OPTING OUT: BIOMETRIC INFORMATION PRIVACY AND STANDING

MICHELLE JACKSON[†]

ABSTRACT

Biometric technology promises to reshape the modern economy. With the increased prevalence of biometric technology comes a heightened risk of data breaches and identity theft. To protect consumers, state legislatures have enacted biometric privacy laws. As more state legislatures define the intangible harm of data misuse, some federal courts have restricted what constitutes an injury sufficient to create Article III standing. This analysis misapplies Spokeo *and undermines legislative efforts to protect individual privacy. Because of the important interests at stake with biometric information privacy, federal courts should follow the Ninth Circuit and recognize the misuse of that data as a sufficient injury to constitute standing. Consumers usually cannot opt out of new biometric technologies implemented at airport gates, shopping centers, and workplaces. The federal courts also should not use standing doctrines to opt out of the intangible harms characterizing the information age.*

INTRODUCTION

Your face is now your boarding pass.[1] JetBlue used this slogan to announce its first fully integrated self-boarding gate, which uses facial recognition technology to verify travelers' identities.[2] This technology operates in conjunction with a partnership with U.S. Customs and Border Protection.[3] To verify a traveler's identity, the technology scans the traveler's face and checks the image against a database maintained by the Department of Homeland Security.[4] The database cross-references these

---

[†] J.D. Candidate 2020, Duke University School of Law.

[1] *Your Face is Your Boarding Pass*, JETBLUE (Nov. 15, 2018), http://mediaroom.jetblue.com/investor-relations/press-releases/2018/11-15-2018-184045420.

[2] *Id.*

[3] *Id.*

[4] Kate Patrick, *Facial Recognition Tech Goes Mainstream: Now Airlines, Retailers Spy On You, Too*, INSIDESOURCES (Apr. 29, 2019), https://www.insidesources.com/facial-recognition-tech-goes-mainstream-now-airlines-retailers-spy-on-you-too/.

images with photos from visa and passport applications, allowing Customs and Border Patrol to record the passenger's departure to determine if they overstayed their visa.[5] The Department of Homeland Security aims to use facial recognition technology to identify 97 percent of all departing air passengers within the next four years.[6] It is unclear how airline travelers can opt out of this collection method.[7]

Consumers likely cannot opt out of the coming biometric technology revolution, either. Businesses already routinely use fingerprints and facial recognition technology for surveillance, marketing, timekeeping, and tracking customers.[8] The market for biometric technology is projected to reach nearly $52 billion by 2023.[9] With the vast expansion of biometric technology comes an increased risk of data breaches and identity theft. The risk of identity theft is particularly dangerous for biometric identifiers,[10] which are completely unique to the individual.[11] Once they are compromised, "the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[12]

---

[5] Emily Birnbaum, *DHS Wants to Use Facial Recognition on 97 Percent of Departing Air Passengers by 2023*, THE HILL (Apr. 18, 2019), https://thehill.com/policy/technology/439481-dhs-wants-to-use-facial-recognition-on-97-percent-of-departing-air.

[6] *Id.*

[7] *See generally* Jason Kelley, *Skip the Surveillance by Opting Out of Face Recognition at Airports*, ELECTRONIC FRONTIER FOUNDATION (Apr. 24, 2019), https://www.eff.org/deeplinks/2019/04/skip-surveillance-opting-out-face-recognition-airports.

[8] *See, e.g.,* Chad Brooks, *The Biometric Time and Attendance System Laws You Should Know*, BUSINESS NEWS DAILY (June 10, 2019) ("Many of today's time and attendance systems offer the options of recording employee time by fingerprint, palm, iris or facial scan."); Kiely Kuligowski, *Facial Recognition Advertising: The New Way to Target Ads at Consumers*, BUSINESS NEWS DAILY (July 18, 2019) (using facial recognition technology to change product displays based on customers); Jennifer Lynch & Adam Schwartz, *Victory! Illinois Supreme Court Protects Biometric Privacy*, ELECTRONIC FRONTIER FOUNDATION (Jan. 25, 2019), https://www.eff.org/deeplinks/2019/01/victory-illinois-supreme-court-protects-biometric-privacy.

[9] Chris Burt, *Biometrics Market to Approach $52 billion by 2023 as Facial Recognition and Banking AI Expand*, BIOMETRICUPDATE.COM (Apr. 12, 2019), https://www.biometricupdate.com/201904/biometrics-market-to-approach-52-billion-by-2023-as-facial-recognition-and-banking-ai-expand.

[10] 740 ILL. COMP. STAT. 14/5(c) (2008)

[11] *Id.*

[12] *Id.*

To protect consumers, states are considering laws regulating the collection of biometric data.[13] One of the earliest and strongest versions of these statutes is the Illinois Biometric Information Privacy Act (BIPA), which regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[14] The act requires companies to obtain affirmative consent before collecting biometric information.[15] To enforce these provisions, the Act includes a private right of action.[16] Lawsuits filed under this private right of action will likely increase, especially after the Supreme Court of Illinois reduced the threshold required to bring a suit under BIPA.[17] Some law firms have established practice groups devoted to biometric privacy.[18] As biometric technology becomes more prevalent and more states pass statutes defining these rights, these trends will continue to surge.[19]

The misuse of biometric information threatens individual privacy rights. As facial recognition technology becomes ubiquitous and more companies collect and disseminate biometric information, the stakes of these injuries increase exponentially. In response to this growing threat, state legislatures have passed statutes protecting biometric information privacy. At the same time, the standing doctrine has restricted what privacy violations constitute concrete harms sufficient for Article III standing. This analysis misapplies *Spokeo*, allows federal judges to substitute their judgment over the judgment of state legislatures, and undermines the effectiveness of state legislative responses to growing threats to individual privacy. Section II of this Note provides background on the standing doctrine and demonstrates how federal courts have used *Spokeo* to restrict cognizable information privacy harms. Section III details the state statutes protecting biometric

---

[13] *See, e.g.,* Quinn Emanuel Urquhart & Sullivan, LLP, *June 2019: The Rise of Biometrics Laws and Litigation*, JD SUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/june-2019-the-rise-of-biometrics-laws-82168/.

[14] 740 ILL. COMP. STAT. 14/5(e) (2008)

[15] 740 ILL. COMP. STAT. 14/15(b) (2008)

[16] 740 ILL. COMP. STAT. 14/20 (2008)

[17] Stephen Mayhew, *Law Firms Establish Biometric Privacy Practice Groups to Focus on BIPA Claims*, BIOMETRICUPDATE.COM (Mar. 22, 2019), https://www.biometricupdate.com/201903/law-firms-establish-biometric-privacy-practice-groups-to-focus-on-bipa-claims.

[18] *Id.*

[19] *See id.* (stating that Alaska, Arizona, Connecticut, Delaware, Florida, Massachusetts, Montana, New Hampshire, and New York City are considering biometric data privacy legislation).

information and the underlying interests at stake and proposes how federal courts should analyze the harm caused by threats to biometric information privacy.

ANALYSIS

I. SPOKEO, STANDING, AND BIOMETRIC PRIVACY

Article III of the Constitution limits the judicial power of the United States only to cases and controversies.[20] To ensure that federal courts remain within this limited grant of authority, the Supreme Court developed the doctrine of standing.[21] The doctrine of standing "limits the category of litigants empowered to maintain a lawsuit in federal court to seek redress for a legal wrong."[22]

The irreducible constitutional minimum of standing requires three elements.[23] The plaintiff must have suffered an injury in fact that can be traced to the defendant's actions and will likely be redressed by a favorable decision.[24] To establish an injury in fact, a plaintiff must show that he suffered from "an invasion of a legally protected interest."[25] This invasion must be concrete, particularized, and "actual or imminent."[26] It cannot be based on a hypothetical injury.[27] An injury is particularized if it affects the plaintiff in a personal and individual way.[28]

The injury in fact must also be concrete.[29] This requirement helps to ensure that the court makes decisions based on "concrete, living contest[s] between adversaries," not abstract, intellectual hypotheticals.[30]

---

[20] U.S. CONST. Art. III, § 2.
[21] Spokeo, Inc. v. Robins (Spokeo I), 136 S. Ct. 1540, 1547, *as revised* (May 24, 2016). *See also* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013) ("The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches.").
[22] *Spokeo I*, 136 S. Ct. at 1547.
[23] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).
[24] *Id.* at 560–61.
[25] *Id.* at 560.
[26] *Id.*
[27] *Id.*
[28] Spokeo, Inc. v. Robins (Spokeo I), 136 S. Ct. 1540, 1548, *as revised* (May 24, 2016).
[29] *Id.*
[30] Fed. Election Comm'n v. Akins, 524 U.S. 11, 20 (1998) (*quoting* Coleman v. Miller, 307 U.S. 433, 460 (1939) (Frankfurter, J., dissenting)).

The injury must be real, not abstract.[31] Intangible injuries, however, may still be considered concrete for the purposes of standing analysis.[32] In determining whether an intangible harm qualifies for standing, courts should take into account history and Congressional judgment.[33] A court is more likely to recognize an intangible harm closely related to a traditional common law harm.[34] The court should also consider Congressional judgment "because Congress is well positioned to identify intangible harms that meet minimum Article III requirements."[35] Congress can elevate injuries to the statute of legally cognizable concrete injuries.[36] This also applies to state legislative judgments.[37]

In some instances, the violation of a procedural right created by statute is enough to constitute a concrete injury.[38] For example, in *Federal Election Commission v. Akins*, the inability to obtain information that should have been publicly disclosed under the Federal Election Campaign Act constituted an injury in fact.[39] The federal statute expressly authorized people to file a complaint to challenge violations of the act.[40] In light of this provision, the Supreme Court concluded that Congress intended to authorize suits challenging these violations.[41] Thus, the plaintiffs' inability to obtain information about campaign

---

[31] *Spokeo I*, 136 S. Ct. at 1548.
[32] *Id.* at 1549. ("'Concrete' is not, however, necessarily synonymous with 'tangible.'").
[33] *Id.*
[34] *See id.* ("Because the doctrine of standing derives from the case-or-controversy requirement, and because that requirement in turn is grounded in historical practice, it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.").
[35] *Id.*
[36] Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992).
[37] *See* Scanlan v. Eisenberg, 669 F.3d 838, 845 (7th Cir. 2012) (noting that the importance of federal congressional judgments and reasoning that "the same must also be true of legal rights growing out of state law") (quoting FMC Corp. v. Boesky*,* 852 F.2d 981, 993 (7th Cir. 1988)).
[38] Spokeo, Inc. v. Robins (Spokeo I), 136 S. Ct. 1540, 1549, *as revised* (May 24, 2016) ("Just as the common law permitted suit in such instances, the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact.").
[39] *See* Fed. Election Comm'n v. Akins, 118 S. Ct. 1777, 1784 (1998) ("The injury of which respondents complain—their failure to obtain relevant information—is injury of the kind that FECA seeks to address.").
[40] *See id.* at 1783 (explaining that Congress has "specifically provided" that anyone who believes FECA has been violated may file a complaint).
[41] *Id.*

donors and contributions constituted a concrete and particular injury.[42] Central to this inquiry was the importance of the interest at stake—voting.[43]

The requirement of a concrete injury is not automatically satisfied, however, whenever a statute provides a right and authorizes someone to sue for the vindication of that right.[44] In another informational injury case, *Spokeo, Inc. v. Robins*, the Supreme Court addressed whether the publication of inaccurate information in violation of the Fair Credit Reporting Act constituted a concrete injury in fact.[45] In *Spokeo*, the Supreme Court held that "Article III standing requires a concrete injury even in the context of a statutory violation."[46] The Court noted that "Congress plainly sought to curb the dissemination of false information by adopting procedures designed to decrease that risk."[47] Because the Ninth Circuit did not address whether the violations entailed "a degree of risk sufficient to meet the concreteness requirement," however, the Court remanded the case.[48]

On remand, the Ninth Circuit considered whether the injuries were sufficiently concrete for Article III standing.[49] An earlier decision from the Second Circuit interpreted *Spokeo* as instructing "that an alleged procedural violation can by itself manifest concrete injury where Congress conferred the procedural right to protect a plaintiff's concrete interests and where the procedural violation presents 'a risk of real harm' to that concrete interest."[50] The Ninth Circuit adopted this test in *Spokeo II*, asking "(1) whether the statutory provisions at issue were established to protect his concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this

---

[42] *See id.* at 1784 ("Given the language of the statute and the nature of injury, we conclude that Congress, intending to protect voters such as respondents from suffering the kind of injury at issue, intended to authorize this kind of suit.").
[43] *See id.* at 1786. ("The informational injury here, directly related to voting, the most basic of political rights, is sufficiently concrete. . . .").
[44] *See* Spokeo, Inc. v. Robins (Spokeo I), 136 S. Ct. 1540, 1548, *as revised* (May 24, 2016) (discussing the standard for establishing the concreteness and particularization of an injury).
[45] *Id.* at 1544.
[46] Frank v. Gaos, 139 S. Ct. 1041, 1045 (2019) (quoting *Spokeo I*, 136 S. Ct. at 1549).
[47] *Spokeo I*, 136 S. Ct. at 1550.
[48] *Id.*
[49] Robins v. Spokeo, Inc. (Spokeo II), 867 F.3d 1108, 1118 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 931, 200 L. Ed. 2d 204 (2018).
[50] *Strubel*, 842 F.3d at 190 (quoting *Spokeo I*, 136 S. Ct. at 1549).

case actually harm, or present a material risk of harm to, such interests."[51]

Applying this test, the Ninth Circuit found that Congress established the Fair Credit Reporting Act to protect consumers' concrete interests.[52] These interests include protecting consumers from the transmission of inaccurate information and protecting consumer privacy.[53] Because of the "ubiquity and importance of consumer reports in modern life," false information in these reports can constitute a real harm to consumers.[54] Congress likely intended to protect against this threat without showing additional injury, especially because a consumer would likely have difficulty determining exactly who accessed the credit report.[55] The Ninth Circuit also analogized the interests protected by the FRCA to other common law reputational and privacy interests, such as defamation and libel.[56] Because of these historical analogs and evidence of Congress's judgment to protect consumers, the Ninth Circuit concluded that the FRCA protected a concrete interest in accurate credit reporting.[57]

To satisfy the second part of the test for when a procedural violation constitutes a concrete injury, the violation must also cause real harm or present a material risk of harm.[58] *Spokeo II* tasked lower courts with examining specific violations to determine whether they raise a real risk of harm to the concrete injuries the statute protects.[59] The Supreme Court did not articulate exactly what qualified as real harm for inaccurate information but explained that it must be something more than an inaccurate zip code.[60] The Ninth Circuit found the inaccurate information disseminated about the plaintiff regarding his age, educational background, and employment history were likely to harm his

---

[51] *Spokeo II*, 867 F.3d at 1113.
[52] *Id.*
[53] *Id.*
[54] *Id.* at 1114.
[55] *Id.*
[56] *Id.*
[57] *Id.* at 1115.
[58] *Id*.
[59] *See id.* at 1116 (explaining that *Spokeo II* "requires some examination of the *nature* of the specific alleged reporting inaccuracies to ensure that they raise a risk of harm to the concrete interests the FCRA protects").
[60] *See* Spokeo, Inc. v. Robins (Spokeo I), 136 S. Ct. 1540, 1550, *as revised* (May 24, 2016) (noting that a "violation of one of the FCRA's procedural requirements may result in no harm").

material interests.[61] Thus, the plaintiff alleged injuries sufficiently concrete for Article III standing.[62]

Federal courts have used the test articulated in *Spokeo* to dismiss a wide range of data privacy lawsuits,[63] including cases alleging violations of biometric privacy laws.[64] In *McGinnis v. U.S. Cold Storage*, the U.S. District Court of the Northern District of Illinois held that failure to provide statutorily required notice when collecting and retaining the plaintiff's fingerprint did not constitute a concrete injury requisite for Article III standing.[65] The plaintiff did not allege anything more than a violation of the requirement in Biometric Information Privacy Act of giving notice and obtaining consent before collecting his fingerprint.[66] He did not allege disclosure to a third party or a data breach or even the risk of disclosure.[67] He simply alleged that he was required to scan his fingerprint for authentication as part of U.S. Cold Storage's time tracking system.[68] The court concluded that mere anxiety about indefinite retention of his biometric information was insufficient to establish a concrete injury for standing.[69]

Courts have stringently applied the analysis in *Spokeo* to dismiss cases for lack of standing in information privacy cases.[70] Generally, courts hesitate to recognize data-breach harms as an injury-in-fact for Article III standing.[71] This continues to be true with misuse of biometric

---

[61] *Spokeo II*, 867 F.3d at 1117.
[62] *Id.* at 1118.
[63] *See, e.g.,* Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 911–12 (7th Cir. 2017) (finding unlawful retention of customer data insufficient to justify standing); Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925, 930 (8th Cir. 2016) (finding unlawful retention of customer data insufficient to justify standing).
[64] *See, e.g.,* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12 (2d Cir. 2017); Rivera v. Google, Inc., 366 F. Supp. 3d 998 (N.D. Ill. 2018).
[65] McGinnis v. United States Cold Storage, Inc., 382 F.Supp.3d 813, 819 (N.D. Ill. 2019).
[66] *Id.* at 818.
[67] *Id.* at 819.
[68] *Id.*
[69] *Id.* at 820.
[70] *See* Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 455 (2017) (noting that "lower courts have continued to scrutinize the harms claimed by plaintiffs and to reject at least some privacy harms as insufficiently 'concrete' to support standing").
[71] *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 785 (2018) ("Looking across the

information privacy. As state legislatures continue expanding what constitutes biometric information harms, the federal courts are counteracting these efforts by restricting the harms that qualify as sufficiently concrete injuries.[72] In *Spokeo*, the Supreme Court suggested that lower courts look to history and Congressional judgment in determining whether injuries are sufficiently concrete.[73] Because *Spokeo* provided little guidance on what harms represent a real and material risk, however, lower courts have relied on their own judgment to determine what harms are sufficient.[74] This allows them to substitute their judgment for that of the state legislators and undermines the effectiveness of new biometric information privacy laws.[75]

II. PROTECTING BIOMETRIC INFORMATION PRIVACY

As biometric technology becomes more ubiquitous, state legislatures are seeking solutions to protect biometric information privacy. Some states are modeling these statutes after the Illinois' Biometric Privacy Act, which was passed in 2008. The Biometric Information Privacy Act regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[76] A biometric identifier includes "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[77] Biometric information encompasses any information "based on an individual's biometric identifier used to identify an individual."[78] Significantly, the Biometric Information Privacy Act requires companies to obtain affirmative consent from consumers before obtaining biometric data.[79]

---

body of jurisprudence of data-breach harms, it is fair to say that courts are reluctant to recognize data-breach harms.").

[72] Wu, *supra* note 70, at 455.

[73] Spokeo, Inc. v. Robins (Spokeo I), 136 S. Ct. 1540, 1550, *as revised* (May 24, 2016).

[74] *See* Wu, *supra* note 70, at 455–57 ("[L]ower courts have continued to scrutinize the harms claimed by plaintiffs and to reject at least some privacy harms as insufficiently 'concrete' to support standing.").

[75] *See* Wu, *supra* note 70, at 456 ("Such a judgment about what 'counts' as a privacy violation is precisely the sort of judgment that the Supreme Court's pre-Spokeo cases avoided but that the Spokeo decision invites.").

[76] 740 Ill. Comp. Stat. Ann. 14/5(g) (2008).

[77] 740 Ill. Comp. Stat. Ann. 14/10 (2008).

[78] *Id.*

[79] 740 Ill. Comp. Stat. Ann. 14/15(d)(1).

The Act also created a right of action for parties to recover from entities that violated the regulations on handling biometric data.[80]

The Illinois Supreme Court interpreted the Act in *Rosenbach v. Six Flags Entertainment Corporation*.[81] The court explained that the Act gives individuals the right to control their biometric information.[82] The procedural protections are important because "technology now permits the wholesale collection and storage of an individual's unique biometric identifiers – identifiers that cannot be changed if compromised or misused."[83] A company's failure to obtain consent before collecting biometric data constitutes an independent harm.[84] The right of the individual to control his or her "biometric privacy vanishes into thin air," and the harm is complete at the moment of the violation.[85]

The court explained that the procedural protection in the Biometric Information Privacy Act is not a mere technicality.[86] It is the statute's primary precautionary measure to protect biometric privacy.[87] Biometric technology is still in its infancy, and businesses do not have mechanisms to remedy these data breaches.[88] The legislature intended that the Act deter businesses from allowing biometric data breaches.[89] Furthermore, the only enforcement mechanism for this Act is the private right of action.[90] The court explained that requiring individuals "to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse . . . would be completely antithetical to the Act's preventative and deterrent purposes."[91] Thus, the court concluded that a plaintiff does not need to allege injury beyond the violation of the rights protected by the Biometric Information Privacy Act.[92]

---

[80] 740 Ill. Comp. Stat. Ann. 14/20.
[81] Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1201–02, (Ill. 2019).
[82] *Id.*
[83] *Id.* (quoting Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).
[84] *Id.*
[85] *Id.* (quoting Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).
[86] *Id.* at *7.
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.* at *8.

Rosenbach was decided about a month after the federal district court came to the opposite conclusion in *McGinnis*. Applying *Spokeo*, violations of the notice-and-consent provisions of the Biometric Information Privacy Act should "by itself manifest concrete injury."[93] The state legislature conferred a procedural right to protect consumer's concrete interests, and the violation of that procedural right presents a risk of real harm to that interest.[94] Furthermore, the Illinois Supreme Court reiterated that the violation of this procedural right constituted an independent harm to the consumer's ability to control his or her biometric information privacy.[95] This harm goes far beyond the hypothetical incorrect zip code the Supreme Court mentioned in *Spokeo*. Zip codes can be altered. Biometric information cannot. Once biometric information is misused, a consumer has no recourse. The violation of this intangible harm constitutes an injury in fact.

How federal courts will interpret the Illinois Biometric Information Privacy Act in light of *Rosenbach* remains unclear. After *Rosenbach*, the Seventh Circuit upheld standing for an alleged violation of the Biometric Information Privacy Act in *Miller v. Southwest Airlines*.[96] In *Miller*, plaintiffs alleged that the airlines use of fingerprints for timekeeping purposes violated the Biometric Information Privacy Act.[97] The potential impact on the workers' terms and conditions of employment gave the case a concrete injury not present in *Spokeo*.[98] The Seventh Circuit has not yet decided a case with similar facts as *Rosenbach*.[99] In past decisions not involving the Biometric Information Privacy Act, the Seventh Circuit has held that retaining personal information did not constitute a concrete injury.[100]

How federal courts respond to future standing challenges involving biometric information privacy will determine the effectiveness of state legislative attempts to protect biometric information. Federal

---

[93] *See* Robins v. Spokeo, Inc. (Spokeo II), 867 F.3d 1108, 1113 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 931 (2018).
[94] Strubel v. Comenity Bank, 842 F.3d 181, 190 (2d Cir. 2016) (quoting Spokeo, Inc. v. Robins (Spokeo I), 136 S. Ct. 1540, 1559, *as revised* (May 24, 2016)).
[95] *Rosenbach*, 129 N.E.3d at 1197, 1201–02.
[96] Miller v. Sw. Airlines Co., 926 F.3d 898, 902 (7th Cir. 2019).
[97] *Id.* at 901.
[98] *Id.* at 902.
[99] The court may have an opportunity to hear a case with similar facts with the appeal from Rivera v. Google, Inc., 366 F. Supp. 3d 998 (N.D. Ill. 2018) (dismissing for lack of standing).
[100] *Rivera*, 366 F. Supp. 3d at 1005 (citing Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 912–13 (7th Cir. 2017)).

judges may have concerns about the impending flood of litigation accompanying these statutes or whether the notice-and-consent provisions are appropriate remedies for violations of biometric information privacy. They should not use standing doctrines, however, to supersede the judgments of state legislatures.[101] The rapid proliferation of facial recognition technology requires a quick, informed response by state legislatures. Allowing courts to scrutinize which privacy harms are cognizable and which are not "undermines the legislature's ability to act to prevent harms proactively."[102] For now, private enforcement is the primacy mechanism to prevent violations of biometric information privacy.[103] Denying relief by characterizing a privacy harm as the wrong kind of harm impedes this enforcement mechanism.[104]

Rather than deepening the split between federal and state courts and between the federal circuits, federal courts should follow the lead of the Ninth Circuit. In *Patel v. Facebook*, the Ninth Circuit concluded that Facebook's collection of the plaintiffs' face templates constituted a concrete injury sufficient for Article III standing.[105] The court explained that the right protected by the Biometric Information Privacy Act was the right to not be subject to the collection of biometric data.[106] Thus, Facebook's violation of the procedural requirements under BIPA violated the plaintiffs' substantive privacy interests.[107] Quoting *Rosenbach*, the court explained that "when a private entity fails to adhere to the statutory procedures . . . the right of the individual to maintain his

---

[101] *See* Wu, *supra* note 70, at 458 ("When courts deny standing in these cases on the basis of the injuries being insufficiently concrete, they are not deciding whether the cases are ones that concern individual rights, but rather deciding the substantive content of those rights. Far from supporting an appropriate separation of powers, this move amounts to a usurpation of legislative power by the federal judiciary.").

[102] *See id.* at 459 ("Moreover, scrutiny of harms undermines the legislature's ability to act to prevent harms proactively, rather than only addressing completed harms.").

[103] *See id.* at 460 ("Denying standing on the basis of the harm being the wrong kind of harm essentially takes private lawsuits in federal courts out of the picture entirely. While the possibility of purely executive or administrative action would remain, such a rule can severely hamper the government's ability to regulate the challenged activity by removing an important tool from the regulatory toolbox.").

[104] *Id.* at 460.

[105] Patel v. Facebook, Inc., 932 F.3d 1264, 1275 (9th Cir. 2019).

[106] *Id.* at 1274.

[107] *Id.*

or her biometric privacy vanishes into thin air."[108] To prevent protections of biometric privacy from vanishing, federal courts should recognize the substantive rights of privacy protected by statutes like the Biometric Information Privacy Act.

CONCLUSION

Biometric technology promises to reshape modern commerce, transportation, law enforcement, and more. The greatest injuries will likely be intangible and based on ephemeral interests in information privacy.[109] As state legislatures attempt to define these intangible harms, the federal courts should not use standing to opt out of providing remedies.

---

[108] *Id*. (quoting Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1201–02 (Ill. 2019)).

[109] *See* Seth F. Kreimer, *"Spooky Action at A Distance": Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745 (2016).