




Winter 2022

## Making Privacy Injuries Concrete

Peter Ormerod

*Western Carolina University*, [pcormerod@wcu.edu](mailto:pcormerod@wcu.edu)

Follow this and additional works at: <https://scholarlycommons.law.wlu.edu/wlulr>

 Part of the [Civil Procedure Commons](#), [Constitutional Law Commons](#), [Privacy Law Commons](#), [Supreme Court of the United States Commons](#), and the [Torts Commons](#)

### Recommended Citation

Peter Ormerod, *Making Privacy Injuries Concrete*, 79 Wash. & Lee L. Rev. 101 (2022).

Available at: <https://scholarlycommons.law.wlu.edu/wlulr/vol79/iss1/4>

This Article is brought to you for free and open access by the Washington and Lee Law Review at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact [christensena@wlu.edu](mailto:christensena@wlu.edu).

# Making Privacy Injuries Concrete

Peter Ormerod\*

## *Abstract*

*In recent years, the U.S. Supreme Court has repeatedly said that the doctrine of Article III standing deprives the federal courts of jurisdiction over some lawsuits involving intangible injuries. The lower federal courts are carrying out the Supreme Court's instructions, and privacy injuries have borne the brunt of the Court's directive. This Article identifies two incoherencies in the Court's recent intangible injury decisions and builds on the work of privacy scholars to fashion a solution.*

*The first incoherency is a line-drawing problem: the Court has never explained why some intangible injuries create an Article III injury in fact while others do not. The second problem is more fundamental: the Court has never provided a justification for using counter-majoritarian constitutional standing to deprive plaintiffs of a remedy against companies engaged in abusive informational practices. These incoherencies have sparked much confusion in the lower courts and have invited curious arguments that the Constitution prohibits courts from adjudicating all but the narrowest sliver of privacy disputes.*

*To address the line-drawing and counter-majoritarian problems, this Article builds on Helen Nissenbaum's contextual*

---

\* Assistant Professor of Business Law, Western Carolina University. For helpful comments and conversations, I'm grateful to Sebastian Benthall, Deven Desai, Dissent Doe, Juliane Fries, Justin Hemmings, Matthew Kugler, Helen Nissenbaum, Jessica Silbey, Larry Trautman, and all the participants in the 2020 Privacy Law Scholars Conference and the 2020 Academy of Legal Studies in Business Annual Conference. Thanks also to Caroline Condrey, Spencer Faircloth, and Jessica Posa for essential research assistance.

*integrity framework. Contextual integrity observes that privacy is context specific and that privacy violations are the byproduct of practices that violate entrenched informational norms.*

*Constructing a legal framework based on contextual integrity solves both problems: contextual integrity provides courts with a principled way to distinguish between informational practices that are injurious and those that are not, and contextual integrity supplies courts with a persuasive justification for dismissing cases divorced from shared conceptions about abusive informational practices. The legal framework proves useful in understanding the statutes and circumstances that create justiciable privacy injuries.*

*It's too late to undo all the havoc wreaked by the Court's constitutional standing cases. This Article proposes a mechanism for cabining the doctrine's most extreme implications and provides courts with a consistent and coherent way to protect privacy.*

### *Table of Contents*

INTRODUCTION .....	103
I. ARTICLE III STANDING: PAST AND PRESENT .....	109
A. <i>A Brief History of Article III Standing</i> .....	109
B. <i>Injury in Fact and Information After Lujan</i> ...	113
II. PRIVACY'S ARTICLE III PROBLEMS .....	119
A. <i>Recent Cases</i> .....	120
1. <i>Clapper v. Amnesty International USA</i> (2013) .....	120
2. <i>Spokeo, Inc. v. Robins</i> (2016) .....	123
3. <i>TransUnion LLC v. Ramirez</i> (2021) .....	125
B. <i>Two Problems</i> .....	128
1. No Line-Drawing .....	128
2. No Justification for Upsetting Political Consensus .....	131
C. <i>Attempts at Solutions</i> .....	136
1. Risk and Anxiety .....	136
2. Objective Versus Subjective Harms .....	138
3. Public and Private Rights .....	139
4. Deference to the Legislature.....	144

III.	PRIVACY AS CONTEXTUAL INTEGRITY .....	146
	A. <i>A Contextual Integrity Primer</i> .....	146
	B. <i>Contextual Integrity’s Limits         and Shortcomings</i> .....	150
IV.	CONTEXTUAL INTEGRITY AS A LEGAL FRAMEWORK FOR ARTICLE III INJURIES .....	154
	A. <i>Constructing the Legal Framework</i> .....	154
	1. Identify the Injury .....	155
	2. Identify the Norm.....	156
	B. <i>Using the Framework</i> .....	157
	1. Authorities that Always or Usually Create an Injury in Fact .....	157
	2. Authorities that Only Occasionally Create an Injury in Fact .....	171
V.	JUSTIFICATIONS .....	176
	A. <i>Virtues and Advantages</i> .....	176
	B. <i>Responding to Objections</i> .....	178
	CONCLUSION.....	182

## INTRODUCTION

Article III of the U.S. Constitution provides that the federal judicial power extends to “Cases” and “Controversies.”<sup>1</sup> In recent decades, the Supreme Court has interpreted this simple provision to limit who can maintain a lawsuit in federal court and to what kinds of cases federal jurisdiction extends.<sup>2</sup> This doctrine, known as Article III standing, requires plaintiffs to show three things: that they have suffered an injury in fact; that the defendant caused the injury; and that the federal courts can redress it.<sup>3</sup> An injury in fact, according to the Court, is a concrete and particularized injury that is actual or imminent and not speculative or conjectural.<sup>4</sup>

---

1. See U.S. CONST. art. III, §§ 1, 2.  
2. See, e.g., *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992).  
3. *Id.*  
4. *Id.* at 560.

The Court only began using the injury in fact requirement to invalidate legislation that authorizes lawsuits in the last thirty years, and limits on suits against non-governmental actors are more recent still.<sup>5</sup> The Court's initial rationale for counter-majoritarian constitutional standing was premised on preventing judicial interference with the Executive Branch.<sup>6</sup> But over time the Court has supplemented the interference rationale with a broader justification—one premised on a cabined interpretation of the cases that the federal judicial power reaches.<sup>7</sup>

The Court's interpretation of the injury in fact requirements—of concreteness, particularity, and actuality or imminence—erects a jurisdictional barrier that a plaintiff asserting a privacy harm can only occasionally overcome.<sup>8</sup> In the past decade, privacy has fared particularly poorly in three cases at the Supreme Court.

---

5. In 1992, “the Court held that Article III required invalidation of an explicit congressional grant of standing to ‘citizens.’ The Court had not answered this question before.” Cass R. Sunstein, *What's Standing After Lujan? Of Citizen Suits, “Injuries,” and Article III*, 91 MICH. L. REV. 163, 165 (1992). “The apparently unanimous view of lower courts had been that a legislative grant of citizen standing was constitutional even without a showing of injury in fact.” *Id.* at 165 n.10; see also *infra* Part II.B.2. *But cf.* *Muskrat v. United States*, 219 U.S. 346, 358–59 (1911) (“The article does not extend the judicial power to every violation of the Constitution which may possibly take place, but to a ‘case in law or equity’ in which a right under such law is asserted in a court of justice.” (internal citation omitted)).

6. See *Lujan*, 504 U.S. at 577 (“To permit Congress to convert the undifferentiated public interest in executive officers’ compliance with the law into an ‘individual right’ vindicable in the courts is to permit Congress to transfer from the President to the courts the Chief Executive’s most important constitutional duty . . .”).

7. Cf. Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 439 (2017) (“Whereas older standing cases focused on whether the plaintiff before the court was the right plaintiff, the newer privacy-based cases are focused on, or making assumptions about, whether or not the harm caused by the defendant is the right kind of harm.”).

8. See Lexi Rubow, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007, 1008 (2014) (“Privacy law plaintiffs have encountered great difficulty in establishing standing because the abstract and context-specific nature of privacy harm does not fit well with current, rigid judicial conceptualizations of injury-in-fact.”).

In 2013's *Clapper v. Amnesty International USA*,<sup>9</sup> the Court held that plaintiffs alleging unconstitutional surveillance lacked standing because they could not prove their harm was "certainly impending."<sup>10</sup> It did not matter, the Court explained, that the plaintiffs expended time, effort, and money to avoid the surveillance, because self-inflicted mitigation costs could not "manufacture" standing.<sup>11</sup> In the years since, many lower courts have relied on *Clapper* to dismiss cases arising from data breaches, reasoning that victims cannot show a certainly impending financial injury and that their mitigation measures are irrelevant.<sup>12</sup>

In 2016's *Spokeo, Inc. v. Robins*,<sup>13</sup> the plaintiff alleged that the defendant's website disseminated a host of falsehoods about him.<sup>14</sup> Despite Congress's choice to authorize the suit by statute, the Court held that the plaintiff had failed to show his injury was concrete.<sup>15</sup> The Court remanded the case and instructed the lower court to consider the falsehoods' "degree of risk" of "real harm" to the plaintiff.<sup>16</sup> In the years since, lower courts have relied on *Spokeo* to dismiss other statutorily authorized suits, reasoning that a plaintiff asserting a privacy injury must also demonstrate some additional, real-world harm.<sup>17</sup>

And in 2021's *TransUnion LLC v. Ramirez*,<sup>18</sup> the Court further limited Congress's ability to create legal rights enforceable in federal court. TransUnion, one of the three major credit-reporting companies, falsely labeled Sergio Ramirez a "potential terrorist."<sup>19</sup> The Court held that class members who had this false designation disseminated to potential employers

---

9. 568 U.S. 398 (2013).

10. *Id.* at 410.

11. *Id.* at 416.

12. *See, e.g.,* *McMorris v. Carlos Lopez & Assocs.*, 995 F.3d 295, 303–05 (2d Cir. 2021).

13. 578 U.S. 330 (2016).

14. *Id.* at 333.

15. *Id.* at 342–43.

16. *See id.* at 341–43.

17. *See, e.g.,* *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 515 (D.C. Cir. 2016).

18. 141 S. Ct. 2190 (2021).

19. *Id.* at 2209.

and lenders did have a sufficiently concrete injury, but those who couldn't prove third-party dissemination did not.<sup>20</sup>

These three decisions create several problems that limit actionable privacy injuries. This Article focuses on two of them. First, the Supreme Court has failed to provide lower courts, litigants, legislatures, and other interested parties with a coherent way to discern which intangible injuries satisfy the injury in fact requirements and which do not.<sup>21</sup> Second, courts have failed to provide a persuasive justification for the now-routine practice of nullifying the product of political consensus.<sup>22</sup>

The first problem—the line-drawing problem—manifests in all informational-injury cases.<sup>23</sup> Most agree that some informational practices are per se injurious and therefore require nothing else from the plaintiff. For example, the Supreme Court has previously held that the unauthorized interception and dissemination of a phone conversation sufficed for Article III purposes.<sup>24</sup> But other informational practices require more; for example, the plaintiff in *Spokeo* needed to show how dissemination of false information about him threatened his real-world interests.<sup>25</sup>

Companies that routinely engage in abusive informational practices have seized on this uncertainty. For example, in various courts and cases over the past four years, Facebook has argued that courts lack jurisdiction over all privacy disputes except when the plaintiff shows that the company disseminated the plaintiff's information to third parties, without the plaintiff's terms-of-service consent, and in a way that specifically and

---

20. *Id.* at 2212–13.

21. See Elizabeth C. Pritzker, *Making the Intangible Concrete: Litigating Intangible Privacy Harms in a Post-Spokeo World*, 26 COMPETITION 1, 5–15 (2017) (explaining circuit splits on this question).

22. See Peter Ormerod, *Privacy Injuries and Article III Concreteness*, 48 FLA. ST. U. L. REV. 133, 169 (2020) [hereinafter Ormerod, *Privacy Injuries*] (“However, a court should give effect to Congress’s policy choices after concluding that the court is ill-suited for and has no justification for second-guessing the byproduct of the political process.”).

23. See Mark Bernstein, *Standing Here or There?*, 106 ILL. BAR J. 38, 40 (2018).

24. See *Bartnicki v. Vopper*, 532 U.S. 514, 525, 533 (2001).

25. See *Spokeo, Inc. v. Robins*, 578 U.S. 330, 342 (2016) (stating that it was not enough for the plaintiff to show a bare procedural violation).

individually identified the plaintiff.<sup>26</sup> It's little surprise that this interpretation immunizes Facebook from nearly every conceivable privacy harm.

The second problem—the lack of a justification for counter-majoritarian Article III standing—is more fundamental. Absent a rationale for courts' practice of substituting their judgment for the political process, legislatures and litigants lack guidance about how to make privacy harms actionable in federal court. As empty-handed legislatures consider new privacy protections, the Court's restrictive interpretation of Article III suggests that abusive informational practices are incapable of individual enforcement—meaning that only a centralized regulator can vindicate individuals' privacy interests.<sup>27</sup>

Other scholars have noted the radical implications of the Court's recent Article III jurisprudence.<sup>28</sup> But others' proposed solutions fall short of solving these two problems. This Article fills that void by proposing a solution to the line-drawing and counter-majoritarian problems. To achieve this end, it builds on

---

26. See Oral Argument at 6:20, *Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019) (No. 18-15982), <https://perma.cc/GQ66-FQJ4> (arguing that “invasion of privacy” injuries require “misuse” or disclosure to a third party); Defendant-Appellee Facebook, Inc.'s Supplemental Brief Re: *Spokeo, Inc. v. Robins* at 11, *Campbell v. Facebook, Inc.*, 951 F.3d 1106 (9th Cir. 2020) (No. 17-16873) (arguing that the dissemination of “anonymized and aggregated” data cannot constitute an injury in fact); Transcript of Oral Argument at 8, *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767 (N.D. Cal. 2019) (No. 18-md-02843-VC) (“Once you have that consent, which is plain and clear and we believe as a matter of law enforceable against the plaintiffs, a person cannot be injured in fact by the sharing of information when the person consented to that very sharing of information.”); Appellee's Brief at 21–24, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020) (arguing that plaintiffs lacked an Article III privacy injury because they didn't allege an unauthorized dissemination of personally identifiable information to third parties); Brief for Amici Curiae eBay, Inc., Facebook, Inc., Google LLC, et al. at 12–17, *TransUnion v. Ramirez*, 141 S. Ct. 972 (2021) (No. 20-297) (urging the Supreme Court to interpret Article III to broadly prohibit statutory damages in class actions).

27. See Wu, *supra* note 7, at 457–61 (explaining why an overly expansive standing inquiry is particularly problematic in the context of suits against private companies).

28. See, e.g., Bernstein, *supra* note 23, at 40.



Helen Nissenbaum's contextual integrity framework.<sup>29</sup> Briefly, contextual integrity observes that privacy interests are context specific, and it posits that privacy violations are the byproduct of practices that breach entrenched informational norms.<sup>30</sup>

Constructing a legal framework based on contextual integrity helps solve both of the problems with the Court's recent injury in fact decisions. First, informational norms—and people's expectations about injurious informational practices—supply courts with a mechanism for distinguishing between informational harms that create an Article III injury and those that do not.<sup>31</sup> Second, informational norms provide judges with a persuasive justification for dismissing cases that involve excessively abstract harms.<sup>32</sup>

The legal framework supplies answers to the question of which statutes and which circumstances create actionable privacy injuries. Illustrations of the framework's utility cover three distinct kinds of authority: first, existing privately enforceable provisions, including those from the Wiretap Act,<sup>33</sup> the Video Privacy Protection Act,<sup>34</sup> the Stored Communications Act,<sup>35</sup> the Fair Credit Reporting Act,<sup>36</sup> the Telephone Consumer Protection Act,<sup>37</sup> Illinois's Biometric Information Privacy Act,<sup>38</sup> and others; second, authorities that are not currently privately enforceable, like the Health Insurance Portability and

---

29. See generally HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2009); see also *infra* Part IV.

30. See Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 33 (2011) (explaining privacy “in terms of expected flows of personal information, modeled with the construct of context-relative informational norms” and stating that “violations of these norms, however, often result in protest and complaint”).

31. See Ormerod, *Privacy Injuries*, *supra* note 22, at 176 (stating that the Supreme Court seems to want something more than mere information collection, like humiliation, mental anguish, or identity theft).

32. See *id.* at 190 (“The informational-injury framework also helps reveal the Court's inability to explain why some informational injuries are concrete and why others are not.”).

33. 18 U.S.C. § 2511.

34. 18 U.S.C. § 2710.

35. 18 U.S.C. § 121.

36. 15 U.S.C. § 1681.

37. 47 U.S.C. § 227.

38. 740 ILL. COMP. STAT. 14/1 (2008).

Accountability Act<sup>39</sup> and the California Consumer Privacy Act;<sup>40</sup> and third, proposed authorities at both the federal and state levels.<sup>41</sup>

It's too late to undo all of the havoc wrought by the Court's constitutional standing cases. But it isn't too late to adopt a framework that cabins the doctrine's most extreme implications and provides courts with a consistent and coherent way to protect privacy.

This Article has five parts. Part I reviews the history of Article III standing and categorizes the Court's recent informational-injury cases. Part II delves into the specifics of *Clapper*, *Spokeo*, and *TransUnion*. It diagnoses and describes the line-drawing and counter-majoritarian problems in detail and explains why other solutions fall short. Part III provides a brief primer on contextual integrity. Part IV first constructs the legal framework based on contextual integrity and then illustrates how to use the framework. Part V justifies the specifics—highlighting the legal framework's virtues and responding to objections.

## I. ARTICLE III STANDING: PAST AND PRESENT

The history of Article III standing is complex and contested. This Part briefly traces the origins of modern standing doctrine and then surveys the Supreme Court's contemporary approaches to informational injuries.

### A. *A Brief History of Article III Standing*

Article III provides that the “judicial Power of the United States’ . . . extends only to Cases and Controversies.”<sup>42</sup> According to the Supreme Court, “[s]tanding to sue is a doctrine rooted in the traditional understanding of a case or controversy,”<sup>43</sup> and the doctrine of standing “limits the category of litigants empowered to maintain a lawsuit in federal court to

---

39. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

40. CAL. CIV. CODE § 1798 (West 2018).

41. See, e.g., S. Res. 2968, 116th Cong. (2020); S.B. 5642, § 1102(b), 243 Leg. Sess. (N.Y. 2019).

42. U.S. CONST. art. III, §§ 1, 2.

43. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016).

seek redress for a legal wrong.”<sup>44</sup> Constitutional standing today has three components: A “plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.”<sup>45</sup>

Legal scholars have contested the accuracy of the Court’s sweeping generalizations that standing to sue is historically grounded.<sup>46</sup> Standing doctrine’s opponents have argued that “[t]here was no doctrine of standing prior to the middle of the twentieth century.”<sup>47</sup> According to this view, the form of the plaintiff’s action was historically the dispositive issue for justiciability—a court asked “whether the matter before it fit one of the recognized forms of action.”<sup>48</sup>

Other scholars have disagreed. Standing doctrine’s proponents contend that history may not compel the contours of modern standing doctrine, but it also doesn’t conclusively defeat it.<sup>49</sup> American courts in the eighteenth and nineteenth centuries did not use the term “standing,” but nonetheless “were well aware of the need for proper parties.”<sup>50</sup>

Central to the dispute is whether nineteenth century courts rooted standing in the federal Constitution. The opponents have argued that “for the first 150 years of the Republic—the Framers, the first Congresses, and the Court were oblivious to the modern conception . . . that standing is a component of the constitutional phrase ‘cases or controversies,’”<sup>51</sup> and that the first reference to “standing” as an Article III limitation dates to

44. *Id.* (citing *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 473 (1982)).

45. *Id.* (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)).

46. *See, e.g.*, Sunstein, *supra* note 5, at 166 (“It has no support in the text or history of Article III. It is essentially an invention of federal judges, and recent ones at that.”).

47. John A. Ferejohn & Larry D. Kramer, *Independent Judges, Dependent Judiciary: Institutionalizing Judicial Restraint*, 77 N.Y.U. L. REV. 962, 1009 (2002).

48. Steven L. Winter, *The Metaphor of Standing and the Problem of Self-Governance*, 40 STAN. L. REV. 1371, 1395 (1988).

49. *See* Ann Woolhandler & Caleb Nelson, *Does History Defeat Standing Doctrine?*, 102 MICH. L. REV. 689, 691 (2004).

50. *Id.*

51. Winter, *supra* note 48, at 1374.

a 1944 Supreme Court decision.<sup>52</sup> The proponents see the history differently: “While the nineteenth-century Court did not always make the constitutional nature of its concerns as clear as the twentieth-century Court has, . . . the Supreme Court did see some standing issues as constitutional, expressing particular concerns about unwarranted judicial interference with the federal and state political branches.”<sup>53</sup>

Everyone agrees, however, that the genesis of the Court’s current approach to Article III standing traces to the middle of the twentieth century.<sup>54</sup> *Flast v. Cohen*,<sup>55</sup> in 1968, represents standing skeptics’ high-water mark. *Flast* concerned taxpayer standing in the context of an alleged Establishment Clause violation.<sup>56</sup> Chief Justice Earl Warren’s opinion allowed the suit to proceed and created the “nexus test.”<sup>57</sup> The nexus test requires “a logical nexus between the status asserted and the claim sought to be adjudicated.”<sup>58</sup> Justice William O. Douglas’s concurrence foreshadowed that the nexus test would not prove “durable.”<sup>59</sup>

Two years later, Justice Douglas wrote for a unanimous court that “[t]he first question is whether the plaintiff alleges that the challenged action has caused him injury in fact, economic or otherwise.”<sup>60</sup> “Unlike the *Flast* ‘nexus,’ the ‘injury in fact’ criterion proved both hardy and luxuriant.”<sup>61</sup> But even after the term “injury in fact” arrived, the strictures of constitutionally grounded standing remained opaque. Some “prudential” limitations on standing could be discarded by

---

52. Sunstein, *supra* note 5, at 169.

53. Woolhandler & Nelson, *supra* note 49, at 713.

54. See, e.g., Freejohn & Kramer, *supra* note 47, at 1009.

55. 392 U.S. 83 (1968).

56. See *id.* at 88.

57. *Id.* at 102.

58. *Id.*

59. *Id.* at 107 (Douglas, J., concurring).

60. Ass’n of Data Processing Serv. Orgs., Inc. v. Camp, 397 U.S. 150, 152 (1970).

61. Seth F. Kreimer, “Spooky Action at a Distance”: *Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 749 (2016).

either Congress or the Court, and a justification for standing's "irreducible" constitutional "core" proved elusive.<sup>62</sup>

The Supreme Court's 1992 decision in *Lujan v. Defenders of Wildlife*<sup>63</sup> spawned the modern approach to Article III standing.<sup>64</sup> *Lujan* involved a suit filed under the citizen-suit provision of the Endangered Species Act (ESA),<sup>65</sup> which authorized "any person" to "commence a civil suit on his own behalf to enjoin any person" allegedly violating the ESA.<sup>66</sup> Wildlife conservation groups brought suit to enjoin a revised regulation that limited the geographic scope of one of the ESA's provisions.<sup>67</sup> Justice Antonin Scalia's majority opinion held that the plaintiffs lacked Article III standing because they had not suffered an "injury in fact."<sup>68</sup>

*Lujan* defines the injury in fact requirement as "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical."<sup>69</sup> The opinion also supplies a justification for the constitutional basis for standing doctrine.<sup>70</sup> *Flast v. Cohen* had rejected the suggestion that standing preserved the separation of powers: "The question whether a particular person is a proper party to maintain the action does not, by its own force, raise separation of powers problems related to the improper judicial

62. See Ormerod, *Privacy Injuries*, *supra* note 22, at 140 ("Prudential limitations on standing were subject to removal by the Court or Congress, whereas 'the constitutional core of standing . . . [was] a minimum requirement of injury in fact which not even Congress can eliminate.'").

63. 504 U.S. 555 (1992).

64. See John H. Hykes III, *Standing, Statutory Violations, and Concrete Injury in Federal Consumer Financial Protection Statutes After Spokeo, Inc. v. Robins*, 21 N.C. BANKING INST. 227, 231–22 (2017) ("The Supreme Court acknowledged in *Lujan* that Congress can elevate to the status of legally cognizable concrete injuries those intangible injuries which otherwise would be constitutionally inadequate.").

65. Pub. L. No. 93-205, 87 Stat. 884 (1973).

66. 16 U.S.C. § 1540(g).

67. *Lujan*, 504 U.S. at 558–59.

68. *Id.* at 577.

69. *Id.* at 560 (internal quotation marks omitted).

70. See Jonathan Poisner, *Environmental Values and Judicial Review After Lujan: Two Critiques of the Separation of Powers Theory of Standing*, 18 ECOLOGY L.Q. 335, 350–52 (1991) (stating that *Lujan* confirmed the inevitability of the proof requirement as part of the separation of powers theory of standing).

interference in areas committed to other branches of the Federal Government.”<sup>71</sup> Having contested *Flast’s* treatment of the separation of powers in a law review article about a decade earlier,<sup>72</sup> Justice Scalia’s *Lujan* opinion enshrines the separation of powers as the justification for constitutional limits on standing:

To permit Congress to convert the undifferentiated public interest in executive officers’ compliance with the law into an “individual right” vindicable in the courts is to permit Congress to transfer from the President to the courts the Chief Executive’s most important constitutional duty, to “take Care that the Laws be faithfully executed.”<sup>73</sup>

The pace of the Supreme Court’s standing cases accelerated after *Lujan*. At the Roberts Court, scarcely a year has passed in the last decade without one or more major decisions premised on Article III standing.<sup>74</sup>

### B. *Injury in Fact and Information After Lujan*

*Lujan’s* definition of the injury in fact requirement poses particular difficulties for injuries that involve information. Information is intangible and non-rivalrous, characteristics that tend to vex courts evaluating whether an informational injury is concrete, particularized, and actual or imminent.<sup>75</sup>

Despite these inherent difficulties, even after *Lujan* there are four distinct bare informational harms that can create a justiciable Article III injury: injuries arising from the wrongful collection of information, injuries arising from the wrongful use

71. *Flast v. Cohen*, 392 U.S. 83, 100 (1968).

72. See Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 890–93 (1983) (discussing the *Flast* holding and impact).

73. *Lujan*, 504 U.S. at 577.

74. See Ormerod, *Privacy Injuries*, *supra* note 22, at 136 (listing such cases decided before or during October Term 2020: *Carney v. Adams*, 141 S. Ct. 493 (2020); *Trump v. New York*, 141 S. Ct. 530 (2020); *Uzuegbunam v. Preczewski*, 141 S. Ct. 792 (2021); *California v. Texas*, 141 S. Ct. 2104 (2021); *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021)).

75. See Kreimer, *supra* note 61, at 752–54 (“Information is intangible. Information is often difficult to combine to particular recipients. And in the age of the Internet, information is immediately available without constraint of time or space.”).

of information, injuries arising from the wrongful dissemination of information, and injuries arising from the wrongful withholding of information.<sup>76</sup> To be clear, not all informational injuries necessarily implicate privacy concerns. But most—and perhaps all—privacy violations involve an informational injury.<sup>77</sup>

The first informational injury is information collection. In an information collection case, a statute prohibits the collection of certain information but an entity collects covered information anyway in violation of the statute.<sup>78</sup> In such a case, the person to whom the information relates (the data subject) has suffered an information collection injury.<sup>79</sup>

The Court has held that some information collection injuries are sufficiently concrete for Article III purposes. For example, in 2001's *Bartnicki v. Vopper*,<sup>80</sup> an unidentified person intercepted and recorded a phone conversation between a union's president and the union's negotiator.<sup>81</sup> A radio show later broadcast the recording, and the conversation participants sought statutory damages under the federal Wiretap Act and its state equivalents.<sup>82</sup> In relevant part, the Wiretap Act prohibits "intentionally intercept[ing] . . . any wire, oral, or electronic communication."<sup>83</sup>

All nine Justices agreed that both the interception of the conversation and its dissemination were concrete injuries<sup>84</sup> (Part I.B.3 revisits *Bartnicki* as an information dissemination case). A six-Justice majority held that enforcing the Wiretap Act's prohibition in this case violated the First Amendment's Free Speech Clause.<sup>85</sup> But the majority expressly acknowledged

76. See Ormerod, *Privacy Injuries*, *supra* note 22, at 133.

77. See *id.* at 138 ("Most privacy injuries are informational in nature.").

78. *Id.* at 143.

79. See *id.* (summarizing such Supreme Court cases).

80. 532 U.S. 514 (2001).

81. *Id.* at 518–19.

82. *Id.*

83. 18 U.S.C. § 2511(1)(a).

84. See Ormerod, *Privacy Injuries*, *supra* note 22, at 143 (discussing *Bartnicki*).

85. See *Bartnicki*, 532 U.S. at 525 ("The only question is whether the application of these statutes in such circumstances violates the First Amendment.").

two things—first, that the defendants had violated the statute when they disseminated the recording; and second, that the Court had jurisdiction to consider the merits of enforcing the statute against the defendants.<sup>86</sup> Any adjudication on the merits presupposes the existence of the jurisdictional requirement of Article III standing.<sup>87</sup> Chief Justice William Rehnquist's dissenting opinion agreed that the plaintiffs suffered an injury but disagreed that the statutes violated the First Amendment.<sup>88</sup>

The second informational injury is information use. Information use injuries encompass several different informational practices.<sup>89</sup> What they have in common is that a defendant uses a data subject's information in an injurious way that does not involve the dissemination of that information.<sup>90</sup> To be sure, uses and disclosures often go hand-in-hand because dissemination is one common way to use information.<sup>91</sup> But disseminations are distinct informational injuries and are addressed next.

Many federal laws limit the permissible uses of certain types of information. For example, the Health Insurance Portability and Accountability Act (HIPAA) gives individuals the right “to request that the covered entity restrict . . . uses or disclosures of protected health information about the individual.”<sup>92</sup> Similarly, the Gramm-Leach-Bliley Act's (GLBA)<sup>93</sup> Privacy Rule limits the “redisclosure and reuse” of some nonpublic personal information.<sup>94</sup>

To date, the Supreme Court has not explicitly addressed when a bare information use injury suffices for Article III purposes. Neither HIPAA nor GLBA are privately enforceable,

---

86. *Id.* at 525.

87. *See, e.g.*, *Frederiksen v. City of Lockport*, 384 F.3d 437, 438 (7th Cir. 2004) (“A suit dismissed for lack of jurisdiction cannot also be dismissed ‘with prejudice’; that’s a disposition on the merits, which only a court with jurisdiction may render.”).

88. *Bartnicki*, 532 U.S. at 553 (Rehnquist, C.J., dissenting).

89. *See Ormerod, Privacy Injuries, supra* note 22, at 144.

90. *See id.* (describing intellectual property law and prohibitions on discrimination as information use restrictions).

91. *See id.* at 147.

92. 45 C.F.R. § 164.522(a)(1)(i)(A).

93. Pub. L. No. 106-102, 113 Stat. 1338 (1999).

94. 12 C.F.R. § 1016.11.



so violations of those authorities' use limitations don't squarely present cases that implicate Article III standing.<sup>95</sup> While the Fair Credit Reporting Act is privately enforceable and does include information use or purpose limitations, those restrictions are best understood as restrictions on dissemination.<sup>96</sup> Nevertheless, the Court has routinely decided cases that presuppose the sufficiency of information use injuries.<sup>97</sup>

Despite the Court's silence on this issue, there are good reasons to believe that at least some information uses are inherently injurious. Examples discussed later in Part IV.B include facial recognition harms, data protection law's purpose restrictions, and prohibitions on spam telephone calls.

The third informational injury is information dissemination. In a dissemination case, a statute prohibits the dissemination of information, and the defendant flouts the proscription to the detriment of the data subject, the plaintiff.<sup>98</sup> The Court has previously recognized the Article III sufficiency of some information dissemination injuries. *Bartnicki* is an obvious example.<sup>99</sup> There, the defendants were those who broadcast the phone conversation recording, and the Court held that "the disclosure of the contents of the intercepted conversations . . . violated the federal and state statutes . . . [and the] petitioners are thus entitled to recover damages from each of the respondents."<sup>100</sup> The only remaining question, the Court said, was "whether the application of these statutes in such circumstances violates the First Amendment."<sup>101</sup>

---

95. See R. Bradley McMahon, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 VILL. L. REV. 625, 643, 650 (2004) (stating that these laws do not provide individuals with private causes of action).

96. See 15 U.S.C. § 1681b(3) (listing permissible uses of the information).

97. See, e.g., *Facebook v. Duguid*, 141 S. Ct. 1163, 1168 (2021) (resolving the merits of a Telephone Consumer Protection Act statutory construction case).

98. See Ormerod, *Privacy Injuries*, *supra* note 22, at 148–49 (discussing cases involving information dissemination).

99. See *id.* at 148.

100. *Bartnicki v. Vopper*, 532 U.S. 514, 525 (2001).

101. *Id.*

*Doe v. Chao*,<sup>102</sup> in 2004, holds the same. There, a plaintiff sued the U.S. Department of Labor for disclosing his Social Security number in violation of the Privacy Act.<sup>103</sup> A six-Justice majority ruled against Doe on the merits of his statutory claim, but nonetheless held that he had suffered an injury in fact.<sup>104</sup> The statute’s reference to “adverse effect’ acts as a term of art identifying a potential plaintiff who satisfies the injury-in-fact and causation requirements of Article III standing, and who may consequently bring a civil action without suffering dismissal for want of standing to sue.”<sup>105</sup> The dissent agreed on the standing issue: “Doe has standing to sue, the Court agrees, based on allegations that he was ‘torn . . . all to pieces’ and ‘greatly concerned and worried’ because of the disclosure of his Social Security number and its potentially ‘devastating’ consequences.”<sup>106</sup>

The final type of informational harm is information withholding. In an information withholding case, a statute provides a plaintiff with a legal right to access certain information.<sup>107</sup> When the entity that controls the information—the defendant—refuses to disclose it, the plaintiff has suffered an information withholding injury.<sup>108</sup>

The Supreme Court has held that an information withholding injury suffices for Article III. In 1998’s *Federal Election Commission v. Akins*,<sup>109</sup> the Federal Election Commission (FEC) had determined that the American Israel Public Affairs Committee (AIPAC) was not a “political committee” as that term is defined in the Federal Election Campaign Act (FECA).<sup>110</sup> That determination exempted AIPAC from needing to disclose information about its membership, contributions, and expenditures.<sup>111</sup> A group of voters eventually brought suit in federal court under a provision of the statute

---

102. 540 U.S. 614 (2004).

103. *Id.* at 616–17.

104. *Id.* at 624.

105. *Id.*

106. *Id.* at 641 (Ginsburg, J., dissenting) (cleaned up).

107. Ormerod, *Privacy Injuries*, *supra* note 22, at 135.

108. *See id.* at 137.

109. 524 U.S. 11 (1998).

110. 2 U.S.C. § 431(4)(A); *Akins*, 524 U.S. at 13.

111. *Akins*, 524 U.S. at 13–14.

that permitted “[a]ny party aggrieved” to seek judicial review of an FEC decision to dismiss a complaint.<sup>112</sup> The FEC sought to dismiss the suit on standing grounds.<sup>113</sup>

The Court held that the informational injury the plaintiffs suffered was sufficient for Article III: “The ‘injury in fact’ that respondents have suffered consists of their inability to obtain information . . . that, on respondents’ view of the law, the statute requires AIPAC make public.”<sup>114</sup> The majority also explained that past cases had “held that a plaintiff suffers an ‘injury in fact’ when the plaintiff fails to obtain information which must be publicly disclosed pursuant to a statute.”<sup>115</sup>

*Akins* is interesting because the plaintiffs faced two hurdles that many privacy plaintiffs will not—particularization concerns and a governmental defendant.<sup>116</sup> First, with respect to particularization, Justice Scalia’s dissent argued that the voters had suffered only a generalized grievance: “[T]he injury or deprivation is not only widely shared but it is undifferentiated. . . . [The] harm caused to Mr. Akins by the allegedly unlawful failure to enforce FECA is precisely the same as the harm caused to everyone else: unavailability of a description of AIPAC’s activities.”<sup>117</sup>

Second, the separation of powers justification for Article III standing is at its zenith when a plaintiff challenges the Executive Branch’s interpretation of the law.<sup>118</sup> And as *Lujan*

112. See 52 U.S.C. § 30109(a)(8)(A).

113. *Akins*, 524 U.S. at 18.

114. *Id.* at 21. Other cases have reached the same conclusion. See, e.g., *Pub. Citizen v. DOJ*, 491 U.S. 440, 449 (1989).

115. *Akins*, 524 U.S. at 21 (citing *Pub. Citizen v. DOJ*, 491 U.S. 440, 449 (1989); *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373–74 (1982)). Lower courts have held that some statutory schemes don’t supply an injury in fact for alleged information withholding injuries. See, e.g., *Elec. Priv. Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity*, 878 F.3d 371, 378 (D.C. Cir. 2017) (rejecting standing for an information withholding injury because the plaintiff did not suffer the type of harm that the statute sought to prevent).

116. See *Akins*, 524 U.S. at 29–30 (Scalia, J., dissenting) (“The provision of law at issue in this case is an extraordinary one, conferring upon a private person the ability to bring an Executive agency into court to compel its enforcement of the law against a third party.”).

117. *Id.* at 35–36 (emphasis omitted).

118. See, e.g., *id.* at 36 (“A system in which the citizenry at large could sue to compel Executive compliance with the law would be a system in which the courts, rather than the President, are given the primary responsibility to ‘take

shows us, these two hurdles are intimately connected—*Lujan* and *Akins* share in common a concern about “[t]he public’s nonconcrete interest in the proper administration of the laws.”<sup>119</sup>

Privacy cases involving withholding injuries are unlikely to create similar problems.<sup>120</sup> Your right to access information about yourself is inherently particularized in a way that the right in *Akins* was not. And many—perhaps most—information access rights that implicate privacy concerns apply to private-sector actors.<sup>121</sup> To be sure, the Court recently held that a company’s violation of a statute that requires information production only sometimes supplies the plaintiff with a sufficiently concrete injury.<sup>122</sup> But even that case confirms that “formatting errors” that violate an information production requirement can suffice for Article III standing.<sup>123</sup>

\* \* \*

This Part has shown that the history of Article III standing is opaque but the Court’s modern approach recognizes that at least some bare informational harms are inherently injurious. The next Part describes privacy’s most recent Article III setbacks at the Supreme Court.

## II. PRIVACY’S ARTICLE III PROBLEMS

In the past decade, the Supreme Court decided three Article III standing cases that have ominous implications for privacy. This Part first surveys these decisions; it then synthesizes the

---

Care that the Laws be faithfully executed.” (quoting U.S. CONST. art. II, § 3)). For more on this, see *infra* Part II.B.2.

119. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring in part and concurring in the judgment in part).

120. The California Consumer Privacy Act, for example, includes several access provisions. See CAL. CIV. CODE §§ 1798.100(a), 1798.110(a) (permitting access to information from business that collect personal information); *id.* § 1798.115(a) (permitting access to information from businesses that sell or disclose personal information).

121. See, e.g., *id.* §§ 1798.100(a), 1798.110(a). For more on this, see *infra* Part IV.B.

122. See *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2213–14 (2021).

123. See *id.* at 2214 (“As for the claims pertaining to the format of TransUnion’s mailings, none of the 8,185 class members *other than the named plaintiff Ramirez* suffered a concrete harm.” (emphasis added)).

problems for privacy that they signal and evaluates other attempts to resolve them.

#### A. *Recent Cases*

In recent years, the Supreme Court's Article III standing jurisprudence has been extraordinarily active.<sup>124</sup> This section focuses on three cases that highlight some significant problems for privacy standing—2013's *Clapper v. Amnesty International USA*, 2016's *Spokeo, Inc. v. Robins*, and 2021's *TransUnion LLC v. Ramirez*.

##### 1. *Clapper v. Amnesty International USA* (2013)

The plaintiffs—attorneys, journalists, and human-rights activists—challenged the constitutionality of a recently enacted statute that expanded the government's foreign surveillance authority.<sup>125</sup> The plaintiffs believed that some of the people with whom they communicated would be targeted by the government's surveillance, and hence that the plaintiffs' communications would be intercepted in violation of the Fourth Amendment.<sup>126</sup> *Clapper* is thus an information collection case: The plaintiffs argued that the government's collection of their communications—in violation of the Fourth Amendment—constituted their injury in fact.<sup>127</sup>

The plaintiffs' theories of harm fell into two categories. First, future harms: they argued there was "an objectively reasonable likelihood that their communications will be acquired under [the statute] at some point in the future."<sup>128</sup> Second, mitigation harms: they argued that "the threat of surveillance will compel them to travel abroad in order to have in-person conversations" and that these "costly and burdensome measures" to avoid surveillance constituted an ongoing present injury.<sup>129</sup>

---

124. See Ormerod, *Privacy Injuries*, *supra* note 22, at 136.

125. See *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 406 (2013).

126. *Id.* at 406–07.

127. See *id.* at 401.

128. *Id.*

129. *Id.* at 407.

The Second Circuit sided with the plaintiffs on both theories. It held that the plaintiffs had standing because there was an objectively reasonable likelihood that their communications would be intercepted<sup>130</sup> and because they were suffering ongoing “present injuries in fact—economic and professional harms—stemming from a reasonable fear of future harmful government conduct.”<sup>131</sup>

The Supreme Court reversed on both future injuries and mitigation harms.<sup>132</sup> Justice Samuel Alito’s opinion for the 5–4 majority rejected the Second Circuit’s future injury standard—“an objectively reasonable likelihood”—and instead offered an exceedingly stringent one: The “threatened injury must be *certainly impending* to constitute injury in fact.”<sup>133</sup> And the plaintiffs fell short of that standard because their allegations rested on a “highly speculative . . . chain of contingencies.”<sup>134</sup> The Court added that the plaintiffs’ allegations were particularly speculative because they “require[d] guesswork as to how independent decisionmakers will exercise their judgment.”<sup>135</sup>

In dissent, Justice Stephen Breyer identified several past decisions in which the Court used a less demanding standard to conclude that a plaintiff alleging future harm had standing.<sup>136</sup> In footnote five of the majority opinion, Justice Alito responded:

Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a “substantial risk” that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.<sup>137</sup>

---

130. *See id.* (citing *Amnesty Int’l USA v. Clapper*, 638 F.3d 118, 133–34, 139 (2d Cir. 2011)).

131. *Id.* (quoting *Amnesty Int’l USA v. Clapper*, 638 F.3d 118, 138 (2d Cir. 2011) (emphasis omitted)).

132. *Id.* at 422.

133. *Id.* at 409 (emphasis added) (internal quotation marks omitted) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)).

134. *Id.* at 410.

135. *Id.* at 413.

136. *See id.* at 432–33 (Breyer, J., dissenting) (listing cases).

137. *Id.* at 414 n.5.

Footnote five also adds that “to the extent that the ‘substantial risk’ standard is relevant and distinct from the ‘certainly impending’ requirement, [the plaintiffs] fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm.”<sup>138</sup>

As one scholar has noted, “Footnote five, in other words, appeared to be an alternative holding in *Clapper*—namely, that even under the less onerous ‘substantial risk’ standard, the plaintiffs in that case had failed to satisfy their burden.”<sup>139</sup> Sixteenth months after *Clapper*, a unanimous Court decided a different future-injury standing case in which Justice Clarence Thomas’s majority opinion applied the “substantial risk” standard—all but ignoring *Clapper*’s “certainly impending” requirement.<sup>140</sup>

The *Clapper* majority also held that the plaintiffs’ present injury claims—their mitigation harms—did not supply an Article III injury in fact.<sup>141</sup> The Court held that the mitigation efforts could not “manufacture standing merely by inflicting harm on themselves based on their fears of a hypothetical future harm that is not certainly impending.”<sup>142</sup> In other words, the Court held that mitigation harms are never sufficient for an injury in fact—they are beside the point, a null set.<sup>143</sup> Mitigation harms only supply standing when they are taken in response to a certainly impending future injury, but a certainly impending injury is, alone, sufficient for standing.<sup>144</sup> In short, there are no cases in which mitigation changes the result. Either a harm is certainly impending (yes standing) or it’s not (no standing), and mitigation efforts don’t matter in either case.

---

138. *Id.*

139. Marty Lederman, *Commentary: Susan B. Anthony List, Clapper Footnote 5, and the State of Article III Standing Doctrine*, SCOTUSBLOG (June 17, 2014, 4:34 PM), <https://perma.cc/G4Q9-6MB2>.

140. *See* Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158, 164–67 (2014).

141. *See* *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 418 (2013).

142. *Id.* at 416.

143. *See id.* at 417.

144. *See id.* at 416.

2. *Spokeo, Inc. v. Robins* (2016)

The Fair Credit Reporting Act (FCRA) seeks to “ensure fair and accurate credit reporting” by “regulat[ing] the creation and the use of consumer reports by consumer reporting agencies.”<sup>145</sup> The statute is privately enforceable, providing that “any person who willfully fails to comply with any requirement of the Act with respect to any individual is liable to that individual’ for, among other things, either ‘actual damages’ or statutory damages of \$100 to \$1,000 per violation, costs of the action and attorney’s fees, and possibly punitive damages.”<sup>146</sup>

Robins, the plaintiff, filed an FCRA suit against Spokeo, a company that operates a “people search engine.”<sup>147</sup> The company’s search results for Robins reported that “he is married, has children, is in his 50’s, has a job, is relatively affluent, and holds a graduate degree.”<sup>148</sup> According to Robins, all of that information was false.<sup>149</sup> *Spokeo* is thus an information dissemination case: Robins argued that Spokeo disseminated false information about him in violation of the statute and in a way that posed a risk to his employment prospects.<sup>150</sup>

In 2010, Robins instituted a putative class action, alleging that Spokeo willfully failed to comply with the FCRA.<sup>151</sup> The district court granted Spokeo’s motion to dismiss, holding that Robins had failed to “properly plead” an Article III injury in fact.<sup>152</sup> The Ninth Circuit reversed.<sup>153</sup> Noting that “the violation of a statutory right is usually a sufficient injury in fact to confer standing,” the Ninth Circuit held that Robins alleged a sufficient injury because he alleged that “Spokeo violated his statutory rights, not just the statutory rights of other people,”

---

145. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 334 (2016) (quoting 15 U.S.C. § 1681(a)) (internal quotation marks and alterations omitted).

146. *Id.* at 335 (internal quotation marks, footnotes, and brackets omitted).

147. *Id.* at 333.

148. *Id.* at 336.

149. *Id.*

150. *See id.* at 336, 350.

151. *Id.* at 336.

152. *Id.* at 337.

153. *Id.*



and because his “personal interests in the handling of his credit information are individualized rather than collective.”<sup>154</sup>

In a 6–2 opinion by Justice Alito, the Court vacated and remanded the case to the Ninth Circuit.<sup>155</sup> The majority explained that remand was necessary because the “Ninth Circuit’s analysis focused on the second characteristic (particularity), but it overlooked the first (concreteness).”<sup>156</sup> The majority’s discussion of Article III concreteness is convoluted, touching on at least four distinct subjects—an injury’s tangibility, the role of history and Congress, procedural versus substantive rights, and the so-called “risk of real harm.”<sup>157</sup> According to the majority, Congress’s “role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.”<sup>158</sup>

Here, the Court held, Robins had merely alleged a “deprivation of a procedural right without [a] concrete interest . . . affected by the deprivation.”<sup>159</sup> The Court acknowledged that, through the FCRA, “Congress plainly sought to curb the dissemination of false information by adopting procedures designed to decrease that risk,” but nonetheless held that “not all inaccuracies cause harm or present any material risk of harm.”<sup>160</sup> For example, the Court said, it is “difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.”<sup>161</sup>

---

154. *Robins v. Spokeo, Inc. (Robins I)*, 742 F.3d 409, 413 (9th Cir. 2014) (emphasis omitted).

155. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 343 (2016).

156. *Id.* at 334.

157. *See id.* at 339–43; *see also* Ormerod, *Privacy Injuries*, *supra* note 22, 151–57 (discussing the Court’s analysis in *Spokeo*).

158. *Spokeo*, 578 U.S. at 341.

159. *Id.* at 346–47 (quoting *Summers v. Earth Island Inst.*, 555 U.S. 488, 496 (2009)).

160. *Id.* at 342.

161. *Id.*

3. *TransUnion LLC v. Ramirez* (2021)

TransUnion is one of the three major credit-reporting companies in the United States.<sup>162</sup> Beginning in 2002, TransUnion began cross-referencing the first and last names of credit-check subjects against the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) list.<sup>163</sup> The OFAC list includes terrorists, drug traffickers, and other serious criminals who threaten America's national security and with whom it is generally unlawful to transact business.<sup>164</sup> Despite producing thousands of false positives and spawning litigation that TransUnion lost, TransUnion continued to cross-reference only subjects' first and last names for nearly a decade.<sup>165</sup>

In 2011, Sergio Ramirez sought to purchase a car, and the ensuing credit check reported that he was a "potential match" for an individual on the OFAC list.<sup>166</sup> Ramirez requested his credit report from TransUnion, and the company sent him two mailings—the first included his credit report and a summary of his rights under the FCRA but omitted the OFAC designation; the second included the OFAC designation but omitted the summary of rights.<sup>167</sup>

Ramirez sued TransUnion and alleged two types of informational injuries: first, information dissemination—that TransUnion's dissemination of the false OFAC designation to the car dealership violated the "maximum possible accuracy" provision of the FCRA; second, information withholding—that both of TransUnion's mailings failed to comply with his information access rights under the FCRA.<sup>168</sup>

The district court certified a class that included 8,185 people whom TransUnion had designated an OFAC match and

---

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

163. *Id.*

164. *Id.*

165. *See id.* at 2201–02; *id.* at 2215–16 (Thomas, J., dissenting) (summarizing *Cortez v. Trans Union LLC*, 617 F.3d 688 (3d Cir. 2010), where Cortez's name erroneously flagged as a match with a person named Cortes on the OFAC list, yet TransUnion failed to remove the alert for years); Brief for Respondent at 14, *TransUnion*, 141 S. Ct. 2190 (No. 20-297) ("After July 26, 2011, TransUnion abandoned the procedures it defends before this Court.").

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

167. *Id.* at 2201–02.

168. *Id.* at 2208.

who had requested and received the same two mailings as Ramirez.<sup>169</sup> Of that class, the parties stipulated that 1,853 people had their credit reports disseminated by TransUnion to potential creditors.<sup>170</sup> Ramirez won at trial and the Ninth Circuit mostly affirmed.<sup>171</sup> In a 5–4 opinion by Justice Kavanaugh, the Supreme Court vacated and remanded the Ninth Circuit’s decision,<sup>172</sup> and the opinion effects two pairs of noteworthy developments.

The first pair concerns the specifics of Ramirez’s case. The Court issued a split decision on both the dissemination and withholding injuries. As to dissemination, the Court held that only the 1,853 people who had their credit reports disseminated to potential lenders had suffered a concrete Article III injury; the other 6,332 had not.<sup>173</sup> The Court explained that, as to the 1,853 people, “a person is injured when a defamatory statement that would subject him to hatred, contempt, or ridicule is published to the third party,” and that the “harm from being labeled a ‘potential terrorist’ bears a close relationship to the harm from being labeled a ‘terrorist.’”<sup>174</sup> But the remaining 6,332 people lacked a concrete injury because their harm “is roughly the same . . . as if someone wrote a defamatory letter and then stored it in her desk drawer,” and a “letter that is not sent does not harm anyone, no matter how insulting the letter is.”<sup>175</sup>

As to the withholding injuries, the Court held that only Ramirez had suffered a concrete injury and that the rest of the class had not.<sup>176</sup> The Court recast Ramirez’s withholding injuries as mere formatting errors, and thus distinguished *Akins* and *Public Citizen v. DOJ*.<sup>177</sup> Because Ramirez had failed to produce any “evidence that, other than Ramirez, a single

---

169. *Id.*

170. *Id.*

171. *Id.* (citing *Ramirez v. TransUnion LLC*, 951 F.3d 1008 (9th Cir. 2020)).

172. *Id.* at 2214.

173. *See id.* at 2208–13.

174. *Id.* at 2208–09 (some internal quotations marks omitted).

175. *Id.* at 2210.

176. *See id.* at 2213–14.

177. 491 U.S. 440 (1989); *see TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2214 (2021).

other class member so much as *opened* the dual mailings, nor that they were confused, distressed, or relied on the information in any way,” the absent class members lacked a sufficiently concrete injury in fact.<sup>178</sup> “Without any evidence of harm caused by the format of the mailings,” the Court explained, “these are bare procedural violations, divorced from any concrete harm.”<sup>179</sup>

In arriving at these holdings, however, the majority opinion produced a pair of novel doctrinal evolutions. First, the Court clarified its language from *Clapper* about future injuries. Ramirez had argued that the 6,332 class members had also suffered a future injury because their credit reports could have been disseminated with the false designation at any time.<sup>180</sup> The Court rejected that argument and suggested that a risk of future injury is never sufficient for Article III in any case where the plaintiffs seek damages.<sup>181</sup> In other words, only in cases for injunctive relief—like *Clapper*—will a plaintiff satisfy Article III for a harm not yet materialized.<sup>182</sup>

Second, the Court elaborated on the constitutional footing of current standing doctrine. For the first time, the Court held that even particularized injuries may violate both Article III and Article II: “A regime where Congress could freely authorize unharmed plaintiffs to sue defendants who violate federal law not only would violate Article III but also would infringe on the Executive Branch’s Article II authority.”<sup>183</sup> Picking up a thread from Justice Thomas’s *Spokeo* concurrence and from the Ramirez oral argument, the Court held that “the choice of how

---

178. *TransUnion LLC*, 141 S. Ct. at 2213–14 (internal quotation marks omitted).

179. *Id.* at 2213 (internal quotation marks and brackets omitted).

180. *Id.* at 2212.

181. *See id.* at 2210–11 (“TransUnion advances a persuasive argument that in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm.”).

182. *See id.* at 2211

If the risk of future harm materializes and the individual suffers a concrete harm, then the harm itself, and not the pre-existing risk, will constitute a basis for the person’s injury and for damages. If the risk of future harm does *not* materialize, then the individual cannot establish a concrete harm sufficient for standing, according to TransUnion.

183. *Id.* at 2207 (emphasis omitted).

to prioritize and how aggressively to pursue legal actions against defendants who violate the law falls within the discretion of the Executive Branch, not within the purview of private plaintiffs (and their attorneys).<sup>184</sup>

### B. *Two Problems*

These three cases signal several significant problems for privacy standing. This section focuses on just two of them: the Court's failure to supply a line-drawing principle for its informational-injury cases and the absence of a justification for upsetting political consensus.

#### 1. No Line-Drawing Principle

*Clapper*, *Spokeo*, and *TransUnion* fail to supply a principle for discerning when an informational injury is concrete, particularized, and actual or imminent.

In *Clapper*, the Court held that the plaintiffs lacked proof that the government would intercept their communications in violation of the Fourth Amendment. Yet all nine Justices seemed to agree that the plaintiffs would have had a concrete (and actual) injury if they could have proven that their communications had already been intercepted.<sup>185</sup> “Notwithstanding the division as to whether plaintiffs had adequately proven a threat of interception, both the majority and dissent in *Clapper* appeared to accept that when the government illicitly acquires private information, an actual interception constitutes a justiciable ‘injury in fact.’<sup>186</sup> Justice Breyer’s dissent stressed that “[n]o one here denies that the Government’s interception of a private telephone or e-mail conversation amounts to an injury that is ‘concrete and particularized.’<sup>187</sup>

But not all information collections create an injury in fact. For example, the District of Columbia’s Use of Consumer

---

184. *Id.*

185. See *supra* notes 141–144 and accompanying text.

186. Kreimer, *supra* note 61, at 758.

187. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 423 (2013) (Breyer, J., dissenting).

Identification Act (D.C. I.D. Act)<sup>188</sup> provides that “no person shall, as a condition of accepting a credit card as payment for a sale of goods or services, request or record the address or telephone number of a credit card holder on the credit card transaction form.”<sup>189</sup> Two D.C. consumers brought suit under the law after their zip codes were requested and recorded at point-of-sale retail transactions.<sup>190</sup> The D.C. Circuit held that the plaintiffs had failed to allege an Article III injury in fact: “If, as the Supreme Court advised [in *Spokeo*], disclosure of an incorrect zip code is not a concrete Article III injury, then even less so is [the plaintiffs’] naked assertion that a zip code was requested and recorded without any concrete consequence.”<sup>191</sup>

This example, in conjunction with *Clapper*, thus illustrates that some informational practices are injurious enough for Article III, but others are not. How is a plaintiff to know? *Clapper* was an easy case on this front because it involved communicative content—phone conversations and the bodies of email messages.<sup>192</sup> The Fourth Amendment (and several statutes)<sup>193</sup> have long singled out communicative content for special protection,<sup>194</sup> but it’s implausible that Article III’s case or controversy requirement observes the same letter-versus-envelope distinction.

In other words, surely the collection of some information other than communicative content suffices for Article III injuries. Federal law, for example, prohibits health insurers

---

188. D.C. CODE § 47-3153 (2022).

189. *Id.* § 47-3153(a).

190. *See* *Hancock v. Urb. Outfitters, Inc.*, 830 F.3d 511, 512 (D.C. Cir. 2016).

191. *Id.* at 514.

192. *See supra* note 187 and accompanying text.

193. *Compare* Wiretap Act, 18 U.S.C. § 511 (prohibiting the “interception and disclosure of wire, oral, or electronic communications”), *with* Pen Register Statute, 18 U.S.C. § 3121 (prohibiting “pen register and trap and trace device use”).

194. *See, e.g.*, *Katz v. United States*, 389 U.S. 347, 352 (1967) (phone conversations); *Berger v. New York*, 388 U.S. 41, 46 (1967) (same); *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (physical letters in the mail); *United States v. Warshak*, 631 F.3d 266, 274 (6th Cir. 2010) (email content); *Carpenter v. United States*, 138 S. Ct. 2206, 2220–22 (2018) (seeming to accept *Warshak*’s conclusion about email content); *id.* at 2230 (Kennedy, J., dissenting) (same).

from collecting individuals' genetic information.<sup>195</sup> If that statute included a private right of action and a plaintiff alleged that an insurer violated the statute, would the plaintiff have an Article III injury in fact? The Court's cases don't supply an answer.

*Spokeo* raises the same problem in the context of information dissemination. Recall that the Court held that it's "difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."<sup>196</sup> But surely some disseminations of information are injurious. After all, on remand in *Spokeo*, the Ninth Circuit conducted a concreteness analysis and concluded that Robins had alleged a sufficient "risk of real harm" to constitute an injury in fact: "Robins's allegations relate facts that are substantially more likely to harm his concrete interests than the Supreme Court's example of an incorrect zip code."<sup>197</sup> For example, the Ninth Circuit said, "Robins alleged that he is out of work and looking for a job, but that Spokeo's inaccurate reports have caused actual harm to his employment prospects by misrepresenting facts that would be relevant to employers."<sup>198</sup> "Even if their likelihood actually to harm Robins's job search could be debated," the court concluded, "the inaccuracies alleged in this case do not strike us as the sort of mere technical violations which are too insignificant to present a sincere risk of harm to the real-world interests that Congress chose to protect with the FCRA."<sup>199</sup>

Other courts have followed suit. The Eleventh Circuit and the Ninth Circuit, for example, have both concluded that disseminating information in violation of the Video Privacy Protection Act<sup>200</sup> is—without anything else—a concrete injury in fact.<sup>201</sup>

Both *TransUnion's* dissemination and withholding conclusions compound this line-drawing problem. As the

---

195. See 29 U.S.C. § 1182(d).

196. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 342 (2016).

197. *Robins v. Spokeo, Inc. (Robins II)*, 867 F.3d 1108, 1117 (9th Cir. 2017).

198. *Id.* (internal quotation marks and brackets omitted).

199. *Id.* (internal quotation marks and brackets omitted).

200. 18 U.S.C. § 2710.

201. See *Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1341 (11th Cir. 2017); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017).

*TransUnion* dissents explain, the distinctions the majority draws between class members are illusory. On dissemination, “TransUnion published [the false OFAC designation] to vendors that printed and sent the mailings,” and in “the historical context of libel, publication to even a single other party could be enough to give rise to suit,” including “a telegraph company, an attorney, or a stenographer who merely writes the information down.”<sup>202</sup> Further, “why is it so speculative that a company in the business of selling credit reports to third parties will in fact sell a credit report to a third party?”<sup>203</sup> On withholding, “the majority makes a set of curious assumptions,” like that “people who specifically request a copy of their credit report may not even ‘open[]’ the envelope,” and “people who learn that their credit files label them potential terrorists would not ‘have tried to correct’ the error.”<sup>204</sup>

In sum, the Court appears unlikely to slow its inexorable campaign to sharply limit intangible injuries. Recent informational standing cases have raised unanswered questions about how courts should draw the line between sufficiently and insufficiently concrete injuries. And even when everyone agrees that an informational practice is injurious, the Court has obfuscated the level of risk that is necessary to establish standing. What makes some informational practices per se injurious? How should lower courts (and legislatures) conduct that analysis? And what level of risk suffices for per se injurious practices?

## 2. No Justification for Upsetting Political Consensus

The failure to supply a line-drawing principle is not, however, the Court’s most fundamental error in its recent standing decisions. The Court has also failed to justify its practice of nullifying duly enacted private rights of action and thereby overriding the byproduct of political consensus.

The only justification the Court has ever offered for standing doctrine is the separation of powers.<sup>205</sup> But upon closer

---

202. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2223 (2021) (Thomas, J., dissenting).

203. *Id.* at 2225 (Kagan, J., dissenting).

204. *Id.* at 2225–26 (emphasis omitted) (alteration in original).

205. *See, e.g., id.* at 2207 (majority opinion).



examination, the separation of powers justification has two distinct constitutional footings—one grounded in Article II and the other in Article III.<sup>206</sup> In recent years, the Court has expanded each, and the net result is an ever-shrinking list of injuries that Congress can make privately enforceable and that federal courts are allowed to entertain.

Start with Article II. *Lujan* held that Congress violated the separation of powers when it attempted to use a citizen-suit provision to handcuff the Executive Branch’s authority to interpret a federal statute.<sup>207</sup> After all, Justice Scalia wrote that “convert[ing] the undifferentiated public interest in executive officers’ compliance with the law into an ‘individual right’” violated Article II’s Take Care Clause.<sup>208</sup> In other words, *Lujan*’s prohibition was relatively modest: do not infringe upon the Executive Branch.

It’s also worth recognizing that *Lujan*’s concern is minimized when Congress enacts a legal right that is adequately particularized: it was the *undifferentiated* public interest in the Executive’s general compliance with the law that doomed the ESA’s citizen-suit provision.<sup>209</sup> In short, outsourcing the interpretation of the law to the public and to the judiciary was the Article II infringement that *Lujan* prohibits.

But in recent years the Court’s standing decisions have added a new and different dimension to the Article II violation, and *TransUnion* supplies a stark example. When a credit-reporting company defames you in violation of a statute, concerns about the Take Care Clause are absent because the Executive Branch isn’t a party to the litigation and its authority to interpret the law isn’t implicated.<sup>210</sup> And yet the Court held

206. See *Allen v. Wright*, 468 U.S. 737, 752, 761 (1984) (discussing Articles II and III as the constitutional basis for the separation of powers explanation of the standing doctrine).

207. See *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 577 (1992).

208. *Id.*

209. See *id.* at 578 (“Nothing in this contradicts the principle that [t]he . . . injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.” (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975))).

210. See, e.g., Jackson Erpenbach, *A Post-Spokeo Taxonomy of Intangible Harms*, 118 MICH. L. REV. 471, 505 (2019) (arguing that “consumer protection cases do not raise concerns of asserting general grievances” because those “suits are filed against private companies and allege conduct as to particular

that “[p]rivate plaintiffs are not accountable to the people and are not charged with pursuing the public interest in enforcing a defendant’s general compliance with regulatory law,” and thus resolving the case “would infringe on the Executive Branch’s Article II authority.”<sup>211</sup> While *Lujan* only prohibited interference, *TransUnion* prohibits usurpation of the Executive Branch’s enforcement authority.

This is an expansion of the prohibition, not just a change in degree, because Congress cannot solve or avoid the problem by adequately personalizing legal rights. The plaintiffs who lost in *TransUnion* had a false OFAC designation placed on their personal credit reports, and the FCRA conferred on them a personal right to accurate information.<sup>212</sup> In the move from interference to usurpation, the Court’s objection shifted from particularization to concreteness.<sup>213</sup>

Now consider Article III. Here too the Court’s justification has shifted and expanded. Few would contest that a congressional authorization for an advisory opinion violates Article III’s requirement of a “judicial” “case” or “controversy.”<sup>214</sup> While the reasoning of 1911’s *Muskrat v. United States*<sup>215</sup> is famously opaque, a plausible interpretation is that Congress’s attempt to authorize a request for an advisory opinion was not a “judicial” case within the meaning of Article III.<sup>216</sup> In other

---

plaintiffs,” and “[t]he executive branch is neither conscripted into action nor relieved of its Take Care Clause duties”).

211. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2207 (2021); *see also* Transcript of Oral Argument at 56–57, *id.* (No. 20-297) (suggesting, in a question by Justice Kavanaugh, that the FCRA constitutes an impermissible attempt by Congress to delegate law enforcement power to private attorneys general).

212. *See TransUnion*, 141 S. Ct. at 2213.

213. *See, e.g., id.* at 2212 (finding that the plaintiffs could not demonstrate that there was a sufficient likelihood of imminent harm and therefore not a serious risk of concrete harm).

214. *See* Sunstein, *supra* note 5, at 179 n.79 (“I do not contend that there are no limits to Congress’ power to decide what is a ‘case’ or ‘controversy.’ In all likelihood, for example, Congress is barred from overcoming the ban on advisory opinions.”).

215. 219 U.S. 346 (1911).

216. *See* William Baude, *Standing in the Shadow of Congress*, 2016 SUP. CT. REV. 197, 206–07, 207 nn.55, 59 (2016).

words, *Muskkrat*'s prohibition was also relatively modest: do not authorize advisory opinions.<sup>217</sup>

Here too, particularization concerns underlie the prohibition. While the statutes in *Muskkrat* explicitly named the parties authorized to sue, the legal right was again little more than an undifferentiated public interest in the proper interpretation of federal law.<sup>218</sup> In recent years, however, the Court's interpretation of Article III's case or controversy requirement has dramatically expanded beyond *Muskkrat*'s modest prohibition. In both *Spokeo* and *TransUnion*, the Court's harping on "concreteness" is a departure from its concern about particularization and injects a limitation on the character of the legal rights that Congress can make privately enforceable.<sup>219</sup> While *Muskkrat* only prohibited advisory opinions, *Spokeo* and *TransUnion* prohibit a vast array of injuries in law.<sup>220</sup>

With both Article II and Article III, the Court's initial concerns and justifications are legitimate. If a proper-party requirement grounded in adverseness is at the heart of standing doctrine, then there is something definitively non-judicial about asking courts "to adjudicate only '[t]he public's nonconcrete interest in the proper administration of the laws.'"<sup>221</sup> But in both cases, the recent expansion of the prohibitions—and the corresponding abandonment of particularization concerns—has eroded their underlying rationales.

*TransUnion* assumes that the Executive Branch has a near monopoly on the enforcement of federal law, but this assumption

217. See *Fairchild v. Hughes*, 258 U.S. 126, 129–30 (1922) (citing *Muskkrat* and holding that an individual citizen does not have a right to institute a judicial proceeding challenging the constitutionality of the proposed Nineteenth Amendment when there was no individual harm alleged).

218. See *Muskkrat*, 219 U.S. at 361 ("[T]here is neither more nor less in this procedure than an attempt to provide for a judicial determination . . . of the constitutional validity of an act of Congress.").

219. See *Spokeo, Inc. v. Robins*, 578 U.S. 330, 334 (2016) (directing courts to consider both the particularity and the concreteness of an alleged injury); *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204–07 (2021) (stating that courts must consider concreteness even where Congress has created "a statutory prohibition or obligation and a cause of action").

220. See, e.g., *TransUnion*, 141 S. Ct. at 2205 ("[U]nder Article III, an injury in law is not an injury in fact.>").

221. Baude, *supra* note 216, at 226–27 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring in part and concurring in the judgment)).

has no grounding in history, text, or common sense: state governments and private parties in both state and federal court have long enforced federal law, so *TransUnion*'s prohibition on usurpation is both novel and groundless.<sup>222</sup> The net effect of *TransUnion* is to funnel litigation that is congressionally authorized but "insufficiently concrete" into state courts.<sup>223</sup> The logical next step is to prohibit the adjudication of federal law in state courts—a breathtakingly ahistorical development.<sup>224</sup>

Similarly, the shifting interpretation of Article III—from prohibiting advisory opinions to prohibiting injuries in law—is startling and has wide-ranging implications. Justice Thomas's *TransUnion* dissent explains that "never before has this Court declared that legislatures are constitutionally precluded from creating legal rights enforceable in federal court if those rights deviate too far from their common-law roots."<sup>225</sup> Following the Court's expansion of Article III's prohibition, "courts alone have the power to sift and weigh harms to decide whether they merit the Federal Judiciary's attention," which "relieve[s] the legislature of its power to create and define rights."<sup>226</sup>

Others have noted the troubling implications of the Court's recent standing jurisprudence. D.C. Circuit Judge Judith W. Rogers has explained, "Standing doctrine preserves the separation of powers by limiting the circumstances in which a private individual may invoke the judicial power to determine the validity of executive or legislative action," but "[s]eparation-of-powers concerns are generally absent . . . when a private party seeks to enforce only his personal rights against

---

222. See generally Margaret H. Lemos, *State Enforcement of Federal Law*, 86 N.Y.U. L. REV. 698 (2011); Tommy Bennett, *The Paradox of Exclusive State-Court Jurisdiction over Federal Claims*, 105 MINN. L. REV. 1211 (2021).

223. See *TransUnion*, 141 S. Ct. at 2224 n.9 (Thomas, J., dissenting).

224. Cf. William A. Fletcher, *The "Case or Controversy" Requirement in State Court Adjudication of Federal Questions*, 78 CALIF. L. REV. 263, 265 (1990) (arguing that state courts should adhere to the Article III case or controversy requirement when adjudicating questions of federal law); Bennett, *supra* note 222, at 1254 ("The first proposal in the scholarly literature is to have state courts follow Article III standing doctrine, at least when adjudicating federal claims.").

225. *TransUnion*, 141 S. Ct. at 2221 (Thomas, J., dissenting).

226. *Id.*

another private party.”<sup>227</sup> Discussing an Eighth Circuit opinion cited with approval in *TransUnion*, William Baude noted that the court has “cast doubt on whether Congress can expand privacy rights beyond their common law scope at all. It is unclear why, in this area, Congress should not be allowed to protect interests beyond those protected by the common law, as it has been allowed in other cases.”<sup>228</sup> And Felix Wu has put a finer point on it: “If government power against private parties is limited by standing doctrine, then the doctrine may be serving deregulatory goals, rather than the separation of powers . . . . Whatever the merits of a deregulatory agenda, that agenda should be established, if at all, through the political process.”<sup>229</sup>

In sum, the Supreme Court has never offered a convincing justification for employing standing doctrine to toss out suits involving particularized injuries brought against private-sector actors. Relying on an opaque and strained interpretation of Articles II and III, the Court has adopted an approach that robs duly elected legislators of their authority to fashion legal rights. Instead of upsetting political consensus about injurious practices, courts should embrace the products of the political process.<sup>230</sup>

### C. *Attempts at Solutions*

Some jurists and scholars have attempted to bring order and clarity to the courts’ standing jurisprudence. This section considers four types of attempted solutions—risk and anxiety, objective versus subjective privacy harms, public and private rights, and deference to the legislature.

#### 1. Risk and Anxiety

Two prominent privacy law scholars, Daniel J. Solove and Danielle Keats Citron, responded to *Clapper* and *Spokeo*’s

---

227. *Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1070 (D.C. Cir. 2019) (Rogers, J., concurring in part and concurring in the judgment) (internal quotation omitted).

228. Baude, *supra* note 216, at 223.

229. Wu, *supra* note 7, at 460.

230. See Ormerod, *Privacy Injuries*, *supra* note 22, at 41 (describing the issues that arise from the Court’s approach in *Spokeo*).

effects in lower-court data-breach cases by positing a two-forked framework for analyzing informational injuries.<sup>231</sup> They observe that “[t]here has been no consistent or coherent judicial approach to data-breach harms,” and that “[m]ore often than not, a plaintiff’s increased risk of financial injury and anxiety is deemed insufficient to warrant recognition of harm, even though the law has evolved in other areas to redress such injuries.”<sup>232</sup>

Solove and Citron survey how courts have recognized the validity of risk and anxiety as legal injuries in other contexts,<sup>233</sup> and they argue that courts should adopt a similar framework in data-breach cases.<sup>234</sup> With respect to risk, they argue that courts “should determine whether a reasonable person would take preventative measures and, if so, assess the harm based on the reasonable cost of such measures.”<sup>235</sup> As for anxiety, “[c]ourts should employ an objective standard, assessing whether a reasonable person would feel anxiety over any unmitigated risk of future injury stemming from a data breach.”<sup>236</sup>

Solove and Citron’s approach illustrates that courts have a tendency to treat privacy harms as exceptional—defying how rules are applied elsewhere in the law.<sup>237</sup> But their approach can’t solve the two problems identified in Part II.B. First, their adoption of an objective standard for both harms does hint at a line-drawing principle, but courts’ recalcitrance in data-breach cases suggests that the standard is of limited utility when reasonable minds differ about the degree of risk created. Second, at least in cases involving common-law claims of negligence, Solove and Citron’s approach sidesteps the most potent separation of powers objections. But in cases involving statutorily-authorized suits against private-sector defendants,

---

231. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 738–45 (2018).

232. *Id.* at 739.

233. *Id.* at 756–73.

234. *See id.* at 774–77.

235. *Id.* at 774; *see id.* at 774–76 (describing the proposed framework to evaluate risk).

236. *Id.* at 774; *see id.* at 776–77 (describing the proposed framework to evaluate anxiety).

237. *See id.* at 773 (describing how both tort and contract cases “recognize the intangible nature of data-breach harms”).

they do not address the underlying structural concern with courts substituting their judgment for the legislature.

Worse, *TransUnion* casts a pall on both sides of their framework. On risk, the Court hints that risk of future injury cannot supply a plaintiff with a concrete injury except when the plaintiff seeks injunctive relief.<sup>238</sup> Because few data-breach victims seek injunctive relief, *TransUnion*'s discussion of risk may imperil plaintiffs who seek damages arising from not-yet-realized data-breach harms. On anxiety, the *TransUnion* majority makes efforts to avoid condemning all psychic injuries, but an unavoidable implication of the Court's dissemination holding is that courts will continue to treat informational injuries as exceptional, given that the Court repeatedly demanded proof about what absent class members knew or thought.<sup>239</sup>

Finally, Solove and Citron's approach—by its own terms—applies only to data-breach cases.<sup>240</sup> While the framework could prove useful in that context, its scope is limited to unauthorized information dissemination cases. Accordingly, their approach leaves unaddressed the standing problems created by other types of injurious uses of information. Risk of and anxiety about identity fraud cannot help in cases that involve, for example, facial recognition harms.

## 2. Objective Versus Subjective Harms

Ryan Calo has argued that privacy harms can be classified into two distinct categories—objective and subjective harms.<sup>241</sup> The subjective category “is the perception of unwanted observation,” and “describes unwelcome mental states—anxiety, for instance, or embarrassment—that accompany the belief that one is or will be watched or monitored.”<sup>242</sup> The objective category “is the unanticipated or

---

238. See *supra* notes 181–182 and accompanying text.

239. See *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2211 n.7 (2021).

240. See Solove & Citron, *supra* note 231, at 745 (focusing on data-breach claims).

241. See M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011).

242. *Id.*

coerced use of information concerning a person against that person,” like selling personal information.<sup>243</sup>

While analytically helpful in taxonomizing distinct types of privacy harms, Calo’s two categories are unavailing in the context of Article III standing. Tasked with using Calo’s categories, a court is likely to analyze objective harms under *Clapper*’s future injury test and will likely regard subjective harms—like Solove and Citron’s anxiety category—as impossible to verify and therefore insufficiently concrete.<sup>244</sup> And here too, *TransUnion* calls into question the Article III sufficiency of both sides of the equation.

### 3. Public and Private Rights

Justice Thomas joined the majority’s opinion in *Spokeo* but filed a separate opinion that lays out his theory of standing.<sup>245</sup> Drawing on scholarship by Anne Woolhandler and Caleb Nelson and by F. Andrew Hessick, Justice Thomas relies on a historical distinction between “public rights” and “private rights” to explain why the Ninth Circuit needed to reassess Robins’s claims.<sup>246</sup>

Public rights are those “that involve duties owed to the whole community, considered as a community, in its social aggregate capacity.”<sup>247</sup> Examples of public rights include “free navigation of waterways, passage on public highways, and general compliance with regulatory law.”<sup>248</sup> Private rights, on the other hand, belong “to individuals, considered as individuals,”<sup>249</sup> and they include “rights of personal security

---

243. *Id.*

244. *Cf. Vance v. Vance*, 408 A.2d 728, 733–34 (Md. 1979) (explaining that recovery for emotional distress requires a “physical injury” and that this requirement was “formulated with the overall purpose in mind of requiring objective evidence to guard against feigned claims”).

245. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 343–49 (2016) (Thomas, J., concurring).

246. *See id.* at 344 (citing Woolhandler & Nelson, *supra* note 49, at 693); *id.* at 347 (citing F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 317–21 (2008)).

247. *Id.* at 345 (internal quotation omitted) (quoting 4 WILLIAM BLACKSTONE, COMMENTARIES \*5 (1769)).

248. *Id.* (citing Woolhandler & Nelson, *supra* note 49, at 693).

249. *Id.* at 344 (quoting 3 WILLIAM BLACKSTONE, COMMENTARIES \*2).



(including security of reputation), property rights, and contract rights.”<sup>250</sup>

Justice Thomas explains that the concrete-injury “requirement applies with special force when a plaintiff files suit to require an executive agency to ‘follow the law.’”<sup>251</sup> On the other hand, “the concrete-harm requirement does not apply as rigorously when a private plaintiff seeks to vindicate his own private rights. Our contemporary decisions have not required a plaintiff to assert an actual injury beyond the violation of his personal legal rights.”<sup>252</sup> In sum, “Congress cannot authorize private plaintiffs to enforce public rights in their own names, absent some showing that the plaintiff has suffered a concrete harm particular to him,” but Congress can “create new private rights and authorize private plaintiffs to sue based simply on the violation of those private rights.”<sup>253</sup>

Justice Thomas nonetheless voted to vacate and remand in *Spokeo*.<sup>254</sup> While the FCRA “creates a series of regulatory duties. . . . owe[d] to the public collectively”—like the “requirement to post a toll-free telephone number on [Spokeo’s] website”—there was “one claim in Robins’ complaint [that] rests on a statutory provision that could arguably establish a private cause of action to vindicate the violation of a privately held right”: the requirement that Spokeo “follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.”<sup>255</sup> “If Congress has created a private duty owed personally to Robins to protect his information,” Justice Thomas concluded, “then the violation of the legal duty suffices for Article III injury in fact.”<sup>256</sup>

Justice Thomas has illustrated his framework three times after *Spokeo*. First, in a case involving allegations that Google disclosed the contents of search queries in violation of the Stored

250. *Id.* (internal quotation omitted) (quoting 3 WILLIAM BLACKSTONE, COMMENTARIES \*1; Woolhandler & Nelson, *supra* note 49, at 693).

251. *Id.* at 346.

252. *Id.* at 347 (citing *Carey v. Piphus*, 435 U.S. 247, 266 (1978)).

253. *Id.* at 348.

254. *See id.*

255. *Id.* at 348–49 (internal quotation marks omitted) (second brackets in original) (quoting 15 U.S.C. § 1681e(b)).

256. *Id.* at 1553 (emphasis omitted).

Communications Act,<sup>257</sup> Justice Thomas explained that the statute “creates a private right” because it “prohibits certain electronic service providers from knowingly divulging the contents of a communication sent by a user . . . of the service.”<sup>258</sup> This “established standing” because the plaintiffs “alleg[ed] the violation of private duties owed personally to them as individuals.”<sup>259</sup>

Second, in *Thole v. United States Bank*<sup>260</sup>—a case involving allegations that a bank violated fiduciary duties under the Employment Retirement Income Security Act (ERISA)<sup>261</sup>—Justice Thomas explained that the statute did not create any private rights that belonged to the participants in a defined-benefit plan: “[N]one of the rights identified by petitioners belong to them. The fiduciary duties created by ERISA are owed to the plan, not petitioners.”<sup>262</sup> Specifically, as “participants in a defined benefit plan, petitioners ha[d] no legal or equitable ownership interest in the plan assets,” and there had “been no assignment of the plan’s rights by ERISA or any contract.”<sup>263</sup>

Third, Justice Thomas authored the principal dissent in *TransUnion*, and his opinion answers several important questions about his interpretation of the public/private rights framework. On the narrow question about the FCRA left unresolved in *Spokeo*, Justice Thomas concluded that the statute creates several private rights.<sup>264</sup> With regard to inaccurate disseminations, the FCRA “creates a duty: to use reasonable procedures to assure maximum possible accuracy. And that duty is particularized to an individual: the subject of

---

257. 18 U.S.C. §§ 2701–2712.

258. *Frank v. Gaos*, 139 S. Ct. 1041, 1047 (2019) (Thomas, J., dissenting) (internal quotation omitted) (quoting 18 U.S.C. §§ 2510(13), 2702(a)(1)–(2), (b)).

259. *Id.* (internal quotation omitted) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 349 (2016) (Thomas, J., concurring)).

260. 140 S. Ct. 1615 (2020).

261. Pub. L. No. 93-406, 88 Stat. 829 (1974).

262. *Thole*, 140 S. Ct. at 1623 (Thomas, J., concurring).

263. *Id.*

264. See *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2218 (2021) (Thomas, J., dissenting).

the report.”<sup>265</sup> The same was true, he says, about the information access rights.<sup>266</sup>

But the opinion also resolves a broader question. *Spokeo* produced uncertainty about how restrictive or permissive Justice Thomas’s framework would prove.<sup>267</sup> William Baude argued that a restrictive answer would wed Congress’s authority to only four specific forms (property, contract, tort, privilege);<sup>268</sup> a more permissive answer seems to jettison the concreteness inquiry entirely, requiring only that a private right be “adequately personalized—owed to a specific person or group of persons rather than to the public at large.”<sup>269</sup> Justice Thomas’s *TransUnion* opinion endorses the permissive version: he critiques the majority’s decision as mandating that, “[n]o matter if the right is personal or if the legislature deems the right worthy of legal protection, legislatures are constitutionally unable to offer the protection of the federal courts for anything other than money, bodily integrity, and anything else that this Court thinks looks close enough to rights existing at common law.”<sup>270</sup> While Justice Thomas’s *Spokeo* opinion laid the foundation for a more aggressive role for the judiciary,<sup>271</sup> his *TransUnion* opinion criticizes the majority’s disrespect for the democratic process.<sup>272</sup>

Justice Thomas’s framework—particularly as refined in his *TransUnion* dissent—is responsive to both of the problems

265. *Id.*

266. *See id.* (discussing 15 U.S.C. § 1681g(a), (c)(2)).

267. *See* Baude, *supra* note 216, at 230.

268. *See id.* at 231 (discussing *Tenn. Elec. Power Co. v. TVA*, 306 U.S. 118 (1939)); *see also* *Tenn. Elec. Power Co. v. TVA*, 306 U.S. 118, 137–38 (1939) (suggesting that a private legal right must be “a legal right,—one of property, one arising out of contract, one protected against tortious invasion, or one founded on a statute which confers a privilege”).

269. Baude, *supra* note 216, at 231.

270. *TransUnion*, 141 S. Ct. at 2221 (Thomas, J., dissenting).

271. *See* *Spokeo, Inc. v. Robins*, 578 U.S. 330, 347 (2016) (Thomas, J., concurring) (“[B]y limiting Congress’ ability to delegate law enforcement authority to private plaintiffs and the courts, standing doctrine preserves executive discretion.”).

272. *See* *TransUnion*, 141 S. Ct. at 2221 (Thomas, J., dissenting) (“According to the majority, courts alone have the power to sift and weigh harms to decide whether they merit the Federal Judiciary’s attention. In the name of protecting the separation of powers, this Court has relieved the legislature of its power to create and define rights.” (citation omitted)).

identified in Part II.B. As to the line-drawing problem, Justice Thomas obviates distinctions between sufficiently and insufficiently concrete injuries.<sup>273</sup> And Justice Thomas’s vociferous criticism of the *TransUnion* majority is rooted in concerns about usurping legislatures’ authority to shape and create new legal rights.<sup>274</sup>

There are, nonetheless, two shortcomings with Justice Thomas’s framework. The first is the most obvious: a majority of the Court has now rejected the permissive version of the public/private rights framework. Given that Justice Gorsuch joined Justice Thomas’s opinion in *Thole*, Justice Gorsuch may be receptive to the more restrictive version of the public/private rights approach.<sup>275</sup> But as the framework becomes increasingly restrictive—and as it thereby limits Congress’s discretion to create and shape new legal rights—the framework’s responsiveness to the line-drawing and counter-majoritarian problems wanes.

Second, it’s not clear what difference—if any—there is between a private right and a particularized right. *TransUnion* suggests there is no difference—that Congress’s adequate personalization of a legal right makes the right a private one.<sup>276</sup> But *Thole* suggests that there *is* some daylight between private rights and particularized rights.<sup>277</sup> ERISA authorizes participants in defined-benefit plans to sue for violations of the

---

273. See *Spokeo*, 578 U.S. at 346–47 (Thomas, J., concurring) (discussing concreteness in relation to public and private rights); *TransUnion*, 141 S. Ct. at 2219 (Thomas, J., dissenting)

Rejecting this history, the majority holds that the mere violation of a personal legal right is *not*—and never can be—an injury sufficient to establish standing. What matters for the Court is only that the “injury in fact be ‘concrete.’” “No concrete harm, no standing.” That may be a pithy catchphrase, but it is worth pausing to ask why “concrete” injury in fact should be the sole inquiry. (citations omitted)

274. See *supra* note 272 and accompanying text.

275. See *Thole v. U.S. Bank N. Am.*, 140 S. Ct. 1615, 1622–23 (2020) (Thomas, J., concurring) (joined by Gorsuch, J.).

276. See *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2220 (2021) (Thomas, J., dissenting) (“A statute that creates a private right and a cause of action, however, does give plaintiffs an adequate interest in vindicating their private rights in federal court.”).

277. See *Thole*, 140 S. Ct. at 1623 (indicating that even though a private cause of action is allowed, it is not available in the particular case).

statute, which therefore differentiates between those authorized to sue (participants, among others) and the public at large.<sup>278</sup>

In other words, Justice Thomas’s implementation of the public/private rights framework can produce arbitrary outcomes—sometimes respecting the democratic process and sometimes not. Recall that the advisory opinions ban is only implicated when plaintiffs have an undifferentiated interest in regulatory compliance.<sup>279</sup> Does anyone really think that ERISA authorizes advisory opinions but that the FCRA doesn’t? By differentiating between the public and plan participants, Congress adequately particularized the ERISA rights.<sup>280</sup> Empowering plan participants to hold self-dealing trustees liable doesn’t constrain the Executive or call for an advisory opinion, so it’s difficult to reconcile Justice Thomas’s *TransUnion* opinion with his approach in *Thole*.

#### 4. Deference to the Legislature

Several commentators have sought to address problems with the Court’s standing jurisprudence by emphasizing the importance of deferring to the legislature’s choice to make a right privately enforceable.

Cass Sunstein, for example, has argued that strict limits on Congress’s standing authority are akin to substantive due process: both “use[] highly contestable ideas about political theory to invalidate congressional enactments, even though the relevant constitutional text and history do not call for invalidation at all.”<sup>281</sup> Relatedly, William Baude has advanced a “more nuanced and sympathetic” version of the analogy.<sup>282</sup> Both substantive due process and limits on Congress’s standing authority begin with uncontroversial propositions but can quickly end up in deeply contested waters. It “might have been satisfying to conclude that standing limitations do not apply to

---

278. See 29 U.S.C. § 1132(a) (permitting plan participants, beneficiaries, and others specifically defined to bring a civil action against those violating the statute).

279. See *supra* notes 214–219 and accompanying text.

280. See *Thole*, 140 S. Ct. at 1625–26 (Sotomayor, J., dissenting) (discussing how plan beneficiaries have a private interest in the plan’s financial integrity).

281. Sunstein, *supra* note 5, at 167.

282. Baude, *supra* note 216, at 224.

the legislature at all—but that would suggest that Congress could even go so far as to authorize federal courts to issue advisory opinions, whose illegality is supposedly one of the paradigm rules of Article III.<sup>283</sup> But procedural legal rights, Baude says, raise similar problems as advisory opinions—“the possibility of courts being asked to adjudicate only the public’s nonconcrete interest in the proper administration of the laws.”<sup>284</sup> In sum, “once courts have started invalidating such statutory rights, it is easy to see how they might keep going.”<sup>285</sup>

In past work, I have argued that informational injuries deserve particular deference.<sup>286</sup> To prevent *Spokeo* and its progeny from gutting privacy law, I have argued that the federal courts “should give binding deference to Congress’s decision to make an injury privately enforceable when three conditions are met: when the plaintiff alleges an informational injury; when the defendant is a private-sector actor; and when Congress has effectively personalized the injury and the plaintiff is among the injured.”<sup>287</sup> The first condition recognizes the inherent difficulties in assessing the “concreteness” of an informational injury, while the second and third conditions rebut separation of powers objections by constraining deference to private-sector defendants and by using particularization to avoid concerns about advisory opinions.<sup>288</sup>

While deference to the legislature blunts the problems outlined in Part II.B, these approaches have their own issues. Approaches that emphasize deference address both the line-drawing and separation of powers problems by removing line-drawing authority from the courts altogether, instead empowering the legislature. But as Baude highlights, it’s not true that the courts have no role in statutory standing cases—the “rule that all federal legal rights can be vindicated in federal court has been replaced with a judicial limitation on which legal rights are sufficiently real to be judicially

---

283. *Id.* at 226.

284. *Id.* at 227 (internal quotation marks and brackets omitted) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring in part and concurring in the judgment)).

285. *Id.*

286. *See generally* Ormerod, *Privacy Injuries*, *supra* note 22.

287. *Id.* at 137–38.

288. *See id.* at 149–64.

enforced.”<sup>289</sup> So allowing any role for the courts introduces the same line-drawing problem that we’re seeking to solve.

In any event, the Supreme Court has evinced no interest in deferring questions of standing to the legislature, and there’s no reason to believe *TransUnion* will be the last word on the matter.

\* \* \*

This Part diagnosed two significant problems with the Supreme Court’s recent Article III standing jurisprudence and illustrated the shortcomings with proposed solutions to these and related problems. The next Part begins laying the groundwork for a new solution.

### III. PRIVACY AS CONTEXTUAL INTEGRITY

Perhaps the simplest approach to privacy is the secrecy paradigm: only that which is secret may be considered private. But decades of scholarship have revealed the incoherency and inadequacy of privacy-as-secrecy.<sup>290</sup> Among the most convincing and influential responses to binary privacy is Helen Nissenbaum’s contextual integrity framework—the simple but profound observation that “a right to privacy is neither a right to secrecy nor a right to control but a right to *appropriate* flow of personal information.”<sup>291</sup>

This Part first describes Nissenbaum’s contextual integrity framework and then highlights its limits. Doing so supplies the tools for forging a legal framework in Part IV that solves the current problems with the Court’s informational-injury standing cases.

#### A. *A Contextual Integrity Primer*

Nissenbaum’s seminal work on contextual integrity begins with dual observations—that information technology holds immense power over us and that prevailing approaches to

---

289. Baude, *supra* note 216, at 227.

290. See, e.g., DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 23 (2008) (“The privacy-as-secrecy conception fails to recognize that individuals want to keep things Private from some people but not others.”); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 22–24 (2018) (identifying three fundamental problems with the secrecy paradigm).

291. NISSENBAUM, *supra* note 29, at 127.

privacy provide unsatisfactory answers to these threats.<sup>292</sup> Most prominently, Nissenbaum argues against several different conceptions of a public/private dichotomy: “Approaches to privacy that restrict its sphere of legitimacy to the private . . . are founded on a set of assumptions about the relationship between privacy and the public/private dichotomy that ultimately are incoherent.”<sup>293</sup> There are, she says, “no actors, no spheres, no information that can be assigned unconditionally to the domain of the public, free of all and any constraints imposed by rights of privacy; none are ‘up for grabs.’”<sup>294</sup>

Nissenbaum’s solution begins with the insight that “[w]hat people care most about is not simply *restricting* the flow of information but ensuring that it flows *appropriately*.”<sup>295</sup> The framework of contextual integrity “makes rigorous the notion of appropriateness” by looking to context-relative informational norms.<sup>296</sup> “When these norms are contravened,” she explains, “we experience this as a violation of privacy.”<sup>297</sup> In short, contextual integrity “is defined in terms of informational norms: it is preserved when informational norms are respected and violated when informational norms are breached.”<sup>298</sup>

Contextual integrity has a descriptive component and a normative component. The descriptive component is a heuristic that speaks to whether a given informational practice violates privacy. Nissenbaum explains that context-relative informational norms have four key parameters: contexts, actors, attributes, and transmission protocols.<sup>299</sup> Together, these parameters “prescribe, for a given context, the type of information, the parties who are the subjects of the information as well as those who are sending and receiving it, and the principles under which this information is transmitted.”<sup>300</sup>

---

292. *See id.* at 19–64, 65–126.

293. *Id.* at 125–26.

294. *Id.* at 126.

295. *Id.* at 2.

296. *Id.* at 127.

297. *Id.*

298. *Id.* at 140.

299. *Id.*

300. *Id.* at 141.



*Contexts:* Nissenbaum defines contexts as “structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes).”<sup>301</sup> Throughout, she references several straightforward examples of contexts, including “a grade school in an educational context; a hospital in a healthcare context; [and] a department store in a commercial marketplace.”<sup>302</sup> Other examples raise harder definitional questions.<sup>303</sup>

*Actors:* There are three relevant types of actors: senders of information, recipients of information, and information subjects.<sup>304</sup>

*Attributes:* Attributes ask about the type of information being transmitted.<sup>305</sup> “In a healthcare context . . . strictures on information flow vary according to roles and . . . type of information . . . whether it be patients’ medical conditions, their attire, their addresses and phone number, the name and code number of their health insurance carrier, or the balance on their accounts.”<sup>306</sup>

*Transmission Protocols:* A transmission protocol, Nissenbaum explains, “is a constraint on the flow . . . of information from party to party in a context.”<sup>307</sup> Examples of transmission protocols include: confidentiality, which prohibits an information recipient from sharing the information with others; reciprocity, which requires bidirectional information flows; desert, which provides that an actor deserves to receive information; and compulsion, which provides that one party is compelled or mandated to reveal information to another.<sup>308</sup>

With these four parameters of norms in hand, Nissenbaum explains how to employ them to identify privacy violations: first, establish the prevailing context; second, identify key actors; third, ascertain what attributes are affected; and fourth,

---

301. *Id.* at 132.

302. *Id.* at 149.

303. *See, e.g., id.* (“Should one tell one’s friend her spouse is having an affair? . . . Should a hospital share injury records with police officers?”).

304. *Id.* at 141–43.

305. *Id.* at 143.

306. *Id.*

307. *Id.* at 145.

308. *Id.*

establish changes in transmission principles.<sup>309</sup> “If the new practice generates changes in actors, attributes, or transmission principles, the practice is flagged as violating entrenched informational norms and constitutes a prima facie violation of contextual integrity.”<sup>310</sup>

Nissenbaum’s framework also has a normative dimension. She explains that, aside from describing and predicting reactions, contextual integrity can serve as a prescriptive guide—telling us which novel informational practices should be regarded as acceptable.<sup>311</sup> The normative component compares “entrenched normative practices against novel alternatives . . . on the basis of how effective each is in supporting, achieving, or promoting relevant contextual values.”<sup>312</sup>

In other words, we ask about *why* information is flowing in a certain way and evaluate whether changes to that flow are in furtherance of the purposes and values of the relevant context. For example, consider a company’s desire to access its employees’ medical records.<sup>313</sup> Nissenbaum explains, “even if a general cost-benefit analysis or a comparison and trade-off of interests indicates in favor of employers, the analysis via contextual integrity would most likely prohibit release of medical information to employers under the assumption that benefits accrued by employers are irrelevant to the attainment of healthcare goals.”<sup>314</sup> In contrast, imagine a person’s desire to access the medical records of a romantic partner.<sup>315</sup> “In the case of lovers, however, what is known of sexually transmitted diseases suggests there might be conditions under which sexual partners may have a right to limited access to each other’s medical records even without permission from the subject,” because doing so furthers the purposes, goals, and values of the healthcare context.<sup>316</sup>

---

309. *Id.* at 149–50.

310. *Id.* at 150.

311. *Id.*

312. *Id.* at 166.

313. *See id.* at 172 (outlining this hypothetical situation).

314. *Id.*

315. *See id.* (setting up this scenario).

316. *Id.*

In sum, Nissenbaum explains, the right to privacy is “a right to live in a world in which our expectations about the flow of personal information are, for the most part, met,” and her contextual integrity framework both describes and prescribes appropriate informational flows “through the harmonious balance of social rules, or norms, with both local and general values, ends, and purposes.”<sup>317</sup>

### B. *Contextual Integrity’s Limits and Shortcomings*

Nissenbaum’s contextual integrity framework is a powerful tool for capturing the key insight that privacy is context specific. But the framework is not without inherent limits and shortcomings—particularly when employed as a legal standard. Most significantly, Nissenbaum’s framework is philosophical and moral in nature, not legal. Attempting to fashion Nissenbaum’s philosophical and moral framework into a legal test is difficult.

Other scholars have noted this difficulty. For example, Dennis Hirsch has evaluated the utility of contextual integrity while addressing harms from predictive analytics.<sup>318</sup> Hirsch first explains contextual integrity’s descriptive force regarding predictive analytics.<sup>319</sup> But the normative component is necessary, Hirsch says, because norms and technology change.<sup>320</sup> In other words, contextual integrity “must identify a way to distinguish norm-breaking data practices that are legitimate and acceptable[] from those that are not.”<sup>321</sup> “Data

317. *Id.* at 231.

318. See Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 468–71 (2020) (noting that Nissenbaum and other scholars leaned on contextual integrity because “notice, consent, and the other elements of the control paradigm do not protect people sufficiently from the harms of predictive analytics”). Hirsch defines predictive analytics as “a technological process that analyzes surface data in order to infer and act on the latent information that lies beneath the surface.” *Id.* at 441–42.

319. See *id.* at 469 (“Business use of predictive analytics that accords with . . . context-specific norms is presumptively appropriate; that which does not . . . is presumptively inappropriate.”).

320. *Id.*

321. *Id.* (citing Helen Nissenbaum & Solon Barocas, *Big Data’s End Run Around Anonymity and Consent*, in *PRIVACY, BIG DATA, AND THE PUBLIC GOOD* 44, 47 (Julia Lane et al. eds., 2014)).

practices that transgress informational norms are permissible where they are ‘more effective in promoting interests, general moral and political values, and context-specific ends, purposes, and values’ such as ‘fairness, justice, freedom, autonomy, [and] welfare’ . . . than those practices that comply with existing informational norms.”<sup>322</sup>

Hirsch takes issue with the normative component of the analysis: A test that relies on evaluating values like fairness, justice, freedom, autonomy, and so forth “is so vague as to be almost unworkable. Which . . . values is one to consider? . . . And who is to say that Nissenbaum and [her coauthor Solon] Barocas have even arrived at the right list?”<sup>323</sup> Further, Hirsch argues, there is an additional layer of difficulty in ascertaining “whether the data practice in question would further these values better than alternative practices that are consistent with existing informational norms.”<sup>324</sup>

In a related vein, Nissenbaum’s framework—by its own terms—is directed toward a specific type of problem: evaluating how technological change and novel information flows violate entrenched norms.<sup>325</sup> Employing it as a legal test applies the framework to different ends—evaluating, instead, whether a defendant’s informational practices have injured the plaintiff.

A second and related limit to contextual integrity—at least when employed as a legal test—is its indeterminacy. The framework has a tendency toward complexity, requiring the identification of five distinct criteria (context, actors, attributes, transmission protocols, and purpose) before a decisionmaker can evaluate whether a norm has been and should be transgressed.<sup>326</sup> And even then, the framework only sometimes provides definite answers.<sup>327</sup>

---

322. *Id.* (quoting Helen Nissenbaum & Solon Barocas, *Big Data’s End Run Around Anonymity and Consent*, in *PRIVACY, BIG DATA, AND THE PUBLIC GOOD* 44, 48 (Julia Lane et al. eds., 2014)).

323. *Id.* at 470.

324. *Id.* at 471.

325. See NISSENBAUM, *supra* note 29, at 21 (laying the background of technological changes and the corresponding impact on “human social activities” before applying the proposed contextual integrity framework).

326. See, e.g., *id.* at 140–47 (detailing each individual criterion at the beginning of the discussion of the contextual integrity framework).

327. The examples related to accessing medical records, *supra* notes 313–316, provide an apt illustration of indeterminacy. “[E]ven if a general

As a philosophical tool, this indeterminacy may not be a problem, but judges, legislatures, and litigants crave rules with clearly right and clearly wrong answers.<sup>328</sup> If contextual integrity has value as a legal test, it must provide clear and straightforward answers to legal questions.

A final pair of shortcomings are related to contextual integrity's explicit reliance on past practice. As Nissenbaum puts it, the descriptive component of contextual integrity "is inherently conservative, flagging as problematic any departure from entrenched practice."<sup>329</sup> To be sure, the framework's normative dimension is intended to combat the descriptive component's inherent conservativeness.<sup>330</sup> By marrying contextual integrity's descriptive and normative components, "there is a presumption in favor of entrenched rules rather than strict adherence to the letter that can be overridden if new practices are demonstrably more effective at achieving contextual values, ends, and purposes."<sup>331</sup>

But as a legal test, the backward-looking nature of contextual integrity raises a problem familiar to privacy law scholars—endogeneity.<sup>332</sup> After all, entrenched informational norms are at least partly dictated by existing legal rules about

---

cost-benefit analysis or a comparison and trade-off of interests indicates in favor of employers, the analysis via contextual integrity would *most likely* prohibit release of medical information to employers." NISSENBAUM, *supra* note 29, at 172 (emphasis added). "In the case of lovers, however, what is known of sexually transmitted diseases suggests there *might be* conditions under which sexual partners *may* have a right to limited access." *Id.* (emphasis added).

328. See, e.g., Jeremy Waldron, *Judges as Moral Reasoners*, 7 INT'L J. CONST. L. 2, 13 (2009) (inferring that bright-line rules are easiest to apply, but not without their own challenges: "even when they are finding and applying clear law—clear statutes, the clear provisions of a constitution, or clear precedents obviously on point—judges are not machines").

329. NISSENBAUM, *supra* note 29, at 161.

330. See *id.* (noting that contextual integrity is a "normative approach to privacy," and with that is "a keener measure of morally relevant change than other predominant approaches").

331. *Id.* at 179.

332. See, e.g., Lauren B. Edelman et al., *The Endogeneity of Legal Regulation: Grievance Procedures as Rational Myth*, 105 AM. J. SOCIO. 406, 407 (1999) (explaining that endogeneity occurs in the legal setting because "the content and meaning of law is determined within the social field that it is designed to regulate").

permissible and impermissible information flows.<sup>333</sup> So contextual integrity as a legal rule simultaneously looks to past practice to define what is acceptable and itself defines what is acceptable.

The endogeneity of privacy expectations sometimes arises with the reasonable expectation of privacy test from *Katz v. United States*.<sup>334</sup> If people reasonably expect that the government will not eavesdrop on their phone conversations, from where does that expectation originate? Surely not on past practice since most wiretaps did not violate the Fourth Amendment before *Katz*.<sup>335</sup>

In some Fourth Amendment cases, the Court ignores expectations or insists they're irrelevant, but other cases turn on the Court's sense of popular expectations about privacy.<sup>336</sup> The net result is circularity: "[R]easonable people should expect the privacy rights granted to them by the courts. So expectations define the scope of the legal protection, but the legal protections themselves should define the expectations."<sup>337</sup> In short, "individual 'expectations of privacy' . . . are not . . . exogenous variables; rather, they are significantly shaped by the law itself."<sup>338</sup>

---

333. See *supra* notes 309–310 and accompanying text (providing the example of how entrenched informational norms interact with privacy violations).

334. 389 U.S. 347 (1967).

335. See, e.g., *Olmstead v. United States*, 277 U.S. 438, 466 (1928) ("The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment.").

336. See Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747, 1756 nn.27–28 (2017) [hereinafter Kugler & Strahilevitz, *The Myth*] (detailing Supreme Court decisions that use "employees' expectations . . . to determine the scope of the Fourth Amendment," in contrast with other decisions that "treat popular expectations as irrelevant").

337. *Id.* at 1750; see also *infra* Part V.B. But cf. Kugler & Strahilevitz, *The Myth*, *supra* note 336, at 1176–94 (using empirical evidence to argue that circularity is a myth).

338. Perry Dane, *A Tale of Two Clauses: Search and Seizure, Establishment of Religion, and Constitutional Reason*, 26 WM. & MARY BILL RTS. J. 939, 961 (2018).

Similarly, if informational norms are shaped by what courts and legislatures define as acceptable and unacceptable, over time contextual integrity becomes self-referential, and the primary justification for an informational practice is that it has been deemed acceptable in the past.

\* \* \*

With this understanding of contextual integrity in hand, the next Part proposes a legal framework for assessing whether a plaintiff alleging an informational injury has suffered a concrete and particularized Article III injury in fact.

#### IV. CONTEXTUAL INTEGRITY AS A LEGAL FRAMEWORK FOR ARTICLE III INJURIES

Contextual integrity's insight that privacy is context specific and governed by context-relative informational norms supplies a foundation for assessing whether a plaintiff alleging an informational injury has suffered an injury in fact. This Part builds on that foundation by fashioning a legal framework for Article III standing based on contextual integrity and by illustrating how to use it.

##### A. *Constructing the Legal Framework*

The central contribution of this framework is that the breach of an informational norm supplies the plaintiff with a concrete injury in fact. When a statute protects a norm and the defendant contravenes the statute and the norm, the plaintiff has a concrete injury. When, instead, a statute authorizes a suit for an informational practice, but the defendant has not contravened an informational norm, the plaintiff lacks a concrete injury in fact.

The legal framework for assessing which informational injuries create a concrete injury in fact therefore has two steps. First, the reviewing court should identify the defendant's acts or practices that the plaintiff is contesting and determine which of the four informational injuries the plaintiff is alleging. Second, the reviewing court should identify whether the contested acts or practices contravene an entrenched informational norm. If so, then the defendant's breach of both the statute and the norm supplies the plaintiff with a concrete injury in fact. If the defendant has only violated the statute—but there has been no

breach of an entrenched informational norm—then the plaintiff must provide some additional basis for invoking the jurisdiction of the federal courts.

### 1. Identify the Injury

The first step of the analysis requires the reviewing court to assess the statutory provision on which the plaintiff's cause of action relies. As detailed in Part I.B, there are four types of informational injuries—collecting, using, disseminating, and withholding. The court's task is to evaluate the allegations in the plaintiff's complaint and determine which one or more injuries are alleged. This analysis should proceed on an allegation-by-allegation basis, isolating each of the plaintiff's theories of injury and each of the defendant's acts or practices the plaintiff contests. Perhaps the plaintiff avers that the defendant collected information in violation of the statute and then proceeded to disseminate the information to third parties also in violation of the statute.<sup>339</sup> The court should assess the collection injury and the dissemination injury separately.

Information collection and dissemination injuries present the most straightforward cases. Information use cases may be more complex because of the myriad injurious ways to use information.<sup>340</sup> Consider, for example, a case involving claims that a social networking company illegally created a facial recognition scan and then used the scan to help tailor advertising. Such a case has two different information use harms: using photos to create the prohibited facial recognition scan is one information use injury and using the scan to tailor and serve advertising is a second information use injury.

Information withholding cases may seem peculiar but should be easy to identify because of their specific set of facts—has information been withheld from a plaintiff that is legally entitled to it? If so, it's safe to assume that the allegation is information withholding.

---

339. See, e.g., *Bartnicki v. Vopper*, 532 U.S. 514, 519 (2001); see also *supra* notes 80–88, 98–101 and accompanying text.

340. See *supra* notes 89–91 and accompanying text.



## 2. Identify the Norm

The second step of the analysis requires the reviewing court to identify which informational norms, if any, the defendant has breached. For each statutory violation that also violates a norm, the plaintiff has a concrete injury in fact. But for each statutory violation that does not violate an entrenched informational norm, the plaintiff must allege more to satisfy the strictures of Article III.

Evaluating the relationship between a statute and an informational norm will often prove helpful. Sometimes a legislature enacts a law that codifies a preexisting informational norm. For example, when Congress first enacted the Wiretap Act in 1968, it codified a preexisting norm against the collection and dissemination of phone conversations.<sup>341</sup> Sometimes a legislature enacts a law that—over time—helps establish a new informational norm. For example, when Congress enacted the Stored Communications Act (and amended the Wiretap Act) in 1986, it helped establish a new informational norm against the collection and dissemination of email content.<sup>342</sup>

In both norm-codification and norm-establishment cases, the fact that a plaintiff alleges a violation of both a statute and a norm is a sufficient basis for invoking the jurisdiction of the federal courts. Only in situations where a statute does not protect an informational norm will a plaintiff need something more. Take the *Spokeo* majority's discussion of disseminating an incorrect zip code in violation of the Fair Credit Reporting Act.<sup>343</sup> Congress helped establish many new informational norms when it enacted the FCRA in 1970, but few people would regard the dissemination of an incorrect zip code as breaching an entrenched informational norm.<sup>344</sup> Hence, the plaintiff in the incorrect-zip-code case will need to show something other than the statutory violation to satisfy Article III—perhaps disseminating an incorrect zip code had some other downstream

---

341. For a more thorough discussion of the Wiretap Act, see *infra* Part IV.B.1.

342. For a more thorough discussion of the Stored Communications Act, see *infra* Part IV.B.1.

343. See *Spokeo, Inc. v. Robins*, 578 U.S. 330, 342 (2016).

344. For a more thorough discussion of the Fair Credit Reporting Act, see *infra* Part IV.B.2.

effects, like increasing the plaintiff's borrowing costs or excluding the plaintiff from prospective employment.<sup>345</sup> The framework thus offers a sufficient basis for demonstrating an injury in fact, but it doesn't operate to the exclusion of other grounds for satisfying Article III.

Identifying entrenched informational norms won't always be easy. In close or convoluted cases, courts should analyze the parameters from Nissenbaum's descriptive component: identifying the context, actors, information type, and expectations should clarify the existence or absence of an informational norm.

### B. *Using the Framework*

With a description of the legal framework in hand, this section now illustrates how to use the framework. The authorities covered in this section include privacy laws large and small—spanning federal and state, privately and publicly enforceable, settled and proposed.

#### 1. Authorities that Always or Usually Create an Injury in Fact

This section reviews a host of legal authorities that always or almost always protect entrenched information norms. As a result, plaintiffs that allege violations of these statutes should usually have a concrete injury in fact.

The Wiretap Act (WTA) is an apt example of a statutory prohibition on collecting and disseminating information that protects entrenched informational norms.<sup>346</sup> Violations of the WTA's prohibition are thus per se concrete Article III injuries in fact.

The WTA punishes any person who intentionally intercepts or intentionally discloses any wire, oral, or electronic communication.<sup>347</sup> Congress first enacted this prohibition in

---

345. See *infra* note 400 and accompanying text.

346. See 18 U.S.C. § 2511(1) (banning the interception or use of certain “wire, oral, or electronic communication”).

347. *Id.*

1968,<sup>348</sup> shortly after and in response to the Supreme Court's decisions in *Berger v. New York*<sup>349</sup> and *Katz v. United States*.<sup>350</sup>

Before *Katz*, the Supreme Court had held in 1928's *Olmstead v. United States*<sup>351</sup> that intercepting a suspect's telephone conversations to obtain evidence of a crime didn't trigger the Fourth Amendment absent a physical intrusion on the suspect's constitutionally protected property.<sup>352</sup> The Court nonetheless "implied that Congress could enact legislation to protect the secrecy of telephone messages by making them inadmissible in federal criminal trials."<sup>353</sup> The *Olmstead* decision "was greeted with little charity," and "[t]he widely felt adverse reaction may have been responsible in part for the passage of the Federal Communications Act<sup>354</sup> some seven years later."<sup>355</sup> Section 605 of that law "prohibited the interception and divulgence in federal trials of evidence obtained through wiretapping," and after its enactment "cases involving the use of wiretapping, whether by federal or state officials, were disposed of under this section."<sup>356</sup> In a series of decisions interpreting section 605, "the Court in effect poured the Fourth Amendment into the Federal Communications Act."<sup>357</sup> A commentator in 1965 explained that "although the Court was chary of broadly defining the fourth amendment to restrict eavesdropping, it was equally reluctant to allow unrestricted

348. See Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 213 (1968).

349. 388 U.S. 41, 63 (1967).

350. See Pub. L. No. 90-351, 82 Stat. 197, 211–12 (discussing the need for the prohibition).

351. 277 U.S. 438 (1928).

352. See *id.* at 464 (contrasting the interception of a telephone conversation with a sealed letter in the mail, the latter of which would be protected from "unlawful rifling by a government agent").

353. Mary E. Bisantz, *Electronic Eavesdropping Under the Fourth Amendment—After Berger and Katz*, 17 BUFF. L. REV. 455, 457 (1968).

354. Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified as amended 47 U.S.C. §§ 151–646).

355. Minn. L. Rev. Ed. Bd., *Eavesdropping and the Constitution: A Reappraisal of the Fourth Amendment Framework*, 50 MINN. L. REV. 378, 388 (1965).

356. Bisantz, *supra* note 353, at 458.

357. Minn. L. Rev. Ed. Bd., *supra* note 355, at 388 (quoting Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 COLUM. L. REV. 165, 177 (1952) (internal quotation marks omitted)).

eavesdropping outside the boundaries of fourth amendment protection.”<sup>358</sup>

State tort law evolved concurrently to recognize a civil cause of action against wiretapping.<sup>359</sup> Taken together, there can be little dispute that—by the time the Court reversed *Olmstead* in 1967<sup>360</sup>—there was a widespread informational norm against intercepting phone conversations. When Congress enacted the WTA in 1968, it therefore codified that norm. As a result, when a plaintiff alleges a violation of the WTA, the plaintiff will typically have a concrete injury.

The Stored Communications Act (SCA) prohibits “obtain[ing] . . . a wire or electronic communication” without authorization.<sup>361</sup> This prohibition “has been interpreted over the years to cover the content of emails, private Facebook messages, [and] YouTube videos,” among other types of information.<sup>362</sup> Congress enacted the SCA in 1986—“at the infancy of the Internet”—in an attempt to extend the WTA’s protections to new digital forms of communication.<sup>363</sup>

As noted, the WTA lagged far behind the public’s widespread use of the telephone—and consequently, far behind the public’s conception of telephonic privacy. Like the WTA, the SCA protects an entrenched informational norm against intercepting and disclosing communicative content, and therefore violations of the SCA constitute concrete injuries.

Courts that have considered whether interceptions that violate the SCA create concrete injuries have agreed that they do. The Ninth Circuit recently explained that Facebook’s interception of the content of user communications violated the amended WTA and the SCA, and held that the statutes “codify a context-specific extension of the *substantive* right to

---

358. *Id.* at 388–89.

359. See William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 390 (1960) (noting the law’s evolution beyond protection of physical intrusions) (citing *Rhodes v. Graham*, 37 S.W.2d 46 (Ky. 1931)).

360. See *Katz v. United States*, 389 U.S. 347, 353 (1967) (partially overruling *Olmstead*).

361. 18 U.S.C. § 2701(a).

362. RICHARD M. THOMPSON II & JARED P. COLE, CONG. RSCH. SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) i (2015), [perma.cc/6PKX-XW3X](https://perma.cc/6PKX-XW3X) (PDF).

363. *Id.* at i, 1–2.

privacy.”<sup>364</sup> A month later, the Ninth Circuit recognized that Facebook’s practice of tracking users’ online browsing habits in violation of the WTA and the SCA were concrete injuries, again noting that “these statutory provisions codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing.”<sup>365</sup> The panels relied on *Spokeo*’s flimsy and malleable distinction between substance and procedure,<sup>366</sup> but contextual integrity shows us that the conclusion is correct—not because the statutes use or avoid specific words, but instead because violations of these laws contravene entrenched informational norms about the confidentiality of communicative content.

The Telephone Consumer Protection Act (TCPA) is an example of an information use injury that protects an entrenched informational norm. In 1991, Congress enacted the TCPA “in light of evidence that consumers ‘consider automated or prerecorded telephone calls, regardless of the content or the initiator of the message, to be a nuisance and an invasion of privacy.’”<sup>367</sup> The statute itself explains: “Many consumers are outraged over the proliferation of intrusive, nuisance calls to their homes from telemarketers.”<sup>368</sup> As the Supreme Court recently noted, a leading Senate sponsor of the TCPA described robocalls in 1991 as “the scourge of modern civilization. They wake us up in the morning; they interrupt our dinner at night; they force the sick and elderly out of bed; they hound us until we want to rip the telephone right out of the wall.”<sup>369</sup>

---

364. *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1117 (9th Cir. 2020) (internal quotation marks and brackets omitted).

365. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020) (citing *Campbell*, 951 F.3d at 117–19).

366. *See Campbell*, 951 F.3d at 1117 (relying on *Spokeo* to link statutory protections of privacy to injuries that traditionally provided grounds for a suit).

367. *See* Petition for a Writ of Certiorari at 3, *Barr v. Am. Ass’n of Pol. Consultants*, 140 S. Ct. 2335 (2020) (No. 19-631), 2019 WL 6115075 (citing Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, § 2(10), 105 Stat. 2394).

368. Pub. L. No. 102-243, § 2(6), 105 Stat. 2394.

369. *See Barr v. Am. Ass’n of Pol. Consultants, Inc.*, 140 S. Ct. 2335, 2344 (2020) (Kavanaugh, J., plurality opinion) (quoting 137 CONG. REC. 30821 (1991) (statement of Sen. Hollings)).

The TCPA is an information use restriction: It prohibits “any person within the United States from making any call using any automatic telephone dialing system . . . to any telephone number assigned to a cellular telephone service.”<sup>370</sup> In other words, the statute restricts how a consumer’s telephone number may be used. And given the statute’s history, there is little doubt that Congress codified an informational norm.<sup>371</sup>

The circuit courts of appeals are divided on when violations of the TCPA confer Article III standing. The contextual integrity legal framework sheds light on which side of the split is correct. In *Salcedo v. Hanna*,<sup>372</sup> the Eleventh Circuit held that receiving an unsolicited text message—sent in violation of the TCPA—did not create a concrete injury in fact.<sup>373</sup> The court repeatedly emphasized that the plaintiff had received only a single unwanted text message and said that neither Congress’s judgment nor history supported standing.<sup>374</sup> Ultimately, the court concluded that the “chirp, buzz, or blink of a cell phone receiving a single text message is more akin to walking down a busy sidewalk and having a flyer briefly waived in one’s face. Annoying, perhaps, but not a basis for invoking the jurisdiction of the federal courts.”<sup>375</sup>

Other circuits—including the Second,<sup>376</sup> Fifth,<sup>377</sup> Seventh,<sup>378</sup> and Ninth<sup>379</sup>—have disagreed. Contextual integrity suggests that calls and texts that violate the TCPA do create a

---

370. Petition for Cert., *supra* note 367, at 3 (internal quotation marks, brackets, and ellipses omitted) (quoting 47 U.S.C. § 227(b)(1)(A)(iii)).

371. See S. REP. NO. 102-178, at 3 (1991) (“Many consumers and consumer representatives believe that legislation is necessary to protect them from these calls. One survey found that about 75 percent of persons contacted favored some form of regulation of these calls, and one-half of these favored prohibiting all unsolicited calls.”).

372. 936 F.3d 1162 (11th Cir. 2019).

373. *Id.* at 1168–74.

374. *Id.* at 1168–72.

375. *Id.* at 1172.

376. See *Melito v. Experian Mtkg. Sols., Inc.*, 923 F.3d 85, 92–93 (2d Cir. 2019).

377. See *Cranor v. 5 Star Nutrition, LLC*, 998 F.3d 686, 690 (5th Cir. 2021).

378. See *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 461–63 (7th Cir. 2020) (Barrett, J.).

379. See *Van Patten v. Vertical Fitness Grp.*, 847 F.3d 1037, 1042–43 (9th Cir. 2017).

concrete injury in fact because Congress imposed restrictions on the use of automated telephone equipment in direct response to widespread outrage—outrage that evidences an entrenched informational norm.<sup>380</sup>

The Video Privacy Protection Act (VPPA) prohibits information dissemination; it provides in relevant part: “A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person.”<sup>381</sup> The impetus for this rather specific restriction was Robert Bork’s Supreme Court nomination Senate confirmation hearings in 1988.<sup>382</sup> A newspaper published a profile of Bork “based on the titles of 146 films his family had rented from a video store . . . . Members of the Judiciary Committee denounced the disclosure.”<sup>383</sup> As one senator explained, “[i]t is nobody’s business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home.”<sup>384</sup> The swift legislative action and bipartisan outrage signal that the VPPA’s dissemination restriction tracks an entrenched informational norm.<sup>385</sup>

Courts weighing the Article III implications of the VPPA’s dissemination restriction have correctly and unanimously concluded that violations of the law create a concrete injury.<sup>386</sup> The Ninth Circuit pointedly noted that the statute “identifies a *substantive* right to privacy that suffers *any time* a video service provider discloses otherwise private information. As a result, every [statutory] violation presents the precise harm and infringes the same privacy interests Congress sought to protect.”<sup>387</sup>

---

380. See Telephone Consumer Prot. Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394.

381. 18 U.S.C. § 2710(b)(1).

382. See S. REP. NO. 100-599, at 5–7 (1988).

383. *Id.* at 5.

384. *Id.*

385. See *id.* at 2 (describing a long line of statutes passed by Congress prior to the VPPA to expand and give meaning to the entrenched right of privacy).

386. See *Perry v. CNN, Inc.*, 854 F.3d 1336, 1341 (11th Cir. 2017); *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 274 (3d Cir. 2016); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 982–84 (9th Cir. 2017).

387. *Eichenberger*, 876 F.3d at 983–84 (alterations omitted).

The FCRA is “America’s first federal consumer information privacy law and one of the first information privacy laws in the world.”<sup>388</sup> Several scholars have mapped credit reporting’s evolution in the United States starting shortly after the Civil War up and through the rise of consumerism in the 1950s.<sup>389</sup> The FCRA is an extraordinarily complex statute that has been amended several times,<sup>390</sup> but the history of its inception is straightforward: Congress became interested in regulating credit reporting in the 1960s in response to perceived abuses among credit reporting agencies.<sup>391</sup> Congress found that credit reporting agencies collected any and all available information—from sexual orientation to alcohol consumption habits—and often disclosed the contents of these then-secret dossiers to law enforcement.<sup>392</sup> Congress enacted the FCRA “to comprehensively regulate consumer reporting and the practice of assembling files about consumers in order to evaluate them for credit, employment, tenancy, ‘consumer-initiated’ transactions, or other opportunities.”<sup>393</sup>

This history suggests that the FCRA established and shaped many now-entrenched norms about information practices in the credit reporting industry. Before the FCRA, illegitimate access to credit reports was widespread: “A 1969 study of the [credit reporting] industry found that anyone with sufficient knowledge of the consumer reporting industry could obtain reports on other individuals.”<sup>394</sup> As a result of the FCRA’s restrictions on disclosures, norms surrounding disclosure of

---

388. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 270 (2016).

389. *See id.* at 271 (discussing JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE: SOCIAL CONTROL IN THE COMPUTER AGE (1974)).

390. *See id.* at 275.

391. *See id.* at 271; The Fair Credit Reporting Act (FCRA) and the Privacy of your Credit Report, ELEC. PRIV. INFO. CTR., <https://perma.cc/KN49-MYDM> (“CRAs assemble reports on individuals for businesses, including credit card companies, banks, employers, landlords, and others. The FCRA provides important protections for credit reports, consumer investigatory reports, and employment background checks.”).

392. *See* HOOFNAGLE, *supra* note 388, at 271.

393. *Id.* at 270.

394. *Id.* at 275 (citing James B. Rule et al., *The Dossier in Consumer Credit*, in ON RECORD: FILES AND DOSSIERS IN AMERICAN LIFE (Stanton Wheeler ed., 1969)).



credit information have become particularly strong—the statute enumerates who can request a credit report, limits credit checks to specific purposes, and requires individualized notice and consent from prospective employees.<sup>395</sup> As a result, many violations of the FCRA should be understood as breaching entrenched informational norms. For example, if an employer runs a credit check without first obtaining consent, courts should consider that a concrete injury in fact because the FCRA has established a norm against the practice.<sup>396</sup>

But not all violations of the FCRA contravene entrenched informational norms. In *Spokeo*, the Supreme Court specifically discussed the disclosure of an incorrect zip code.<sup>397</sup> The dissemination of an incorrect zip code is potentially a violation of the FCRA, but it doesn't necessarily breach an entrenched informational norm.<sup>398</sup> The Court suggested that the incorrect zip code wasn't a concrete injury in fact because it was "difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."<sup>399</sup> But without contextual integrity's key insight, speculating about the likelihood of a concrete harm is an analytical dead end. The better way to analyze the example is to simply ask: does the dissemination of an incorrect zip code breach an entrenched informational norm? The answer may often—although not always—be no.<sup>400</sup>

In *TransUnion*, the Court held that 1,853 class members who had false OFAC designations disseminated to third parties had a concrete injury in fact.<sup>401</sup> There can be little doubt this conclusion is consistent with the contextual integrity framework: falsely labeling someone a potential terrorist to a

395. See 15 U.S.C. § 1681b.

396. See 15 U.S.C. § 1681b(b) (providing conditions for furnishing and using consumer reports for employment purposes).

397. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 342 (2016).

398. See *id.* (finding the dissemination of an incorrect zip code to present no material risk of harm).

399. *Id.*

400. Cf. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 145–46 (2019) (illustrating that the dissemination of an incorrect zip code can produce concrete harms).

401. See *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208–09 (2021).

potential lender or employer violates entrenched informational norms.<sup>402</sup>

But the Court also held that 6,332 class members who stipulated that their credit reports had not been disclosed to third parties lacked a concrete injury under the FCRA, because their “harm is roughly the same . . . as if someone wrote a defamatory letter and then stored it in her desk drawer.”<sup>403</sup> The contextual integrity framework shows that this conclusion is probably wrong, though it’s not totally indefensible. On the one hand, TransUnion’s OFAC-matching process was woefully deficient and endured for inexcusably long,<sup>404</sup> which suggests that TransUnion has little respect for entrenched informational norms. But there is a closer question about whether actual nondisclosure of false information breaches informational norms in the same way that actual disclosure so obviously does. If the majority is right that the false designations were not disseminated to any third parties—a dubious proposition, at best<sup>405</sup>—then it’s difficult to conclude that the undisclosed false designations contravened an informational norm. At the very least, however, the Court should have remanded the case with instructions to allow the 6,332 plaintiffs to show their credit reports were disseminated beyond what was stipulated.<sup>406</sup>

The FCRA also includes information access rights, and violations of these access rights constitute information

---

402. See *id.* at 2208 (“Under longstanding American law, a person is injured when a defamatory statement ‘that would subject him to hatred, contempt, or ridicule’ is published to a third party.”).

403. *Id.* at 2210.

404. See *id.* at 2215 (Thomas, J., dissenting)

TransUnion “made surprisingly few changes” after [losing in *Cortez*]. It did not begin comparing birth dates. Or middle initials. Or citizenship. In fact, TransUnion did not compare *any* new piece of information. Instead, it hedged its language saying a consumer was a “potential match” rather than saying the person was a “match.”

*id.* at 2221 (“[T]his is a rather odd case to say that Congress went too far.”); *id.* at 2222 (“[T]hen there is the standalone harm caused by the rather extreme errors in the credit reports.”).

405. See *supra* notes 202–204 and accompanying text.

406. Cf. *TransUnion*, 141 S. Ct. at 2212 (characterizing this possibility as a “serious argument” but nonetheless coming to the cursory conclusion that the “inferences on which the argument rests are too weak”).

withholding injuries.<sup>407</sup> Before the FCRA, consumers had no right to access their credit reports, and the credit reporting trade association told its members that reports “must not be revealed to the subject reported on.”<sup>408</sup> Congress has amended the FCRA to make access more affordable and readily available.<sup>409</sup> Today, the right to access one’s own credit report—and to correct erroneous information—is a deeply entrenched informational norm, so violations of the right of access should be considered concrete injuries in fact.<sup>410</sup>

It’s for this reason that the *TransUnion* majority’s information withholding holding is clearly wrong. The Court held that everyone except the named plaintiff lacked standing to pursue the withholding claims because they “identified no downstream consequences from failing to receive the required information.”<sup>411</sup> But the contextual integrity framework condemns the “downstream consequences” inquiry, and instead asks whether the statute particularizes a right against breaching an informational norm. As we’ve already seen, the FCRA adequately particularizes several informational interests, and Justice Kagan’s *TransUnion* dissent identifies several implausible assumptions underlying the majority’s information-withholding conclusion.<sup>412</sup> In short, the FCRA has established an informational norm that empowers individuals to access their credit reports; when TransUnion sent every class member a pair of non-compliant, opaque, and confusing

---

407. See HOOFNAGLE, *supra* note 388, at 278 (“[I]f the consumer report is relied upon *at all* to make an adverse decision, the consumer should be told. In employment situations, the employer is required to provide a copy of the consumer report used to make the determination and a statement of the applicant’s rights under the FCRA.”).

408. *Id.* at 274 (citing JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE: SOCIAL CONTROL IN THE COMPUTER AGE (1974)).

409. See Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, §§ 211–212.

410. See Melinda Opperman, *The Importance of Checking Your Credit Score on a Regular Basis*, CREDIT.ORG, <https://perma.cc/G3Y5-P9B4> (explaining that consumers regularly check their credit score and annual credit report).

411. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2214 (2021) (internal quotation marks omitted).

412. See *id.* at 2225–26 (Kagan, J., dissenting).

mailings, it breached that norm. As a result, every class member had a concrete withholding injury.

In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA).<sup>413</sup> BIPA prohibits the collection and retention of biometric identifiers by non-governmental actors absent informed written consent.<sup>414</sup> BIPA's prohibitions are best understood as information collection and information use restrictions.<sup>415</sup>

BIPA provides an excellent illustration of the intractable nature of the concreteness inquiry for informational injuries because the law is privately enforceable.<sup>416</sup> Under *Spokeo*, how should a court answer the question of whether an illegal collection or retention of a facial recognition scan is a sufficiently concrete injury? BIPA supplies a stringent procedural framework for obtaining informed consent,<sup>417</sup> but *Spokeo* singles out procedural violations as falling short of a concrete injury.<sup>418</sup>

The contextual integrity legal framework supplies answers to these questions. Matthew B. Kugler has shown that “people are concerned about the collection of biometric information, even when it is presented in mundane, matter-of-fact contexts,” “that they are willing to forgo benefits to avoid the collection of biometric information, and that they would be willing to pay more for services that protect biometric privacy.”<sup>419</sup> Kugler's empirical work also shows that Americans reactions to the use of biometric technology can be variable. For example, most respondents were fairly comfortable with limited uses closely related to security (e.g., unlocking a phone using facial recognition), whereas supermajorities were uncomfortable with broad scale public tracking.<sup>420</sup>

---

413. Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14 (2008).

414. *See id.* §§ 10, 15.

415. *See id.* § 5 (describing the Act as an effort to regulate “the collection, use, [and other aspects] of biometric identifiers and information”).

416. *See id.* § 20.

417. *See id.* § 15(b) (providing three prerequisites before a private entity may obtain a person or customer's biometric identifier or information).

418. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 342 (2016).

419. Kugler, *supra* note 400, at 111 (2019); *see id.* at 121–30 (reviewing participant responses from various studies involving private use of biometric data).

420. *Compare id.* at 112, *with id.* at 138–41.

Kugler’s findings strongly suggest that new informational norms about biometric information are becoming entrenched. Outside a few narrow examples, survey respondents showed widespread discomfort with practices that potentially violate BIPA.<sup>421</sup> As a result, most violations of BIPA—though perhaps not all—breach informational norms and therefore create concrete injuries.

At least some courts have recognized that BIPA violations create concrete injuries.<sup>422</sup> For example, in a case involving Facebook’s photo-tagging suggestion feature, the Ninth Circuit held that the plaintiffs had Article III standing because BIPA’s prohibitions “were established to protect an individual’s concrete interests in privacy, not merely procedural rights.”<sup>423</sup>

BIPA cases to date represent low-hanging fruit; much more difficult questions about the concreteness of procedural violations loom. Kugler’s analysis rightly shows that *Spokeo*’s substance/procedure distinction is of limited utility in these second-wave BIPA cases.<sup>424</sup> The contextual integrity legal framework avoids these semantic games and cuts to the heart of Kugler’s empirical findings: that there are informational norms against many uses of biometric technology, irrespective of whether the legal violations are characterized as procedural or substantive.<sup>425</sup>

The Drivers Privacy Protection Act (DPPA)<sup>426</sup> is another example of an information use restriction that protects entrenched informational norms. The DPPA restricts how motor

421. See *id.* at 140 (“Using facial recognition to track people on public streets (68.1% uncomfortable), detect photos of celebrities online (73.8%), or to link profiles of people across social networking sites (69.1%) made majorities uncomfortable.”).

422. See, e.g., *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019); *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1207 (Ill. 2019). *But see* *Rivera v. Google, Inc.*, 366 F. Supp. 3d 998, 1013 (N.D. Ill. 2018) (“Plaintiffs do not present any evidence showing that Google commercially ‘exploited’ their faces or the face templates they created. Without more, Plaintiffs’ injury in this case does not bear a close relationship to the tort of intrusion upon seclusion.”).

423. *Patel*, 932 F.3d at 1274 (internal quotation marks omitted).

424. See Kugler, *supra* note 400, at 145–49 (outlining the dilemma whereby procedural violations are easily demonstrable but insufficient to bring adverse claims).

425. See *supra* note 298 and accompanying text.

426. 18 U.S.C. § 2721.

vehicle records may be used.<sup>427</sup> Like the TCPA, Congress enacted the DPPA in response to widespread outrage at abusive informational practices. The DPPA was a “reaction to . . . a series of abuses of drivers’ personal information,” including the 1989 death of actress Rebecca Schaeffer, who was killed by an obsessed fan who obtained her address through her California motor vehicle record.<sup>428</sup> One senator explained: “Many Americans are infuriated and, more importantly, they are vulnerable to these violations of privacy.”<sup>429</sup>

In *Heglund v. Aitkin County*,<sup>430</sup> the U.S. Court of Appeals for the Eighth Circuit recognized that violations of the DPPA create concrete injuries.<sup>431</sup> In that case, a former law enforcement officer’s ex-husband accessed her personal information in violation of the DPPA; an audit of the state’s driver’s license database revealed that her information had been accessed 446 times in a ten-year period.<sup>432</sup> The Eighth Circuit refused to dismiss the case on standing grounds: “In enacting the DPPA, Congress recognized the potential harm to privacy from state officials accessing drivers’ personal information for improper reasons. . . . [The plaintiffs] claim that [the defendant] violated the DPPA’s substantive protections by invading [her] privacy.”<sup>433</sup> Here again, a court’s reasoning initially seems to turn on a substance/procedure distinction.<sup>434</sup> But contextual integrity shows us that the DPPA’s protections are substantive because violating the statute also violates an entrenched informational norm. In other words, the informational norm makes the statutory protection substantive.

---

427. See *id.* § 2721(a) (restricting disclosures); *id.* § 2721(b) (providing exceptions for “[p]ermissible [u]ses”).

428. *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*, ELEC. PRIV. INFO. CTR., <https://perma.cc/T77C-NT2R>.

429. *Id.*

430. 871 F.3d 572 (8th Cir. 2017).

431. See *id.* at 578.

432. *Id.* at 575–76.

433. *Id.* at 577–78.

434. See *id.* at 578 (distinguishing this substantive allegation from a procedural violation in a different case concerning a “statutory duty to destroy personally identifiable information the cable company lawfully obtained”).

Although not privately enforceable, the Health Insurance Portability and Accountability Act's Privacy Rule (HIPAA or "the Rule") is an example of a legal authority that codified preexisting information dissemination and information access norms. The Rule provides that a covered entity "may not use or disclose protected health information, except as permitted or required by" the Rule.<sup>435</sup> Congress enacted the statute in 1996 and the Rule was finalized in 2000.<sup>436</sup> But Americans expected confidentiality in their medical records long before 2000. Prosser's privacy tort taxonomy identified civil medical disclosure cases from the 1920s and '30s.<sup>437</sup> And both before and after HIPAA's enactment, state statutes have both restricted medical disclosures<sup>438</sup> and mandated patient access to medical records.<sup>439</sup>

Like HIPAA, the Family Educational Rights and Privacy Act (FERPA)<sup>440</sup> is not privately enforceable, and, like HIPAA, it protects entrenched informational norms regarding information dissemination and information access.<sup>441</sup> FERPA, also known as the Buckley Amendment after its principal sponsor, Senator James Buckley, prohibits educational institutions from disclosing "personally identifiable information in education records" without the written consent of the student or, if the student is a minor, the student's parents.<sup>442</sup> While there are a dearth of legislative records preceding the law's initial

435. 25 C.F.R. § 164.502(a) (2013).

436. *Summary of the HIPAA Privacy Rule*, HHS, <https://perma.cc/LL77-U3AX>.

437. See Prosser, *supra* note 359, at 393 n.88 (citing *Banks v. King Features Syndicate*, 30 F. Supp. 352 (S.D.N.Y. 1939) (newspaper publication of x-rays of woman's pelvic region under Oklahoma law); *Griffin v. Med. Soc'y*, 11 N.Y.S.2d 109 (Sup. Ct. 1939) (publication in medical journal of pictures of plaintiff's deformed nose); *Feeney v. Young*, 181 N.Y.S. 481 (App. Div. 1920) (public exhibition of filmed caesarian operations)).

438. See, e.g., N.Y. EDUC. LAW § 6530(23) (McKinney 2021) (defining "professional misconduct" to include the revealing of "personally identifiable facts, data, or information obtained in a professional capacity without the prior consent of the patient").

439. See, e.g., N.Y. PUB. HEALTH LAW § 18 (McKinney 2019).

440. 20 U.S.C. § 1232g.

441. See *id.* (protecting dissemination of and access to information pertaining to students).

442. *Id.* § 1232g(b)(2).

enactment, Senator Buckley later explained in a speech to the Legislative Conference of Parents and Teachers that FERPA “was adopted in response to ‘the growing evidence of the abuse of student records across the nation.’”<sup>443</sup> States have also sought to regulate and restrict access to educational records,<sup>444</sup> further illustrating the existence of an informational norm against both unfettered access and unjustified withholding.

## 2. Authorities that Only Occasionally Create an Injury in Fact

This section reviews a host of legal authorities that have a more tenuous relationship to entrenched informational norms. As a result, sometimes a plaintiff that alleges a violation of one of these statutes will have a concrete injury in fact, but sometimes not.

We’ve already seen an illustration of a collection injury that does not violate an entrenched informational norm. In *Hancock v. Urban Outfitters*,<sup>445</sup> the D.C. Circuit held that—while it is a violation of the D.C. I.D. Act to request a customer’s zip code at a retail point-of-sale transaction—the “naked assertion that a zip code was requested and recorded without any concrete consequence” was insufficient for Article III standing.<sup>446</sup>

Retailers routinely ask consumers for personal information at point-of-sale transactions—loyalty programs, after all, are premised on the connection between a consumer’s purchases and a stable identity, whether it’s a phone number, email address, or other identifier. It’s therefore implausible that the D.C. I.D. Act protects an entrenched informational norm against requesting something as vague as a zip code since people routinely share far more personalized information in retail transactions. The law’s prohibitions do not map onto entrenched informational norms because they simultaneously outlaw too

---

443. *Family Educational Rights and Privacy Act (FERPA)*, ELEC. PRIV. INFO. CTR., <https://perma.cc/S72V-SUUJ>.

444. *See, e.g.*, MASS. GEN. LAWS ch. 71, § 34H (2019) (granting the department of education the right to promulgate regulations controlling state administration of student information).

445. 830 F.3d 512 (D.C. Cir. 2016).

446. *Id.* at 514; *see* D.C. CODE § 47-3153(a) (2022) (“[N]o person shall, as a condition of accepting a credit card as Payment for a sale of goods or services, request or record the address or telephone number of a credit card holder on the credit card transaction form.”).



much and too little: the law prohibits even requests for information but includes an exception “if the information is necessary for the shipment, delivery, or installation of consumer goods, or special orders of consumer goods or services.”<sup>447</sup>

This is not to suggest that no violations of the D.C. I.D. Act are enforceable. Certain types of transactions may dictate stronger interests in discretion and using a consumer’s information in a way that is inconsistent with informational norms is rife with potential abuse. But it does suggest that the D.C. Circuit’s conclusion in *Hancock* was right—contextual integrity explains that a retailer’s request for a zip code does not violate entrenched information collection norms and, without more, there is therefore no concrete injury.

The Cable Communication Policy Act (Cable Act)<sup>448</sup> provides in relevant part that a “cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected.”<sup>449</sup> In *Braitberg v. Charter Communications*,<sup>450</sup> the Eighth Circuit held that retaining customer records in violation of the Cable Act did not create a concrete Article III injury.<sup>451</sup>

The opinion’s reasoning failed to supply a coherent line-drawing principle or explain why Congress couldn’t regulate information use and retention practices. But contextual integrity helps answer both questions. Few Americans would be surprised to learn that companies hoard customer data, and this country has never really sought to implement a legal mandate to destroy or purge data.<sup>452</sup> Because there is no entrenched informational norm to destroy unnecessary data, the statutory violation is not, alone, sufficient for Article III.<sup>453</sup> Reflecting on *Braitberg*’s reasoning, one

447. D.C. CODE § 47-3153(a)–(b) (2022).

448. 47 U.S.C. §§ 521–573.

449. *Id.* § 551(e).

450. 836 F.3d 925 (8th Cir. 2016).

451. *See id.* at 931.

452. *See* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1942 (2019) (noting that, outside a few exceptions, under current law any information “may be gathered by anyone and kept forever” (internal quotation omitted)).

453. *See Braitberg*, 836 F.3d at 930 (“Congress’s role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a

commentator suggested that “the Eighth Circuit cast doubt on whether Congress can expand privacy rights beyond their common law scope at all.”<sup>454</sup> But that’s too strong. Congress *can* expand privacy rights beyond the common law, but concrete informational injuries require a violation of both the statute and an informational norm.<sup>455</sup> Unless and until Americans’ expectations about information retention practices change, violations of information destruction mandates do not create concrete injuries.

The Fair and Accurate Credit Transactions Act (FACTA)<sup>456</sup> imposes a truncation requirement for payment card numbers on point-of-sale transaction receipts.<sup>457</sup> The law stipulates that “no person . . . shall print more than the last 5 digits of the card number or the expiration date.”<sup>458</sup> Because FACTA is privately enforceable, many circuit courts have struggled with the question of whether non-compliant receipts create a concrete injury in fact.<sup>459</sup> Courts have engaged in convoluted analyses about how likely a given non-compliant receipt is to aid in effecting identity theft.<sup>460</sup> Contextual integrity helps solve this

---

statutory right and purports to authorize that person to sue to vindicate that right.” (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016))).

454. Baude, *supra* note 216, at 223.

455. *See id.* (discussing the constraints the common law places on Congress’s ability to expand privacy rights).

456. Pub. L. No. 108-159, 117 Stat. 1952 (2003).

457. *Id.*

458. 15 U.S.C. § 1681c(g)(1).

459. *See, e.g.*, *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019) (discussing how courts analyze standing when presented with a private enforcement action under FACTA); *Katz v. Donna Karan Co.*, 872 F.3d 114, 121 (2d Cir. 2017) (same); *Meyers v. Nicolet Rest. of De Pere, L.L.C.*, 843 F.3d 724, 727 (7th Cir. 2016) (same); *Bassett v. ABM Parking Servs., Inc.*, 883 F.3d 776, 783 (9th Cir. 2018) (same); *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 925–26 (11th Cir. 2020) (en banc) (same); *Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1067 (D.C. Cir. 2019) (same).

460. For example, in *Kamal v. J. Crew Grp.*—a case in which the retailer printed the first six and last four digits of the plaintiff’s payment card—the court explained that the “threat consists of a highly speculative chain of future events” wherein the plaintiff “loses or throws away [the receipt], which is then discovered by a hypothetical third party, who then obtains the six remaining truncated digits along with any additional information required to use the card, such as the expiration date, security code or zip code.” *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019) (internal quotation omitted) (alteration in original).

intractable and unknowable inquiry by avoiding it altogether. Instead, courts should evaluate whether disclosing more than five digits breaches an informational norm. Surely some non-compliant receipts do, like those that print all or nearly all digits, but many situations—like printing six or seven digits—likely do not.

There are several recent examples of statutes and proposals that restrict how information may be used, but the legal prohibition's relationship to informational norms is still ambiguous. The California Consumer Privacy Act (CCPA)<sup>461</sup> introduces new conditions on data processing.<sup>462</sup> Its “rule does not stop companies from using data for new purposes—it just requires disclosure if they do so.”<sup>463</sup>

Legislative proposals in recent years have included additional information use restrictions. For example, U.S. Senator Maria Cantwell has introduced the Consumer Online Privacy Rights Act (COPRA).<sup>464</sup> Among many other provisions, COPRA includes a duty of loyalty, which prohibits covered entities from “processing or transfer[ring] . . . covered data in a manner that causes or is likely to cause” financial, physical, or reputational injuries; physical or other offensive intrusions into an individual's private affairs or concerns; or other substantial injuries to an individual.<sup>465</sup> Proposed legislation in New York similarly seeks to prohibit covered entities from “us[ing] personal data . . . in any way that . . . will benefit the online service provider to the detriment of an end user.”<sup>466</sup>

---

461. CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2020).

462. *See id.* § 1798.100(b) (“A business that collects a consumer's personal information shall . . . inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.”).

463. Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1757 (2021).

464. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019); *see* Adam Schwartz, *Sen. Cantwell Leads with New Consumer Data Privacy Bill*, ELEC. FRONTIER FOUND. (Dec. 3, 2019), <https://perma.cc/EJX4-RW5L>.

465. S. 2968 § 101(b).

466. S.B. 5642 § 1102(b), 242 Leg. Sess. (N.Y. 2019).

Data-use restrictions, while commonplace elsewhere in the world, are a novel development in domestic law.<sup>467</sup> While some empirical evidence suggests that Americans favor use restrictions and balk when they learn about unfettered data flows,<sup>468</sup> it's ambiguous whether flouting a use restriction would violate an entrenched informational norm. Of course, over time, an informational norm against unfettered data use may become entrenched. And in that case, use restrictions could be a successful norm-establishment example. But because these are mostly proposals—and others are not individually enforceable—the norm is inchoate.

The same is true for these authorities' information access provisions. Norms surrounding access to the dossiers that enable targeted advertising are ambiguous. The CCPA and the proposed COPRA both include rights of access, but targeted advertising is a much more recent phenomenon than credit reporting.<sup>469</sup> As norms over access to marketing datasets evolve, it's possible that consumers will increasingly expect reliable access.

\* \* \*

Contextual integrity shows us that judicial investigations into an information injury's "concreteness" need not be an irresolvable morass. While contextual integrity reveals that courts often reach the correct conclusion about a given injury's concreteness, the legal framework helps refine and guide Article III standing analysis.

---

467. See Chander et al., *supra* note 463, at 1747–49 (comparing the United States' domestic informational privacy laws with those of the European Union).

468. See, e.g., Kirsten Martin & Ari Waldman, Perceptions of the Legitimacy of Algorithmic Decision-Making 22 (Nov. 16, 2021) (unpublished manuscript) (on file with author) ("In general, respondents judged human and algorithmic decisions as less legitimate when based on aggregated data than when based on specific data for a given decision . . ."); Noah Aphorpe et al., *Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity*, PROC. ACM ON INTERACTIVE, MOBILE, WEARABLE & UBIQUITOUS TECHS., May 2018, at 1, 9–10 (finding that survey respondents responded most negatively to situations where "information is used for advertising").

469. See, e.g., Letter from Jane C. Horvath, Senior Dir., Glob. Priv., Apple, to Dr. Jan. Rydzak, Ranking Digit. Rts. (Nov. 19, 2020), <https://perma.cc/5E6G-W5GS> (PDF) ("Privacy-focused ad networks were the universal standard in advertising before the practice of unfettered data collection began over the last decade or so.").

## V. JUSTIFICATIONS

This Part identifies the legal framework's virtues and then responds to objections about the proposal.

A. *Virtues and Advantages*

There are four interrelated virtues and advantages to the proposed legal framework.

The first virtue of the legal framework is that it solves the line-drawing problem described in Part II.B.1. The breach of an informational norm supplies the source of a plaintiff's concrete injury. Where the defendant has not breached a norm in violation of a statute, the plaintiff lacks a concrete injury.

The analysis thus keys courts into the true stakes of informational-injury cases: has the defendant engaged in an informational practice that contravenes entrenched norms? This directs the courts away from unknowable inquiries—like how likely identity theft will follow from a noncompliant receipt,<sup>470</sup> or how likely it is that an employer will rely on the results of an internet search query to reject a prospective employee's application.<sup>471</sup>

Many of the problems that arise in privacy injury cases flow from the need to make speculative and subjective assessments about the likelihood of visceral “real harm.”<sup>472</sup> The proposed framework eschews these difficult issues—charging courts with a question about the here and the now.

Nissenbaum explains that contextual integrity “not only helps predict when an activity or practice is likely to arouse protest, indignation, or resistance, it helps explain and pinpoint

---

470. See, e.g., *Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1067 (D.C. Cir. 2019) (discussing the difference in risk between a receipt containing only the first six digits and a receipt with the entire card number (citing *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 116–17 (3d Cir. 2019))).

471. See, e.g., *Spokeo, Inc. v. Robins*, 578 U.S. 330, 353–54 (2016) (Ginsburg, J., dissenting) (discussing amici briefs that describe the threat to Robins's employment prospects); *id.* (“I therefore see no utility in returning this case to the Ninth Circuit to underscore what Robins's complaint already conveys concretely: Spokeo's misinformation cause[s] actual harm to [his] employment prospects.” (internal quotation omitted) (alteration in original)).

472. Cf. *id.* at 341 (majority opinion) (suggesting that “the risk of real harm” can “satisfy the requirement of concreteness”).

the sources of objection.”<sup>473</sup> This legal framework builds on these insights by recognizing that the practices that arouse protest, indignation, and resistance are themselves the source of a legal injury.

The second virtue of the legal framework is that it is responsive to concerns of political accountability and the separation of powers described in Part II.B.2. The framework allows for judicial discretion and control over Article III injuries but simultaneously empowers legislatures to have a say in the evolution of informational norms. Importantly, the framework applies to both private-sector and public-sector actors. Far from raising separation of powers concerns, the framework recognizes that violating expectations is itself the injury and hence treats all norm violators the same. At the same time, the framework remains faithful to the judiciary’s concerns about advisory opinions and undifferentiated procedural injuries. Focusing the analysis on norms avoids abstraction concerns by tying the plaintiff’s injury to the violation of expectations about informational practices.

The third virtue is related to the first two. Making norms and expectations the source of the plaintiff’s injury protects privacy for privacy’s own sake. Other approaches to this problem use privacy as a stand-in for other interests—like risk and anxiety.<sup>474</sup> Privacy is but a proxy for other harms, like the increased risk of identity fraud and the mental anguish associated with worrying about it.<sup>475</sup> According to these approaches, courts and commentators can use “privacy” as a shorthand, but what we’re really protecting is a right to control information and to protect it from potential misuse.<sup>476</sup>

In contrast, the framework proposed here does not treat privacy as a stand-in for other underlying interests. Instead, it protects people’s expectations about injurious informational practices without needing to rely on the attenuated possibility of financial harm. Like Nissenbaum says, “What people care

---

473. NISSENBAUM, *supra* note 29, at 148.

474. *See* Solove & Citron, *supra* note 231, at 756–67.

475. *See id.* at 754 (“Most courts consider plaintiffs’ fear, anxiety, and psychic distress about their increased risk of identity theft and other abuses too remote to warrant recognition.”).

476. *See id.* at 764–67 (analyzing the consumer’s fear of information misuse in the privacy context).

most about is . . . that [information] flows *appropriately*,<sup>477</sup> and the proposed legal framework gives teeth to people’s expectations about appropriate informational practices.

The final advantage of the proposed framework is that it simultaneously provides a solution to all three injury in fact requirements: concreteness, particularization, and actuality. Concreteness is easy and has been the source of most discussion. In short, breaching a statutorily protected norm is itself a concrete injury.

Relying on legislative authorization helps solve particularization concerns. A court determines whether the plaintiff is among the injured by assessing whether the defendant actually contravened the plaintiff’s expectations about informational practices. This type of analysis avoids the advisory-opinion ban by ensuring that an informational-injury plaintiff is seeking to vindicate her own interests and expectations and not seeking “general compliance with regulatory law” or attempting to vindicate interests owed to society at large.<sup>478</sup>

Finally, the framework solves the future-injury conundrum by sidestepping it entirely. Unlike other approaches that rely on risk calculations, the legal framework charges courts with assessing an injury to expectations in the past and present. This makes contravention of norms and expectations an “actual” injury, rather than a conjectural or speculative one.

### B. *Responding to Objections*

There are five objections to the proposed framework that are worth confronting directly.

One objection reprises an argument I’ve made in the past. It goes like this: There is no justification for

---

477. NISSENBAUM, *supra* note 29, at 148.

478. *Cf. Spokeo Inc., v. Robins*, 578 U.S. 330, 349 (2016) (Thomas, J., concurring)

If Congress has created a private duty owed personally to Robins to protect *his* information, then the violation of the legal duty suffices for Article III injury in fact. If that provision, however, vests any and all consumers with the power to police the “reasonable procedures” of Spokeo, without more, then Robins has no standing to sue for its violation absent an allegation that he has suffered individualized harm.

counter-majoritarian Article III standing doctrine in cases against private-sector actors.<sup>479</sup> In the absence of separation-of-powers concerns, courts should automatically defer to the legislature and should not substitute their judgment for political consensus.<sup>480</sup> The framework makes a fundamental error, the objection goes, because it allows courts to invalidate legislatively prescribed causes of action that pose no risk of interfering with the Executive Branch.<sup>481</sup>

While it's true enough that separation of powers concerns are at a nadir in cases against private defendants, they are not absent entirely. Congress could not, for example, authorize advisory opinions.<sup>482</sup> Attempting to limit Article III standing to the advisory-opinion ban exclusively is unworkable because “courts saw in some procedural legal rights the same things that had concerned them about advisory opinions—the possibility of courts being asked to adjudicated only “[t]he public nonconcrete interest in the proper administration of the laws.”<sup>483</sup> And that concern remains present in both cases against governmental and non-governmental actors.

The rejoinder to this objection is twofold. First is that the framework always respects political consensus that reflects expectations about informational norms. The judiciary will supplant legislative judgment only in cases where legislatures operate without regard to norms or where legislatures' attempts to fashion new norms are unreasonable or ineffectual. Second is that the framework's particularization mechanic avoids cases that create the possibility of adjudicating non-concrete interests. The framework requires a plaintiff to allege a violation of an entrenched informational norm owed to her specifically, and doing so ensures that courts do not issue advisory opinions.

---

479. See, e.g., Ormerod, *Privacy Injuries*, *supra* note 22, at 42–43.

480. See *id.* at 39 (arguing that it is for Congress to determine an informational injury's “concreteness” and not the judiciary).

481. *Id.*

482. See Baude, *supra* note 216, at 226 (explaining that the illegality of advisory opinions is one of the “paradigm rules of Article III”).

483. See *id.* at 226–27 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring in part and concurring in the judgment) (internal quotation marks omitted)).



A second objection is that the framework is too narrow, that it only resolves informational-injury standing cases. In fact, the framework's circumscribed focus on informational injuries should instead be considered an asset. As the Supreme Court's recent ERISA standing case deftly illustrates, intangible injuries unrelated to information raise distinct considerations that cannot be resolved with reference to informational norms.<sup>484</sup> The contextual integrity framework solves a wide swath of intangible injury questions and shouldn't be cast aside because it is not a panacea for every intangible injury.

A third objection is that the framework is vague, complex, and indeterminate. Of course, some questions under the framework remain difficult. But the advantage of the framework is that it provides a principled way to analyze privacy injuries and that it eschews unknowable inquiries. Matthew B. Kugler's empirical study of biometric privacy injuries is a deft illustration of how to identify entrenched informational norms,<sup>485</sup> and computer scientists have also used contextual integrity to empirically measure informational norms.<sup>486</sup> In any event, discerning norms is considerably easier than many of the inquiries about informational injuries that courts currently engage in.<sup>487</sup> For example, scholars have recently used a survey method to reveal informational norms about internet-connected smart-home devices.<sup>488</sup> The authors' statistically significant findings<sup>489</sup> should give courts and litigants confidence that similar survey evidence can help

---

484. See *Thole v. U.S. Bank N. Am.*, 140 S. Ct. 1615, 1621 (2020) (explaining that noneconomic informational injuries still need to be "concrete" even in the context of a statutory violation).

485. See Kugler, *supra* note 400, at 119–30.

486. See, e.g., Sebastian Benthall et al., *Contextual Integrity Through the Lens of Computer Science*, 2 *FOUND. & TRENDS PRIV. & SEC.* 1, 12 (2017) ("[Contextual integrity] posits contextual information norms to model privacy expectations and explains when such expectations are morally legitimate and warrant societal protection.").

487. See, e.g., *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 116–17 (3d Cir. 2019) (speculating about the likelihood of identity theft in a FACTA case); *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016) (speculating about the "risk of real harm" in an incorrect zip code dissemination case).

488. See Apthorpe et al., *supra* note 468, at 4–9.

489. See *id.* at 11.

definitively address difficult and seemingly ambiguous questions about entrenched informational norms.

A fourth objection has surfaced previously: that a legal rule that relies so heavily on expectations is circular. This objection argues that legal rules produce norms and expectations, and therefore relying on norms and expectations to fashion legal rules is misguided because a court's use of expectations results in the judiciary merely talking to itself.<sup>490</sup>

While the theory may be intuitive, the objection is ultimately groundless because empirical research shows only the most tenuous causal relationship between judicially prescribed rules and widespread beliefs.<sup>491</sup> Matthew B. Kugler and Lior Jacob Strahilevitz have repeatedly shown that Fourth Amendment doctrine rarely tracks people's actual expectations and beliefs.<sup>492</sup> For example, Kugler and Strahilevitz have shown that a clear plurality of a representative sample of survey respondents do not draw distinctions between short- and long-term location tracking, despite numerous recent Fourth Amendment cases suggesting that the latter raises more significant constitutional problems than the former.<sup>493</sup> Even more striking, Kugler and Strahilevitz have shown that Fourth Amendment circularity is a myth—that the Supreme Court, at best, can “move privacy expectations only slightly and only for a very short time.”<sup>494</sup>

A final objection is a wholesale rejection of the framework—that we shouldn't require a *Katz*-esque reasonable-expectation-of-privacy analysis to ascertain whether a court has jurisdiction. Courts have proven poor at discerning expectations of privacy in Fourth Amendment merits determinations, the thinking goes, so inviting judges to perform a similar analysis in the civil jurisdictional context is a mistake.

There are two problems with this final objection: first, scholars have shown that actual expectations are irrelevant to

---

490. See Kugler & Strahilevitz, *The Myth*, *supra* note 336, at 1750.

491. See, e.g., Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 218–20 (2016).

492. See *id.* at 209–10 (describing how individual expectations do not align for the Supreme Court's Fourth Amendment jurisprudence).

493. See *id.* at 245–59.

494. Kugler & Strahilevitz, *The Myth*, *supra* note 336, at 1751.

Fourth Amendment decisions;<sup>495</sup> and second, pessimism about courts' ability to use actual expectations in Article III decisions isn't warranted.

As to the former, Orin S. Kerr has argued that the *Katz* inquiry only has a single objective step and has illustrated that defendants' subjective expectations are irrelevant to outcomes.<sup>496</sup> Matthew Tokson undertook a comprehensive study of reasonable-expectation-of-privacy Supreme Court decisions and found three principles that drive outcomes—the intimacy of the place or thing targeted, the amount of information sought, and the cost of the investigation.<sup>497</sup> Together, this research suggests that—notwithstanding Fourth Amendment doctrine's expectations-based nomenclature—the Fourth Amendment analysis bears little resemblance to the contextual integrity framework outlined here. And as to the latter, the illustrations in Part IV.B and the empirical research highlighted in this Part suggest that courts are perfectly capable of using informational norms and actual expectations of privacy, should they try.

#### CONCLUSION

The Supreme Court keeps saying that some statutorily authorized intangible injuries don't create an Article III injury in fact. But the Court hasn't explained how to identify injuries that are sufficient for Article III purposes and hasn't provided a justification for overriding political consensus. Scholars and jurists have attempted to bring order to the Court's recent standing jurisprudence, but those attempts have fallen short of solving these dual incoherencies with the doctrine.

This Article fills the void. Contextual integrity is a powerful tool for identifying when an injury is concrete, and fashioning a legal framework based on contextual integrity supplies courts with a justification for dismissing cases disconnected from

---

495. See Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2015) (explaining how actual expectations factor in to Fourth Amendment decisions); Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 13–30 (2020) (documenting how courts depart from human expectations when deciding a Fourth Amendment case).

496. See Kerr, *supra* note 495, at 114.

497. See Tokson, *supra* note 495, at 13–30.

shared conceptions of informational norms. The legal framework has substantial explanatory power—identifying what animates recent Article III cases and providing a roadmap for future privacy disputes.

Without a principled mechanism for evaluating intangible injury cases, standing jurisprudence threatens every individually enforceable privacy right. A contextual integrity legal framework supplies courts, legislatures, and litigants with a consistent and coherent way to protect privacy.