was the first step in the Court's cobbling together of a faux-historical theory of standing. As the *Spokeo* Court announced, an important factor in assessing the concreteness of a claimed harm was whether it "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or

[54] *Id.* at 333.

[55] Exacerbating this situation, the National Security Agency has failed to provide a public estimate of the number of the communications of U.S. persons "incidentally" collected pursuant to Section 02. *See* Jake Laperruque, *CDT and over 20 Civil Society Groups Call for Estimate of Americans Impacted by FISA Section 702 Surveillance*, CTR. FOR DEMOCRACY & TECH. (Oct. 16, 2024), https://cdt.org/insights/cdt-and-over-20-civil-society-groups-call-for-estimate-of-americans-impacted-by-fisa-section-702-surveillance/ [https://perma.cc/YM2N-QCPV].

[56] *Spokeo*, 578 U.S. at 342.

[57] *Id.* at 340.

[58] *Id.* at 342.

[59] *Id.*

[60] *Id.*

American courts."[61] This pronouncement is startling; it was also made without additional clarification of its basis or logical justification.

To understand why this move is a radical one, we should link it to the *Spokeo* Court's dismissal of the concreteness of a mere "procedural" violation. Prior to *Spokeo*, the Supreme Court had long held that Congress could create new interests and rights by enacting them in law.[62] Consider *Trafficante v. Metropolitan Life Insurance Co.*,[63] a unanimous opinion from 1972. In it, the Court found that Article III permitted Congress broad powers in creating new rights and assigning enforcement powers to individuals to receive remedies for violations.[64] Quoting the lower court's opinion, the *Trafficante* Court held that Congress could legislate standing broadly, "as is permitted by Article III of the Constitution," and let private parties enforce a federal statute against discriminatory housing practices.[65]

Another example of Congressional creation of new kinds of statutory rights would be the "informational interests" of "testers," who are individuals gathering information about matters such as the potential discriminatory practices of landlords and hotel owners.[66] The Supreme Court has long upheld the federal laws that permit these parties access to federal courts. We return to the important matter of informational interests below, as it is closely related to classic kinds of data privacy rights.

As for data privacy law, *Spokeo* evaluated a claim raised under the FCRA, the first federal information privacy law in the United States, and a statute that had survived almost a half-century without any doubts about the constitutionality of the interests that it provides to individuals or the obligations it places on credit reporting agencies.[67] Moreover, the FCRA's obligations and interests embody Fair Information Practices ("FIPs").[68] Just as any language has its linguistic elements, such as verbs, nouns and articles, data privacy law constructs itself out of different FIPs, which are expressed in concrete ways that vary in different statutes and regulations. FIPs establish duties and responsibilities for entities that process personal data and set out interests that people should have regarding

[61] *Id.* at 341.

[62] *See, e.g.*, FEC v. Akins, 524 U.S. 11 (1998); Havens Realty Corp. v. Coleman, 455 U.S. 363 (1982); Warth v. Seldin, 422 U.S. 490 (1975); Linda R.S. v. Richard D., 410 U.S. 614 (1973); Trafficante v. Metro. Life Ins. Co., 409 U.S. 205 (1972); FCC v. Sanders Bros. Radio Station, 309 U.S. 470 (1940).

[63] 409 U.S. 205 (1972).

[64] *Id.* at 209.

[65] *Id.* (quoting Hackett v. McGuire Bros., 445 F.2d 442, 446 (3d Cir. 1971)).

[66] *Havens Realty Corp.*, 455 U.S. at 373-74.

[67] For background on this statute, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 631-33 (8th ed. 2024).

[68] *See* Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV. 1252, 1259-61 (2022).

their information.[69] FIPs have been enormously influential in shaping data privacy statutes and are the common building blocks of modern data privacy law.

In *Spokeo*, however, the Court suggested that some FIPs established in law might be insufficient for standing purposes. A critical factor in deciding concreteness will be to assess whether the injury to a FIP resembles one protected by the common law. Yet, the function of FIPs, the reason for their creation, was to go beyond those protections. This Essay develops this point below. The *Spokeo* Court ended by ordering the Ninth Circuit to re-evaluate the case and decide if there had been a concrete injury to Robins.[70] On remand, the Ninth Circuit promptly found concrete harm and, hence, standing for the plaintiffs.[71] While all ended well for Robins at the Ninth Circuit, the *Spokeo* Court had started to construct a constitutional hurdle against enforcement of FIPs by private parties.

B. TransUnion*: Adopting Common Law Faux-Historicism for Standing*

The next step, the one taken by the Supreme Court in *TransUnion,* is to draw on *Spokeo* to craft something new under the sun: a common law historicism grafted onto standing doctrine. The question was which injuries mattered for constitutional standing, and the answer would now turn on whether the common law protected against analogous harms.[72]

1. The Facts

In this class action lawsuit, plaintiffs sued TransUnion for preparing misleading credit reports in violation of FCRA requirements. The credit reports in question "erroneously flagged many law-abiding people as potential terrorists and drug traffickers."[73] TransUnion had drawn on the Treasury Department's list of "specially designated nationals," which recorded the names of terrorists and drug traffickers. The Office of Foreign Assets Control ("OFAC") at the Treasury Department maintained this governmental database, and TransUnion termed its add-on product, the "OFAC Name Screen Alert."[74] It packaged this information along with its established line of credit reports and sold it to businesses at an enhanced price compared to the price solely for credit reports.

The product was good news for TransUnion as a source of additional revenue, but bad news for many individuals. TransUnion had engaged in a strikingly haphazard approach to aggregating the governmental information with its existing databases. As Justice Thomas pointed out in dissent, it "did not compare birth dates, middle initials, Social Security numbers, or any other available

[69] *Id.* at 1261-64.

[70] Spokeo, Inc. v. Robins, 578 U.S. 330, 342-43 (2016).

[71] Robins v. Spokeo, Inc., 867 F.3d 1108, 1118 (9th Cir. 2017).

[72] TransUnion LLC v. Ramirez, 594 U.S. 413, 424 (2021).

[73] *Id.* at 442 (Thomas, J., dissenting).

[74] *Id.* at 419 (majority opinion).

identifier routinely used to collect and verify credit-report data."[75] Rather, TransUnion drew on first and last names on the OFAC list and matched that information with first and last names in its own credit report database.[76]

The result? As Justice Thomas noted in his dissent, "[u]nsurprisingly, these reports kept flagging law-abiding Americans as potential terrorists and drug traffickers."[77] In its decision finding for the class, the Ninth Circuit declared that these practices of TransUnion violated requirements under the FCRA both to "follow reasonable procedures to assure maximum possible accuracy" in consumer credit files and to provide mandated disclosures to consumers of their rights and information in their reports.[78]

2. The Holding

For the *TransUnion* majority, some, but not all, of the plaintiffs identified concrete harms for purposes of Article III standing. The certified class had 8,185 members, but the Supreme Court found only 1,853 members of the class, including Ramirez, identified a concrete harm.[79] TransUnion had disseminated the credit reports of these 1,853 individuals to businesses; the other 6,332 class members did not have their information sent out. For the Court, "the mere existence of inaccurate information in a database is insufficient to confer Article III standing."[80] It also rejected the claims that TransUnion had failed to comply with the FCRA's mandated disclosure requirements; Justice Kavanaugh created a clever, if misleading, neologism to minimize these failures by terming them "formatting errors."[81]

In *Spokeo*, the Court discussed a number of approaches for determining whether a harm was concrete before landing, almost in an aside, on how it would be "instructive" to consider whether an alleged intangible injury "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[82] In *TransUnion*, the Court elevated this inquiry to the predominant focus for standing analysis. History and tradition were the crucial issues, and the critical analysis "asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury."[83] At the same time, however, "*Spokeo* does not require an exact duplicate in American history and tradition."[84] But courts may not "loosen

[75] *Id.* at 443 (Thomas, J., dissenting).

[76] *Id.*

[77] *Id.* at 444.

[78] Ramirez v. TransUnion LLC, 951 F.3d 1008, 1025 (9th Cir. 2020).

[79] *See TransUnion*, 594 U.S. at 442.

[80] *Id.* at 434.

[81] *Id.* at 418.

[82] Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016).

[83] *TransUnion*, 594 U.S. at 424.

[84] *Id.*

Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts."[85]

From that point, the majority opinion in *TransUnion* drifted into the kind of vagueness also found in *Spokeo*. Tangible harms, such as physical harms and monetary harms, were concrete ones.[86] Various intangible harms could also count, especially ones "traditionally recognized as providing a basis for lawsuits in American courts."[87] These injuries "include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion."[88] The first item in the list refers to common law defamation; the next ones represent two of the four privacy torts. As for Congress, its views may be "instructive," as *Spokeo* had already conceded, but Congress could not make all interests legally protectible merely by enacting protection for them into legislation.[89]

In short, a plaintiff will not satisfy the injury-in-fact requirement simply because a statute grants a right to her. Here was a novel approach; the Supreme Court had long upheld the ability of Congress to create statutory rights for which a violation would be deemed an injury sufficient for standing.[90] As noted above, for example, the Supreme Court had upheld the interests of "testers," who were found to have standing related to receipt of "truthful information about available housing," regardless of whether these individuals planned to rent the properties in question.[91]

As for the plaintiffs in *TransUnion*, the majority identified a decisive difference between the plaintiffs whose information had been released by the credit reporting agency (the 1,853) and those whose information remained in the TransUnion database (the 6,332). For those whose information had not been released, the Court analogized the situation to the common law tort of defamation. It was as if a defamatory letter was written, but kept stored in a desk drawer. For the *TransUnion* Court, "[a] letter that is not sent does not harm anyone, no matter how insulting the letter is. So too here."[92]

As for the claims regarding the failure of TransUnion to properly provide statutorily required information to the plaintiffs, the Supreme Court dismissed these claims for all class members as a mere "formatting error."[93] It rejected the argument made by the United States as amicus curiae that the plaintiffs had suffered a concrete "informational injury." The Court found that the plaintiffs

[85] *Id.* at 425

[86] *See id.*

[87] *Id.*

[88] *Id.*

[89] *See id.* (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016)).

[90] *See* cases cited *supra* note 62.

[91] Havens Realty Corp. v. Coleman, 455 U.S. 363, 373-74 (1982).

[92] *TransUnion*, 594 U.S. at 534.

[93] *Id.* at 441.

had failed to show "any evidence of harm" caused by the insufficiencies of the disclosure to them by TransUnion.[94]

The *TransUnion* holding represents a significant threat to information privacy law. Foundational FIPs mandate that a party receive notice and access to one's personal information. In the privacy guidelines adopted by the Organisation for Economic Cooperation and Development ("OECD") in 1980, these requirements are termed the "Individual Participation Principle."[95] In the American Law Institute's *Principles of the Law: Data Privacy* (2020), a project that seeks to "guide the protection of data privacy in various areas and types of law," these FIPs are expressed through various mandates, including requirements of "Individual Notice" and "Access and Correction."[96] Yet, *TransUnion* makes federal courts the arbiter, rather than Congress, of the kinds of violations of FIPs that are constitutionally cognizable.

The result in *TransUnion* also ignores the aim of the FCRA, a statute in which Congress embedded FIPs to protect personal privacy. It took this action at a time when the credit reporting industry had begun to digitalize its products and services. A historian of financial identity in the United States, Josh Lauer explains that the FCRA was a response to the ongoing computerization of the paper records of the consumer reporting industry.[97] Lauer writes, "Where the existence of millions of individual paper files, dispersed among thousands of local credit bureaus, had been uncontroversial, the prospect of this detailed personal information flowing directly into a single database produced terror."[98] After enactment of the FCRA, the blue-ribbon Privacy Protection Study Commission noted how "[p]ersonal interaction in consumer credit transactions has declined markedly in the last several decades," and that "recorded information is now the paramount factor in establishing and maintaining credit relationships."[99]

The *TransUnion* Court's desk drawer metaphor is inapposite. In enacting the FCRA, Congress intended to create safeguards in response to a mass collection and processing of digitalized information unknown to the common law. The FCRA is concerned with how the credit reporting industry collects, retains, and sells personal information as well as the kinds of rights that consumers should have in light of the practices of these companies. It seeks to prevent harms from

[94] *Id.* at 440-41.

[95] OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA § 13 (2002).

[96] PRINCIPLES OF THE L., DATA PRIV. intro. note, §§ 4, 8 (AM. L. INST. 2020). Along with Daniel Solove, I was one of the co-reporters of this project. For background on the Principles, see Solove & Schwartz, *supra* note 68, at 1259-61.

[97] JOSH LAUER, CREDITWORTHY: A HISTORY OF CONSUMER SURVEILLANCE AND FINANCIAL IDENTITY IN AMERICA 217-18 (2017).

[98] *Id.* at 217.

[99] PRIV. PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 41 (1977).

personal data stored in computerized "desk drawers," also known as servers, by going far beyond the issue of the external transmission of personal information to third parties, which is all the *TransUnion* Court cares about. In rewriting the FCRA, the *TransUnion* Court also engages in a time-travel tactic and invents a constitutional tradition that shackles data privacy law to the common law.

II. PRIVACY STANDING AND THE THREAT TO FIPS

The Supreme Court has turned standing doctrine, traditionally a vehicle for judicial restraint and deference to the legislative branch, into a means of increasing its own power. Although Justice Kagan joined the majority in *Spokeo*, she dissented in *TransUnion* with a warning that the decision "transforms standing law from a doctrine of judicial modesty into a tool of judicial aggrandizement."[100] *TransUnion* also represents the Court devising an offshoot of its fealty to originalism—in *TransUnion*, it grafts a branch on Article III that is devoted to common law privacy. In this Part, I wish first to discuss the flimsy basis for this new doctrine of faux-historical privacy standing. In this Part's final Section, I analyze this doctrine's destructive potential for data privacy law.

A. *The Invention of Common Law Privacy Standing*

Early in his *TransUnion* opinion, Justice Kavanaugh announces with a flourish, "[W]e start with the text of the Constitution."[101] But standing doctrine is entirely judge-made, and after giving an air of textualism to his analysis by quoting the two key words of Article III, "cases" and "controversies," Justice Kavanaugh's majority opinion shifts to discuss and develop the series of Supreme Court cases, all recent in vintage, that have constructed modern standing doctrine.

There is scant textualism, or, indeed, originalism in the majority opinion.[102] Mincing no words, Professor Cass Sunstein observes, "As far as constitutional law is concerned, the injury-in-fact test was made up out of whole cloth."[103] The cases on which *TransUnion* depends begin with *Lujan v. Defenders of Wildlife* (1992),[104] a case decided some 205 years after the ratification of the Constitution.[105]

TransUnion does not engage with the Founders' views regarding "injury in fact," if, indeed, evidence exists on that subject. Sunstein notes, "The approach

[100] TransUnion LLC v. Ramirez, 594 U.S. 413, 461 (2021) (Kagan, J., dissenting).

[101] *Id*. at 423 (majority opinion).

[102] Indeed, as Dean Chemerinsky has noted, an originalism approach to Article III standing is itself problematic. For one thing, an originalistic view of Article III would not appear to permit judicial review. ERWIN CHERMINSKY, WORSE THAN NOTHING: THE DANGEROUS FALLACY OF ORIGINALISM 76 (2022).

[103] Cass R. Sunstein, *Injury in Fact, Transformed*, 2021 SUP. CT. REV. 349, 349 (2021).

[104] 504 U.S. 555 (1992).

[105] *See TransUnion*, 594 U.S. at 423; *see also Lujan*, 504 U.S. at 555.

in *TransUnion* is a concoction. The Court has invented a tradition."[106] The majority is not really interested in originalism, however, but merely waves its hand in direction of the importance of "history and tradition." Rather, it is Justice Thomas, in dissent, who discusses originalism, and argues that allowing recovery for the full class in *TransUnion* and on all their claims would be consistent with the law at the time of the Founding as well as the Framer's vision.

For Justice Thomas, the key to understanding the scope of judicial power is whether or not an individual asserts her own rights. He argues, "At the time of the founding, whether a court possessed judicial power over an action with no showing of actual damages depended on whether the plaintiff sought to enforce a right held privately by an individual or a duty owed broadly to the community."[107] If an individual sought to sue someone for a violation of personal rights, "the plaintiff needed only to allege the violation."[108] If the lawsuit was based on "the violation of a duty owed broadly to the whole community, such as the overgrazing of public lands," the plaintiff needed to show damages.[109] Hence, "[t]he First Congress enacted a law defining copyrights and gave copyright holders the right to sue . . . even if the holder 'could not show monetary loss.'"[110]

In *TransUnion*, each class member had established a violation of private rights as established by the FCRA and that statute protected these interests with a private right of action. For Justice Thomas, that ended the question of whether or not the plaintiffs had "a sufficient injury to sue in federal court."[111] But the invented tradition in *TransUnion* is that privacy harms grounded in federal statutes must relate, somehow, to something in the law, somewhere, that conveys an impression of age. That something proves to be "reputational harms, disclosure of private information, and intrusion upon seclusion."[112]

The *TransUnion* Court focuses on the first of these three categories, which is that of the legal protection against defamation. This tort interest is indeed anchored in the traditional common law; the defamation tort goes back to pre-Norman times in England.[113] In the United States, the Restatement (Second) of Torts adopted it in its section 558.[114] As Jonathan Weinberg has shown, however, the defamation tort proved inadequate to stop invasions of privacy and related harm to individuals at the birth of credit reporting during the nineteenth

[106] Sunstein, *supra* note 103, at 369.

[107] *TransUnion*, 594 U.S. at 446-47 (Thomas, J., dissenting).

[108] *Id.* at 447.

[109] *Id.* (citing Spokeo, Inc. v. Robins, 578 U.S. 330, 346 (2016) (Thomas, J., concurring)).

[110] *Id.* (quoting Muransky v. Godiva Chocolatier, Inc., 979 F.3d 917, 972 (11th Cir. 2020) (Jordan, J., dissenting)).

[111] *Id.* at 450.

[112] *Id.* at 425 (majority opinion).

[113] SOLOVE & SCHWARTZ, *supra* note 67, at 165.

[114] RESTATEMENT (SECOND) OF TORTS § 558 (AM. L. INST. 1977).

century.[115] In his conclusion, the "defamation case law of the period . . . didn't meaningfully address the privacy challenges the credit bureaus posed."[116]

Hence, the *TransUnion* Court was, at best, turning to a potential remedy for a digital age problem that already had a failed track record during the analogue era. Moreover, the *TransUnion* Court did not discuss the next two items on its list, the tort protections against disclosure of private information and intrusion upon seclusion, nor the origins of these interests. These two torts represent highly successful jurisprudential contributions from Berkeley Law's Dean William Prosser, and their path into widespread adoption is a success story of which most law professors can only dream.[117] Their entry into the common law is also relatively recent.

Beginning with his Cooley Lecture at Michigan (1953), continuing with a little studied paper published in German in a German law review (1956), and reaching a high point with his much-cited article in the *California Law Review*, *Privacy* (1960), Prosser developed four additions to existing common law protections for privacy.[118] Then as reporter of the American Law Institute's Restatement (Second) of Torts (1977), Prosser introduced these new torts into the mainstream.[119] From there, and over the next decades, state legislatures and courts in all fifty states adopted at least one of the four Prosser torts. This process was a gradual one; for example, Minnesota did not accept any of these torts until 1998 and the decision of its Supreme Court in *Lake v. Wal-Mart Stores, Inc*.[120]

There is also an alternative route for torts privacy than the Prosser approach. As Jessica Lake shows in her pathbreaking book, *The Face That Launched a Thousand Lawsuits*, the "right to privacy" before Prosser had developed "primarily in response to complaints by women about the unauthorized publication of their photographic portraits."[121] Lake interprets this caselaw as demonstrating that "a right to privacy is best understood as part of women's broader political struggle for citizenship rights at the turn of the twentieth century."[122] Lake's scholarship allows us to connect privacy to contemporary

---

[115] Jonathan Weinberg, *"Know Everything That Can Be Known About Everybody": The Birth of the Credit Report*, 63 VILL. L. REV. 431, 467 (2018).

[116] *Id.* at 475.

[117] Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's* Privacy *and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CALIF. L. REV. 1925, 1926 (2010).

[118] *Id*. at 1937.

[119] *Id*.

[120] 582 N.W.2d 231 (Minn. 1998).

[121] JESSICA LAKE, THE FACE THAT LAUNCHED A THOUSAND LAWSUITS: THE AMERICAN WOMEN WHO FORGED A RIGHT TO PRIVACY 225 (2016)

[122] *Id.* at 226.

issues of personal autonomy—issues more pertinent than ever in the age of government digital surveillance and data capitalism.[123]

Ignoring this alternate route, the *TransUnion* Court focused on the Prosser torts. Yet, in his work, Prosser did not engage with the issue of computers processing personal information, a matter that was on the horizon during the period of his herculean endeavors regarding the privacy torts. The pioneers in this regard on this side of the Atlantic were Arthur Miller and Alan Westin.[124] In Europe, Spiros Simitis played a critical role in developing data privacy law, including overseeing the enactment of a pathbreaking data protection statute in 1970 in the German state of Hesse.[125] Like the law in Hesse, the FCRA was intended as a response to the processing of personal data through computers. As for Prosser and the critical Restatement sections creating the four privacy torts, they do not make a single mention of computers, digitization, or data processing.[126]

The critical question, and one that the *TransUnion* Court does not acknowledge, is why the Constitution's Article III should be interpreted as favoring defamation and the Prosser torts over congressional enactments to protect privacy. On the one hand, we have Congress enacting FIPs to protect individuals against the risks of industrial processing of personal data. On the other, we have the states, both through legislation and judicial decisions, adopting the Prosser privacy torts. Yet, these civil law remedies, which were not conceptualized as a response to the emerging information society, are ill-suited as a response to the kinds of problems following from digitization of personal data. Here, one need only to point to the chorus of scholars who have made precisely this point about the shortcomings of Prosser's privacy handiwork.[127]

---

[123] Danielle Citron has called for an updating of Prosser's torts taxonomy to better protect individuals from modern threats to privacy. *See generally* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805 (2010).

[124] *See generally* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

[125] On the development of this pathbreaking law in Hesse, see Spiros Simitis, *Privacy—An Endless Debate?*, 98 CALIF. L. REV. 1989, 1995-96 (2010). For a history of the development of privacy in Germany at that time, see LARRY FROHMAN, THE POLITICS OF PERSONAL INFORMATION: SURVEILLANCE, PRIVACY, AND POWER IN WEST GERMANY 177-94 (2021). For an account from that period looking at European developments, see FRITS W. HONDIUS, EMERGING DATA PROTECTION IN EUROPE (1975).

[126] *See* RESTATEMENT (SECOND) OF TORTS §§ 652B-652E (AM. L. INST. 1977).

[127] *See* Citron, *supra* note 123, at 1809 (detailing how "privacy tort law is ill-suited to address" modern challenges due to technologies, such as "today's databases"); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1918 (2010) ("[Privacy torts] have not adapted to new privacy problems such as the extensive collection, use, and disclosure of personal information by businesses."); Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 777-78 (noting limitation of common

While *TransUnion* is not anchored in an originalism concerned with the Founder's view from 1787, it does more generally rely on "history and tradition" in deciding Congress's power to create rights. This reliance on venerable privacy common law concepts is a smokescreen to increase the Court's own power at the cost of Congress's ability to protect data privacy. Our guide here can be Professor Cass Sunstein.

In a careful exegesis, Professor Sunstein explores the history of the idea of "injury in fact" in federal standing law, which he terms "a truly astonishing tale."[128] Sunstein demonstrates that the Court is engaging in a sleight of hand to shift standing principles to "traditional private rights."[129] *TransUnion* and the standing cases that lead up to it represent "an effort to use common-law baselines in such a way as to strike down actions by the democratic branches of government, and thus to limit the reach of regulatory enactments."[130] Sunstein also points out, with emphasis in the original, that "one thing is clear: *in the most important cases in which the injury-in-fact test is causing problems for standing, the plaintiffs are typically the beneficiaries of regulatory protection*."[131] He notes that these disfavored litigants might be consumers, as in *TransUnion*, but, in other cases, were civil rights organizations, poor people, or environmentalists.[132]

Now we come to the question of why information privacy rights are among the interests that the Supreme Court disfavors through recourse to common-law baselines. Leaving the Supreme Court's hallowed courtroom in Washington, D.C., we can consider the pomp and circumstances in Westminster Abbey on May 6, 2023 for the coronation of King Charles III. In the *New York Review of Books*, Fintan O'Toole called the coronation ceremony "a charade of historic continuity" that actually was, in large part, based on "a series of relatively recent inventions."[133] Most of the ceremony itself had been made up at the start of the twentieth century, and most examples of "royal bling" on hand were mere replicas for originals destroyed during the English Revolution.[134] But the intention was to depict historical continuity going back to medieval times.

O'Toole's characterization of the coronation of King Charles III tracks earlier scholarship by David Cannadine and Eric Hobsbawm, two famous historians, about "invented traditions" in European history.[135] For Cannadine, the reign of

law privacy torts that "eliminate their usefulness in responding to violations of privacy in cyberspace").

[128] Sunstein, *supra* note 103, at 349.

[129] *Id*. at 351.

[130] *Id*. at 371.

[131] *Id*. at 370.

[132] *Id*.

[133] Fintan O'Toole, *Golden Coats, Sacred Spoons*, N.Y. REV. BOOKS (May 7, 2023), https://www.nybooks.com/online/2023/05/07/golden-coats-sacred-spoons-coronation/.

[134] *Id*.

[135] *See* THE INVENTION OF TRADITION (Eric Hobsbawm & Terence Ranger eds., 2014).

Queen Victoria marked an early heyday of invented tradition.[136] Fast-forwarding then to the reign of Queen Elizabeth II, Cannadine noted how "the slide into impotence" of the United Kingdom as a great power was accompanied by an increase in "the ritual of monarchy."[137] The goal was to provide "an impression of stability."[138] Hobsbawn agrees with Cannadine that periods of rapid change invite the invention of new traditions.[139] Finally, and similarly, O'Toole finds that British royal ceremonies and their faux-ancient aspects have increased as British power declined throughout the Twentieth Century.[140]

This shared analysis points to two important differences between the Supreme Court and the Royal Family regarding the invention of traditions. First, when it comes to information privacy, the statutory landscape at present is not one of rapid change. The attempt to enact a federal privacy statute is stalled, and the Court's assault on the FCRA takes aim at a law that has been in place since 1970. Hence, the disfavoring of data privacy legislation must be driven by something else. As a general matter, and as Sunstein puts it, the Supreme Court's standing jurisprudence reveals its antipathy towards the beneficiaries of regulatory protection. In the cases of *Spokeo and TransUnion*, moreover, litigants had claims that threatened corporate profits and practices.

Second, and in contrast to the British monarchy and the British Empire, the Supreme Court does not present a study in declining power. The U.S. Supreme Court's new conservative super-majority has been doing quite well for itself. *TransUnion* generates a faux-historical tradition around data privacy in order to displace Congressional lawmaking. By devising a supposed tradition resting on common law privacy, the conservate super-majority on the Court continues its project of altering precedent to increase its own power.

B. *The Risk to Data Privacy Law*

TransUnion raises a considerable threat to American privacy law and its safeguarding of individuals. As noted, it endangers a variety of FIPs, which are in place to protect individuals from the dangers of digitization of personal data. In this section, we successively explore the concept of "formatting errors"; the protection by *TransUnion* of data processing companies at the cost of consumers; and recent developments in lower court cases regarding privacy standing. Turning then to the future, we consider two final topics. These concern the threat by *TransUnion* to a range of data privacy statutes and the propensity

---

[136] David Cannadine, *The Context, Performance and Meaning of Ritual: The British Monarchy and the 'Invention of Tradition', c. 1820-1977*, *in* THE INVENTION OF TRADITION, *supra* note 135, at 101, 108.

[137] *Id*. at 157.

[138] *Id.*

[139] Eric Hobsbawm, *Mass-Producing Traditions: Europe, 1870-1914*, *in* THE INVENTION OF TRADITION, *supra* note 135, at 263, 263.

[140] O'Toole, *supra* note 133.

of the Supreme Court super-majority to modify doctrine and bend facts on behalf of favored litigants.

1. "Formatting Errors"

The *TransUnion* Court trivializes the failure of a credit reporting agency to provide statutorily mandated information to its users. It does so by characterizing these shortcomings as "formatting errors." As the Court explains, TransUnion did not send the plaintiffs correct copies of their credit files, as required by the FCRA.[141] The mandated disclosure would have informed them of their presence on the OFAC list. The Court then immediately notes that TransUnion did send this information in its second mailing to the plaintiffs.[142] Additionally, TransUnion failed to include a summary of rights in this second mailing to plaintiffs, as required by law, although it did include it in the first one.[143] Both failures, as the Court concedes, deprived the plaintiffs "of their right to receive information" in order to "protect consumers' interests in learning of any inaccuracies in their credit files so that they can promptly correct the files before they are disseminated to third parties."[144]

Yet, these statutory harms were deemed insufficient for constitutional purposes. These mistakes were not considered to be "concrete" harms. In *TransUnion*, the Supreme Court revisited the results of long-ago legislative bargaining, and ones that had survived subsequent amendments to the FCRA. It did so in order to rewrite this statute. As Daniel Solove and Danielle Citron observe, the Supreme Court in *TransUnion* took a pen to a statute to excise parts that it disliked.[145]

The Court may not favor the interests that the FCRA protects and the private right of actions that it provides, but Congress made its own decision in this regard. Congress had engaged in lengthy negotiations to arrive at the final form of this statute. For example, the FCRA encourages private enforcement of the law to ease the burden on regulators.[146] At the time of the FCRA's enactment, the private right of action in this statute "was included as a trade in exchange for severely limiting state privacy and defamation claims."[147] Reflecting legislative bargaining during its enactment, the FCRA provides partial immunity for credit reporting agencies from lawsuits in state courts based on defamation and invasion of privacy claims.[148]

[141] TransUnion LLC v. Ramirez, 594 U.S. 413, 417 (2021).

[142] *Id*. at 420.

[143] *Id*.

[144] *Id*. at 440.

[145] Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez, 101 B.U. L. REV. ONLINE 62, 70 (2021).

[146] *Id*.

[147] *Id*.

[148] 15 U.S.C. § 1681h(e).

2. Favoring Credit Reporting Agencies

TransUnion disfavors the interests of consumers and favors the interests of credit reporting agencies engaged in the widespread collection and commodification of personal data. Credit reporting companies, like TransUnion, exist to sell information to businesses, such as the Nissan dealership in Dublin, California, which is where the incident that led to the *TransUnion* litigation occurred.[149] The Nissan dealer had accessed Sergio Ramirez's information from TransUnion when he sought to purchase an automobile. Once it discovered that Ramirez was on the OFAC terrorist list, it refused to allow him to carry out this transaction.[150]

Individuals such as Ramirez are not the clients of credit reporting agencies, but their product. The raw material for these businesses is the personal information of consumers, who, to the extent that they have complaints and requests for service, represent only a drain on profits. Hence, the FCRA seeks, as a counterweight, to mandate that this information be accurate, and that consumers receive information about these entities' practices and are able to correct false data held by credit reporting agencies.

Despite the FCRA's statutory protections, credit reporting agencies are notorious for the inaccuracies in their databases and their lack of responsiveness to individual parties. The *TransUnion* litigation followed an earlier Third Circuit case, *Cortez v. TransUnion, LLC*,[151] which concerned similar practices around the OFAC database and led to a $100,000 award to the injured party.[152] The Third Circuit characterized the shortcomings of TransUnion's data practices as "reprehensible."[153]

More recently, TransUnion settled with the Federal Trade Commission and the Consumer Financial Protection Board for $23 million for its reporting of inaccurate eviction records when supplying records for tenant screening.[154] In another recent action, the Consumer Financial Protection Bureau ordered TransUnion to pay "$8 million for lying to consumers" about the status of their requested credit freezes as well as about their requests to lift the freezes on a temporary basis when they applied for credit.[155] The assessed total includes a $5 million dollar penalty and $3 million in consumer compensation.

---

[149] *TransUnion*, 594 U.S. at 420.

[150] *Id.*

[151] 617 F.3d 688 (3d Cir. 2010).

[152] *Id.* at 695-96.

[153] *Id.* at 723.

[154] *FTC and CFPB Settlement to Require Trans Union to Pay $15 Million over Charges It Failed to Ensure Accuracy of Tenant Screening Reports*, FTC (Oct. 12, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-cfpb-settlement-require-trans-union-pay-15-million-over-charges-it-failed-ensure-accuracy-tenant [https://perma.cc/7SYN-7YQN].

[155] *CFPB and FTC Take Actions Against TransUnion for Illegal Rental Background Check and Credit Reporting Practices*, CONSUMER FIN. PROT. BUREAU (Oct. 12, 2023),

Other credit reporting agencies have been the source of privacy investigations and lawsuits. Like TransUnion, Equifax is one of the largest credit reporting agencies. It suffered a massive data breach in 2017 involving some 147 million people in the United States. This Equifax breach led to a large class action settlement in January 2020, which included $425 million in monetary and injunctive relief.[156]

The Supreme Court's decision in *TransUnion*, while stripping statutory protections from individuals, leaves businesses well protected for shortcomings in the accuracy of credit reports and in their procedures. As Justice Thomas points out in his *TransUnion* dissent, a business—such as the Nissan dealership in Dublin—that purchases an "OFAC Name Screen Alert" would suffer a "monetary harm" if it did not receive a report for which it had contracted.[157] Such a loss would represent a concrete, financial injury, and the business would have standing to bring a claim against TransUnion. But when class members do not receive statutorily-mandated information about an OFAC report being part of their credit report, there was inadequate harm to them for standing purposes.

3. Post-*TransUnion* Caselaw: An Uncertain Landscape

Regarding the evidence, some courts have used *TransUnion* to stop lawsuits on standing grounds. An example of such a decision is *I.C. v. Zynga, Inc.*,[158] an opinion from the Northern District of California. In contrast, *Bohnak v. Marsh & McLennan Cos.*,[159] a judgment from the Southern District of New York, took a different approach to evaluating the reach of the privacy tort of intrusion upon seclusion.[160]

In *Zynga*, Judge Rogers decided that social game players, whose personal information was allegedly hacked during a data breach, lacked standing due to their failure to allege an injury in fact. Among their claims regarding standing, the *Zynga* plaintiffs alleged "invasions of privacy bearing a close relationship to harms caused by the common law private torts of disclosure of private facts and intrusion upon seclusion."[161] These are the two Prosser torts that met with the

https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-take-actions-against-transunion-illegal-rental-background-check-and-credit-reporting-practices/ [https://perma.cc/GX36-FSG5]. For a media report, see Ann Carrns, *TransUnion Failed to Quickly Place or Remove Freezes on Credit Reports*, N.Y. TIMES (Oct. 28, 2023), https://www.nytimes.com/2023/10/27/your-money/transunion-credit-report-freezes-cfpb.html.

[156] *Equifax Data Breach Settlement*, FTC, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement [https://perma.cc/S244-3TB7] (last visited Oct. 9, 2024).

[157] *TransUnion*, 594 U.S. 413, 455-56 (2021).

[158] 600 F. Supp. 3d 1034, 1055 (N.D. Cal. 2022).

[159] 580 F. Supp. 3d 21 (S.D.N.Y. 2022).

[160] *Id.* at 29.

[161] *Zynga*, 600 F. Supp. 3d at 1048. In contrast, the court in *James v. Walt Disney Co.*, 701 F. Supp. 3d 942 (N.D. Cal. 2023), distinguished *Zynga* as a data breach case, and found that

approval of the *TransUnion* Court. But for Judge Rogers, the information leaked in the data breach did not meet the requirement of these torts for a "highly offensive" action.[162] As the district court concluded, it "does not view the collection of email addresses, phone numbers, Zynga usernames, Zynga passwords, and Facebook usernames as so private that their revelation would be highly offensive to a reasonable person."[163] As a result, the alleged privacy injuries were not sufficiently concrete to provide a basis for Article III standing.

This result can be contrasted with the district court's holding in *Bohnak* as well as the Second Circuit's treatment of this case on appeal. For the Southern District of New York, Judge Hellerstein evaluated the claims of employees of a company for alleged injuries arising from a data breach compromising their personal information. For our purposes, the most important part of this opinion concerns Judge Hellerstein's decision that "the exposure to the risk of identity theft causes concrete injury," which meant that the plaintiffs had Article III standing.[164] Judge Hellerstein stated, "I find that the data breach's exposure of Plaintiff's [personally identifiable information] causes a separate concrete harm, analogous to that associated with the common-law tort of public disclosure of private information."[165]

Where Judge Rogers had evaluated whether or not a "highly offensive" action had taken place, which the literal language of the Prosser torts requires, Judge Hellerstein was willing to accept less. In his assessment, a data breach exposing personal information "to third parties without authorization or consent could plausibly be offensive to a reasonable person."[166] Thus, an initial open question, as illustrated by *Zynga* and *Bohnak*, is just how close an alleged injury has to be to the privacy torts. Both district court judges had cited *TransUnion* to the effect that a concrete harm need only bear a "close relationship" to a traditionally recognized harm, and need not possess all "elements for a common law analogue" in order to secure standing.[167]

Hence, one issue is whether courts should use the test of "highly offensive," or merely that of "offensiveness." Note, as well, that these cases differ as to whether the offensiveness of a privacy invasion should be assessed based on *the sensitivity of the data* released, with the disclosure of only certain sensitive data being offensive (*Zynga*), or according to *the offensiveness of the act of releasing*

the privacy issue in the instant case concerned an individual's control of information relating to her person. *Id.* at 951.

[162] *Zynga*, 600 F. Supp. 3d at 1048-49.

[163] *Id.* at 1049.

[164] *Bohnak*, 580 F. Supp. 3d at 27.

[165] *Id.* at 29.

[166] *Id.* at 30. Note that while Judge Hellerstein dismissed Bohnak's claims for damages, the Second Circuit reversed this part of the opinion and found that Bohnak's alleged injury from an increased risk of harm could support a claim for damages. Bohnak v. Marsh & McLennan Cos., 79 F.4th 276, 290 (2d Cir. 2023).

[167] *Zynga*, 600 F. Supp. 3d at 1048-49; *see Bohnak*, 580 F. Supp. 3d at 27.

the data (*Bohnak)*. In *Bohnak*, the Second Circuit, like the district court in this case, came down firmly in favor of considering the nature of the release and not merely the degree of sensitivity of the personal data. It stated, "the core injury here—exposure of Bohnak's private [personally identifing information] to unauthorized third parties—bears some relationship to a well-established common-law analog: public disclosure of private facts."[168]

4. The Threat to Data Privacy Law

In the uncertain landscape following *TransUnion*, it is important to assess which aspects of data privacy laws are most endangered. In his analysis of this case, Dean Chemerinsky presents a long list of federal laws where lower courts have permitted standing based solely on the violation of rights created by statute.[169] Such standing is permitted even where no common-law or historical analogue of such rights exists.[170] To this catalogue, we can add the impact of this case on federal data privacy statutes that contain a private right of action.

The plaintiffs in *Spokeo* and *TransUnion* brought their lawsuits pursuant to a statutory grant in the FCRA; those in *Clapper* drew on a similar provision in FISA. In addition to those two laws, other statutes with private rights of actions include the Cable Communications Policy Act, the Drivers Privacy Protection Act, the Telephone Consumer Protection Act, and the Video Privacy Protection Act (VPPA).[171] Protection of FIPs in these statutes is now endangered by the future vagaries of how federal courts evaluate the relationship of these statutes to defamation, intrusion upon seclusion, and the public disclosure of private facts. Yet, numerous provisions in these laws do not relate to these torts. Like many data privacy laws, the VPPA requires the destruction of personal information.[172] The requirement for data destruction in the VPPA is that it be carried out "as soon as practicable."[173] Under one reading of *TransUnion*, however, this provision should not be enforced without a showing of harm.

This example is far from hypothetical. Post-*Spokeo* and pre-*TransUnion*, the Eighth Circuit dismissed a claim under the Cable Communications Act based on a cable provider illegally retaining personal information.[174] While this action violated the Cable Communications Act, a statute dating to 1984, the Eighth Circuit found in *Braitberg v. Charter Communications, Inc.* that the failure to destroy personal information was not an interest for which Congress could authorize suit. The appellate court stated, "the retention of information lawfully

[168] *Bohnak*, 79 F.4th at 285.

[169] Erwin Chemerinsky, *What's Standing After* TransUnion LLC v. Ramirez, 96 N.Y.U. L. REV. ONLINE 269, 285-86 (2021).

[170] *Id.* at 286.

[171] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 169-70 (7th ed., 2024).

[172] Video Privacy Protection Act, 18 U.S.C. § 2710(e).

[173] *Id.*

[174] Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925 930-31 (8th Cir. 2016).

obtained, without further disclosure, traditionally has not provided the basis for a lawsuit in American courts."[175]

Another VPPA example concerns a 2012 amendment to it, which has been termed "the Netflix Amendment."[176] This provision allows individuals to more easily consent to sharing information about their watching of audio-visual materials. But the law also polices the terms of this consent to make sure it is a meaningful expression of the individual's wishes. Consent is to be collected "in a form, distinct and separate from any form setting forth other legal or financial obligations of the consumer."[177] Consent also must be withdrawable at any time, or on a case-by-case basis.

Yet, again, a company's failure to follow these requirements will not track the kinds of harms that defamation or the privacy torts seek to stop. Much content disclosed illegally will presumably neither be reputation ruining (as defamation requires) nor offensive or highly offensive (as the two privacy torts require). Thorough its narrowing of Article III standing, the Supreme Court permits dismissal of some privacy cases and reduces the size of other privacy class-action lawsuits. The consequence will be to encourage businesses to underinvest in privacy compliance.

A final uncertainty as it affects data privacy law concerns the right to access information about oneself. This FIP is an absolute mainstay of data privacy legislation. It is also included in all international expressions of FIPs, such as that of the Organisation of Economic Cooperation and Development's from 1980 and Convention 108 of the Council of Europe from 1981.[178] And, of course, it is found in the FCRA. In *TransUnion*, the majority opinion distinguishes between the FCRA and established "informational injury" law[179] According to the Court, TransUnion's shortcomings only involved plaintiffs receiving information "in the wrong format" and not a failure to provide the information altogether.[180] As this Essay has pointed out, the idea of the "formatting error" is a made-up concept from the *TransUnion* majority. This language minimizes failures by a credit reporting agency to follow established FIPs that Congress had enacted into law.

At the same time, the *TransUnion* Court briefly did assert the continuing validity of its precedents upholding the public's right to receive information under Freedom of Information statutes or Sunshine laws.[181] It also mentioned with approval its established caselaw finding standing for "testers" checking on fair housing laws. Yet, the validity of the tester precedent is far from certain.

---

[175] *Id*. at 930.

[176] *See* § 2710(b).

[177] § 2710(b)(2)(B)(i).

[178] OECD, *supra* note 95, § 13; Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, art. 8, Jan. 28, 1981, E.T.S. No. 108.

[179] TransUnion LLC v. Ramirez, 594 U.S. 413, 442 (2021).

[180] *Id* at 441 (emphasis omitted).

[181] *Id*.

There is a circuit split regarding the informational interests of testers under the American with Disabilities Act ("ADA").[182] This issue will have significant spillover implications for data privacy legislation, but, for the time being, questions about standing under this federal law remain open. There has also been a recent development in this regard.

After hearing argument in *Acheson Hotels, LLC v. Laufer*[183] on October 4, 2023, the Supreme Court dismissed the litigation as moot on December 5, 2023.[184] *Acheson* involved a right to receive information, which, as we have seen, is also a matter that came up in *TransUnion* regarding Ramirez's right to be given certain kinds of data about the practices of a credit reporting agency. In *Acheson*, the issue was whether a "tester" of provisions of the ADA had Article III standing to contest a hotel's failure to provide mandated disability accessibility information on its website, even if she lacked any intention of visiting that place of public accommodation.[185] Due to the unusual procedural posture of the *Acheson* litigation, however, the Supreme Court ultimately dismissed the case. It did so by citing the plaintiff's words, "mootness is easy and standing is hard."[186] If future litigation in this area weaponizes constitutional standing to weaken statutory rights to receive information under the ADA or other laws, it will also have negative implications for this aspect of data privacy statutes.

5. Calvinball

A final result of the *Spokeo* and *TransUnion* decisions has been to increase the power of federal courts to pick and choose among the parties seeking judicial redress. Fans of the legendary comic strip, "Calvin and Hobbes," will recall the game of Calvinball. In it, the players make up rules as they go. A classic Calvinball tournament involves, for example, scoring points by using a croquet mallet to hit badminton birdies against a tree.

There is more than a hint of Calvinball in the Supreme Court's approach to standing. From the majority's perspective, the glorious result is being able select certain litigants to be favored and others to be shunted to the side. As we have seen, *Spokeo* and *TransUnion* do not look to full-blown originalism, but merely "history and traditions" in the common law of privacy, including recent developments, namely, the Prosser torts, that are conveniently grandfathered into this story. That is the chosen methodology for deciding on concrete harms. But in an opinion decided the same term as *TransUnion*, the Supreme Court decided that originalism was the proper methodology for deciding redressability, which is the third prong of standing.[187]

[182] Acheson Hotels, LLC v. Laufer, 601 U.S. 1, 3 (2023).

[183] *Id.* at 1.

[184] *Id.*

[185] *Id*. at 3.

[186] *Id*. at 4.

[187] Uzuegbunam v. Preczewski, 592 U.S. 279, 298 (2021).

An eight-one opinion, *Uzuegbunam v. Preczewski*,[188] sees Justice Thomas, on behalf of the majority, analyzing decisions of "courts at common law," including English precedents from the seventeenth century, before declaring that this approach to redressability "was followed both before and after ratification of the Constitution."[189] The holding of *Uzuegbunam* regarding redressability as an element of standing is that nominal damages, awarded by courts or expressed in a statute, will be sufficient—even in the absence of actual harm.[190] At no time has the Supreme Court explained why one methodology is appropriate for the third prong of standing, redressability, but another one for evaluating the first prong. It lacks any sorting concept or meta-principle in this regard.

Rather, as in Calvinball, the Supreme Court is making it up as it goes long. All of which is not to say, however, that the Supreme Court is entirely without guardrails in its standing jurisprudence. For example, consider *Food and Drug Administration v. Alliance for Hippocratic Medicine*.[191] The case concerned a challenge to a revision of the policies of the Food and Drug Administration ("FDA") towards mifespristone, an abortion drug. The new FDA regulation relaxed the existing requirements for this pharmaceutical by making it "easier for doctors to prescribe and pregnant women to obtain" the drug.[192] Plaintiffs in the case were pro-life medical associations and physicians. In a unanimous decision, the Supreme Court declared, "Under Article III of the Constitution, a plaintiff's desire to make a drug less available *for others* does not establish standing to sue."[193] In particular, the Court found problems in the causation requirement for standing.[194]

The conservative super-majority that overturned *Roe v. Wade*[195] in *Dobbs v. Jackson Women's Health Organization*[196] had demonstrated that it is no fan of reproductive freedom. Nonetheless, the claims of the plaintiffs in *Alliance for Hippocratic Medicine* were too flimsy for it. Among the problems were that "the plaintiff doctors and medical associations do not prescribe or use mifepristone."[197] Moreover, the "FDA has not required the plaintiffs to do anything or to refrain from doing anything."[198]

---

[188] *Id.* at 281.

[189] *Id*. at 285-87.

[190] *Id*. at 292.

[191] 602 U.S. 367 (2024).

[192] *Id.* at 373.

[193] *Id.* at 374.

[194] *Id.* at 382-83.

[195] 410 U.S. 113 (1973), *overruled by* Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

[196] *Dobbs*, 597 U.S. at 215.

[197] *All. for Hippocratic Med.*, 602 U.S. at 385.

[198] *Id.* An essay in the Journal of the American Medical Association advises that this opinion is to be "read with caution" and warns against threats involving "future strategies to attack science, undermine FDA authority, and constrain abortion rights." Michele B.

The result of Calvinball for standing has been to permit considerable leeway for lower courts to go one way or another. The malleability of the Supreme Court's opinions in this area is well illustrated by the issue of future harm as a basis for standing. This topic is one that looms large in data breach cases. In *TransUnion*, the Supreme Court stated that a risk of future harm "cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm."[199] It then raised the possibility, in a footnote, 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."[200] The *TransUnion* Court then observed, "We take no position on whether or how such an emotional or psychological harm could suffice for Article III purposes—for example, by analogy to the tort of intentional infliction of emotional distress."[201] It concluded by noting that the plaintiffs before it, at any rate, had not raised such a theory of Article III injury.[202]

The result has been considerable uncertainty regarding standing in data breach cases. Consider, first, a sample of recent cases that did *not* find standing. *In re Practicefirst Data Breach Litigation*[203] involved a judgment that in the data breach context, as for the common-law privacy tort, there must be willful disclosure and publication of a plaintiff's confidential information.[204] These

Goodwin, Allison M. Whelan & Lawrence O. Gostin, Food and Drug Administration v. Alliance for Hippocratic Medicine—*A Cautious Win for Reproductive Health Care and FDA Authority*, 332 JAMA 453, 454 (2024).

Murthy v. Missouri, 144 S. Ct. 1972 (2024), provides another example of a potentially favored set of plaintiffs, whose claims the Supreme Court nonetheless rejected. *Id.* at 1981. In contrast to the unanimous decision in *Food and Drug Administration v. Alliance for Hippocratic Medicine*, *Murthy* was a six-three decision with the most conservative Justices dissenting and ready to find standing. *Id.* at 1997 (Alito, J., dissenting). In *Murthy*, two states and five social-media users sued Executive Branch officials and agencies. *Id.* at 1983 (majority opinion). Their contention was that the Biden administration had pressured the platforms to censor their speech, which was deemed to contain false or misleading information about the COVID pandemic. In an opinion by Justice Barrett, the majority found the plaintiffs fell short due to a "lack of specific causation findings" and a lack of proof of "a substantial risk of future injury." *Id*. at 1987, 1993. In contrast, Justice Alito, joined by Justice Thomas and Justice Gorsuch, dissented and argued that "top federal officials" in the Biden administration "continuously and persistently hectored Facebook to crack down on what the officials saw as unhelpful social media posts." *Id.* at 2004 (Alito, J., dissenting). The dissenters found Article III standing for the plaintiffs and argued that Article III standing "is cheapened when the rules are not evenhandedly applied." *Id.* at 2009.

[199] TransUnion LLC v. Ramirez, 594 U.S. 413, 436 (2021).

[200] *Id*. at 436 n.7.

[201] *Id.*

[202] *Id*.

[203] No. 121CV00790, 2022 WL 354544 (W.D.N.Y. 2022).

[204] *See id.* at *6-7.

conditions will not be met in most cases involving an unauthorized data breach. The defendant will not have willfully disclosed information; rather, this entity will have been hacked by a third party. As a further example, in *Kim v. McDonalds USA, LLC*,[205] the district court found that a threat of future harm alone cannot satisfy Article III standing, including for a plaintiff who, post-data breach, received a phishing email that threatened to release his information.[206] Finally, in *C.C. v. Med-Data Inc*.,[207] the district court dismissed a case involving a breach of "highly sensitive data" despite the plaintiff's introduction of research and reports about identity theft crimes that pointed to 19% risk of fraud for consumers receiving a data breach notification.[208] The *Med-Data* district court concluded, "[a] 19% risk isn't 'certainly impeding' harm."[209]

But there are also lower courts that have found standing and developed privacy-friendly rulings in data breach cases. For example, the Third Circuit in *Clemens v. ExecuPharm, Inc.*[210] found that:

> [I]n the data breach context, where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk . . . of identity theft causes him to presently experience emotion distress . . . .[211]

In other data breach cases, some courts found Article III standing due to a combination of the risk of future harm and a plaintiff expending resources on current protective measures.[212] Thus, out-of-pocket expenses, lost time, and other opportunity costs attempting to mitigate a data breach are "separate and concrete harms."[213] These cases may be inconsistent, however, with Supreme Court precedent, namely Justice Alito's firm admonition in *Clapper* that the

---

[205] No. 21-CV-05287, 2022 WL 4482826 (N.D. Ill. 2022).

[206] *See id.* at *5.

[207] No. 21-2301, 2022 WL 970862 (D. Kan. 2022).

[208] *See* C.C. v. Med-Data Inc., No. 21-2301-DDC-GEB, 2022 WL 970862, *7 (D. Kan. 2022).

[209] *Id.*

[210] 48 F.4th 146 (3d Cir. 2022).

[211] *Id.* at 155-56. For a similar result, see Ortiz v. Perkins & Co., No. 22-CV-03506-KAW, 2022 WL 16637993, at *4 (N.D. Cal. 2022). *See also Kim*, 2022 WL 4482826, at *6 ("[E]motional injuries [from a data breach] constitute 'quintessential abstract harms that are beyond' a court's power to remedy." (quoting Wadsworth v. Kross, Lieberman & Stone, Inc., 12 F.4th 665, 668 (7th Cir. 2021)). For a district court case distinguishing itself from *Clemens*, see *In re* Retreat Behav. Health LLC, No. 5:23-CV-00026-MRP, 2024 WL 1016368 (E.D. Pa. Mar. 7, 2024). In that case, "an unauthorized person *may* have accessed a data set including Plaintiffs' personal information" while in *Clemens*, a known hacking group "stole plaintiff's personal data, held it for ransom, and later published it for sale on the Dark Web." *Id.* at *2-3.

[212] *See* Bohnak v. Marsh & McLennan Cos., 79 F.4th 276, 286-87 (2d Cir. 2023).

[213] *Id*. For similar results, see *Clemens*, 48 F.4th at 159.

plaintiffs could not "manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."[214] Whether a data breach involves an imminent harm—as opposed to the NSA engaging in surveillance of a given set of plaintiffs—may turn on the facts of a given data security incident.[215]

We conclude by broadening our discussion of the selection of favored litigants beyond data privacy and data breach cases. As Sarah Lipton-Lubet notably put it, there are "multiple egregious examples of the Supreme Court's rewarding of artificial plaintiffs suffering invented harm."[216] One of her examples is *303 Creative LLC v. Elenis*, the case, already discussed above, involving the worries of a future designer of wedding websites. Another relevant case is *Kennedy v. Bremerton School District*.[217] These examples demonstrate "the Supreme Court's contempt for facts," a phenomenon identified by the editors of no less a media outlet than *Scientific American*.[218]

For the *Bremerton School District* majority, the plaintiff football coach was involved in "brief, quiet prayer" at work, an activity in which the school district interfered.[219] In his concurrence, Justice Alito referred to the case as involving a person acting "in a purely private capacity," when "a brief lull in his duties apparently gave him a few free moments to engage in private activities."[220] In her dissenting opinion, however, Justice Sotomayor published multiple photographs of Coach Kennedy on the football field surrounded by a large group of students, whose participation in prayer he had solicited before the game.[221] In other photos reproduced in her dissent, the media and bystanders, whom the coach had informed in advance of his plans, gather round to watch these

[214] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013).

[215] For the Eleventh Circuit, for example, the posting of breached information on the dark web did not constitute a future harm, but a "present injury." *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 890 (11th Cir. 2023). Jim Dempsey provides an invaluable up-to-date account of this evolving caselaw at his blog updating his cybersecurity law treatise, JAMES X. DEMPSEY & JOHN P. CARLIN, CYBERSECURITY LAW FUNDAMENTALS (2d ed. 2024). *See Updates and Supplemental Material to Chapter 4, Data Breach Litigation – Standing*, CYBERSECURITY L. FUNDAMENTALS, https://cybersecuritylawfundamentals.com/chapter-4 [https://perma.cc/3ZMJ-66UF] (last updated Aug. 23, 2024).

[216] Sarah Lipton-Lubet, *The Supreme Court's Conservatives Can't Stop Falling for Phony Plaintiffs*, SLATE (Oct. 3, 2023, 9:00 AM), https://slate.com/news-and-politics/2023/10/supreme-courts-conservative-plaintiffs-alito.html [https://perma.cc/2JGT-DNPX].

[217] 597 U.S. 507 (2022).

[218] *The Supreme Court's Contempt for Facts Is a Betrayal of Justice*, SCI. AM. (July 10, 2024), https://www.scientificamerican.com/article/the-supreme-courts-contempt-for-facts-is-a-betrayal-of-justice/ [https://perma.cc/9RN7-3EFT].

[219] *Bremerton Sch. Dist.*, 597 U.S. at 519.

[220] *Id.* at 545 (Alito, J., concurring).

[221] *See id.* at 549, 553, 555 (Sotomayor, J., dissenting).

ostensibly "private activities."[222] Like Chico Marx in *Duck Soup*, the *Bremerton School District* Court essentially demands, "Who you gonna believe, me or your own eyes?"[223]

CONCLUSION

Regarding the Supreme Court, Professor Noah Feldman views the "conservative constitutional revolution at the Court" as "ongoing," but as having "reached the end of its beginning."[224] For Feldman, the question is now whether the majority of the Court wishes "to upend the entire edifice of constitutional law" and to choose "a descent into doctrinal anarchy."[225] He predicts that "the conservative constitutional revolution will become an internal struggle between the extremely radical and the merely radical."[226]

A possible future internal struggle might be between Justice Thomas's originalism for privacy standing and the *TransUnion* majority's faux-historicism. Ironically enough, Justice Thomas's brand of data-privacy originalism offers the possibility for saving many FIPs. Private rights of action in data privacy laws typically will meet the bar for standing devised by Justice Thomas—they create private and not public rights consistent with his interpretation of the common law at the time of the Founding. In contrast, many FIPs will rest on uncertain terrain post-*TransUnion* as courts consider their relation to defamation, the public disclosure tort, and intrusion upon seclusion. In its caselaw regarding privacy standing, the Supreme Court invents a new tradition and requires a shift to common-law privacy baselines. The Supreme Court took this action to restrict the reach of data privacy laws, to limit the lawmaking of Congress, and to increase its own power.

[222] *See id.* at 553.

[223] DUCK SOUP (Paramount Pictures 1933).

[224] Noah Feldman, *The Court's Conservative Constitutional Revolution*, N.Y. REV. BOOKS (Oct. 5, 2023), https://www.nybooks.com/articles/2023/10/05/the-courts-conservative-constitutional-revolution-noah-feldman/.

[225] *Id*.

[226] *Id*.