BIPA AND ARTICLE III STANDING: ARE NOTICE AND CONSENT MORE THAN "BARE PROCEDURAL" RIGHTS?

Carmen Sobczak†

I. INTRODUCTION

Modern technology has increasingly come to rely on the private sector's collection and use of biometric data. Many individuals willingly hand over this data to facilitate interactions with electronic devices, happy to scan fingerprints and facial geometries so they can unlock their smartphones without a password. Companies also give customers the option to supply biometrics for enhanced security. For example, several banks authenticate clients with fingerprints, voiceprints, face scans, or iris scans.[1] Some biometric data collection, however, is far less voluntary. Schools, employers, and churches use fingerprints and face scans to track attendance.[2] Hundreds of retail stores have purchased facial recognition systems to "identify known shoplifters," and can share data with other businesses without providing any notice to their customers.[3] Video doorbells equipped with facial recognition, like Nest,

DOI: https://doi.org/10.15779/Z38W669904

† J.D. 2021, University of California, Berkeley, School of Law. Sincere thanks to Jim Dempsey, Professors Kenneth Bamberger and Talha Syed, my fellow students in the 2019 Law & Technology Writing Workshop at Berkeley Law, and the Berkeley Technology Law Journal editors.

1. *See BofA Merrill Adds Biometrics and Integrated Token to CashPro® Mobile*, BANK OF AM. (July 2, 2018, 9:00 AM), https://newsroom.bankofamerica.com/press-releases/corporate-and-investment-banking-sales-and-trading-treasury-services/bofa-merrill-18; Dan Hansen, *Voiceprint: A Security Game-Changer for Banks and Credit Unions of All Sizes*, BIZTECH (Nov. 5, 2018), https://biztechmagazine.com/article/2018/11/voiceprint-security-game-changer-banks-and-credit-unions-all-sizes; *BBVA, The First Bank with Access to Its Mobile App Via Iris Scanning, Thanks to Samsung*, BBVA (Nov. 16, 2017), https://www.bbva.com/en/bbva-first-bank-access-mobile-app-iris-scanning-thanks-samsung.

2. *See* Nicole Nguyen, *Chokepoint: Regulating US Student Mobility Through Biometrics*, 46 POL. GEOGRAPHY 1, 2 (2015); Selena Larson, *Beyond Passwords: Companies Use Fingerprints and Digital Behavior to ID Employees*, CNN BUS. (Mar. 18, 2018, 3:35 PM), https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html; *Face Recognition App — The Churchix App*, CHURCHIX, https://churchix.com/face-recognition-app (last visited Feb. 3, 2021).

3. *See* Alfred Ng, *With Facial Recognition, Shoplifting May Get You Banned in Places You've Never Been*, CNET (Mar. 20, 2019, 8:11 AM), https://www.cnet.com/news/with-facial-recognition-shoplifting-may-get-you-banned-in-places-youve-never-been.

empower the homeowner to scan and identify any person who approaches their door.[4]

While biometric information can greatly increase efficiency and security, its collection, use, and storage pose significant threats to individual privacy. Biometric identifiers are distinct from other forms of identification; unlike social security numbers, they are impossible—or, at least, incredibly difficult, expensive, and painful—to change.[5] This permanence drastically raises the stakes of identity theft and fraud.[6] Moreover, each novel application of biometric technology introduces new threats, such as the clear risk of racial profiling in software used to identify shoplifters.[7] Risks like these are exacerbated by the fact that facial recognition technologies can be inaccurate and have been found to disproportionately misidentify people of color.[8] The rapidly growing use of biometric data in the private sector also fuels fears surrounding corporate mass surveillance, as cameras with identification capacity can significantly chill freedoms of speech, assembly, and association.[9] And corporate surveillance has begun to look more and more like government surveillance through public-private partnerships that give law enforcement agencies access to video footage from individually-owned cameras.[10]

---

4. *See* Samuel Gibbs, *Nest Hello Review: Google's Smart Facial-Recognition Video Doorbell*, THE GUARDIAN (Sept. 20, 2018, 4:33 AM), https://www.theguardian.com/technology/2018/sep/20/nest-hello-review-google-smart-facial-recognition-video-doorbell.

5. *See* Adam Schwartz, *The Danger of Corporate Facial Recognition Tech*, ELEC. FRONTIER FOUND. (June 7, 2016), https://www.eff.org/deeplinks/2016/06/danger-corporate-facial-recognition-tech.

6. *See id.*

7. *See id.*

8. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, AM. CIVIL LIBERTIES UNION (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

9. *See* Farhad Manjoo, *San Francisco is Right: Facial Recognition Must be Put on Hold*, N.Y. TIMES (May 16, 2019), https://www.nytimes.com/2019/05/16/opinion/columnists/facial-recognition-ban-privacy.html; Sigal Samuel, *Activists Want Congress to Ban Facial Recognition. So They Scanned Lawmakers' Faces.*, VOX (Nov. 15, 2019, 10:10 AM), https://www.vox.com/future-perfect/2019/11/15/20965325/facial-recognition-ban-congress-activism.

10. *See* Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach; Rani Molla, *Activists Are Pressuring Lawmakers to Stop Amazon Ring's Police Surveillance Partnerships*, VOX (Oct. 8, 2019, 7:00 AM), https://www.vox.com/recode/2019/10/8/20903536/amazon-ring-doorbell-civil-rights-police-partnerships.

In 2008, Illinois became the first state to enact a statute explicitly protecting biometric privacy.[11] Following the notable bankruptcy of Pay By Touch, a company that created systems for fingerprint-based purchasing, the General Assembly grew concerned about the fate of residents' biometric data.[12] Representative Kathy Ryg asserted that in light of the sale of the Pay By Touch database to a third party, Illinois was in "serious need of protections for [its] citizens . . . when it [came] to biometric information."[13] The Illinois Biometric Information Privacy Act (BIPA), which regulates the collection and retention of biometric data and prohibits its sale, passed unanimously.[14]

While several states have since approved similar legislation giving individuals control over their biometric data, BIPA is thus far unique in that it empowers Illinois residents to enforce that control through a private right of action.[15] Those who are "aggrieved by a violation of" the statute can sue for liquidated damages of up to $5,000.[16]

Beginning in 2019, courts began to see a "flood" of class actions brought under BIPA, including a lawsuit against Facebook that settled for $650 million.[17] Many of these cases raised the question of whether plaintiffs can sue for a procedural infringement of BIPA without showing additional harm. The Illinois Supreme Court definitively held in 2019 that they can, establishing that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act," to bring suit in state court.[18] But federal courts split as to whether such infringements satisfy constitutional

11. *See* 740 ILL. COMP. STAT. 14/1–14/99 (2008); Thomas F. Zych, Steven G. Stransky & Brian Doyle-Wenger, *State Biometric Privacy Legislation: What You Need to Know*, LEXOLOGY (Sept. 5, 2019), https://www.lexology.com/library/detail.aspx?g=ebc0e01c-45cc-4d50-959e-75434b93b250.

12. H.R. Deb. Transcript, 95th Gen. Assemb. No. 276 (Ill. 2008) (statement of Rep. Kathy Ryg).

13. *Id.*

14. *See* S.B. 2400: S. Vote, 3d Reading, 95th Gen. Assemb. (Ill. 2008); S.B. 2400: H.R. Roll Call, 3d Reading, 95th Gen. Assemb. (Ill. 2008).

15. Texas and Washington also enacted legislation specifically protecting biometric privacy, though neither includes a private right of action. Quinn Emanuel Urquhart & Sullivan, LLP, *June 2019: The Rise of Biometric Laws and Litigation*, JDSUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/june-2019-the-rise-of-biometrics-laws-82168. Arkansas, California, and New York all amended statutory definitions of personal information to include biometrics. Zych et al., *State Biometric Privacy Legislation*, *supra* note 11.

16. 740 ILL. COMP. STAT. 14/20 (2021).

17. *See* Tiffany Cheung, Michael Burshteyn & Camille Framroze, *Privacy Litigation 2020 Year in Review: BIPA Litigation*, MORRISON FOERSTER (Jan. 12, 2021), https://www.mofo.com/resources/insights/210111-bipa-litigation.html; Taylor Hatmaker; *Facebook Will Pay $650 Million to Settle Class Action Suit Centered on Illinois Privacy Law*, TECHCRUNCH (Mar. 1, 2021 1:36 PM), https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa.

18. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 40 (2019).

standing requirements. In particular, courts disagreed over whether plaintiffs suffer an injury in fact for the purposes of Article III standing when their only alleged harm is the collection of their biometric data without written notice and consent in violation of BIPA section 15(b).[19] In 2017, the Second Circuit answered this question in the negative.[20] The Ninth Circuit concluded the opposite two years later, becoming the first federal appellate court to hold that a procedural violation of BIPA can amount to an injury in fact.[21] And in 2020, the Seventh Circuit sided with the Ninth,[22] settling a robust debate in the Illinois district courts.

Making sense of BIPA's private right of action, particularly as it relates to the statute's notice and consent requirements, is critical for understanding the current landscape of biometric privacy protection—and the enforceability of privacy rights in general—in the United States. First, as evidenced by the Facebook lawsuit, BIPA has had a huge impact on global companies, who now face massive liability for violations of one state's statute. Plaintiffs have brought suit against Google, Amazon, Snapchat, Vimeo, Juul, WeWork, Home Depot, Dr. Pepper, and many other companies, both technology-centered and not.[23] The ACLU also relied on BIPA section 15(b) as the basis for a lawsuit

19. *See* 740 ILL. COMP. STAT. 14/15(b) (2021) (establishing a written notice and consent regime for the collection of biometric data). Federal cases were brought under other BIPA provisions as well, but this Note focuses on section 15(b).

20. Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12 (2d Cir. 2017) (summary order).

21. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.).

22. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).

23. *See* Jennifer Lynch & Adam Schwartz, *Victory! Illinois Supreme Court Protects Biometric Privacy*, ELEC. FRONTIER FOUND. (Jan. 25, 2019), https://www.eff.org/deeplinks/2019/01/victory-illinois-supreme-court-protects-biometric-privacy; Daniel R. Stoller, *Amazon Says Alexa Biometric Privacy Claims Should be Dismissed*, BLOOMBERG LAW (Dec. 10, 2019, 9:29 AM), https://news.bloomberglaw.com/privacy-and-data-security/amazon-says-alexa-biometric-privacy-claims-should-be-dismissed; Maryam Casbarro, *Update from LitLand: Vimeo Faces BIPA Lawsuit*, JDSUPRA (Nov. 8, 2019), https://www.jdsupra.com/legalnews/update-from-litland-vimeo-faces-bipa-40471; Chris Burt, *Juul and WeWork Sued Under BIPA for Collecting Customer Biometrics*, BIOMETRICUPDATE (Nov. 8, 2019), https://www.biometricupdate.com/201911/juul-and-wework-sued-under-bipa-for-collecting-customer-biometrics; Chris Burt, *BIPA Suit Brought Against Home Depot for Loss Prevention Biometrics*, BIOMETRICUPDATE (Sept. 9, 2019), https://www.biometricupdate.com/201909/bipa-suit-brought-against-home-depot-for-loss-prevention-biometrics; Daniel R. Stoller, *Dr. Pepper Employee Biometric Privacy Case Moves to Federal Court*, BLOOMBERG LAW (Nov. 1, 2019, 11:07 AM), https://news.bloomberglaw.com/privacy-and-data-security/dr-pepper-employee-biometric-privacy-case-moves-to-federal-court.

against controversial facial recognition company Clearview AI.[24] Second, Illinois's experience with BIPA lawsuits will likely influence other states' decisions regarding their own biometric legislation.[25] Absent a federal statute,[26] states are acting on their own, and in different ways, to grant residents control over biometric data. BIPA is currently serving as an experiment on whether private enforcement of biometric privacy statutes is desirable, both from legal and policy standpoints.[27] Finally, the debate over standing to sue for violations of section 15(b)'s notice and consent requirements could inform other spheres of privacy regulation, as notice and consent regimes are considered "[t]he dominant legal and regulatory approach to protecting information privacy."[28]

This Note explores the question of standing in BIPA litigation involving allegations that companies have collected biometric data without notice and consent in violation of section 15(b). Ultimately, it argues that section 15(b) protects a concrete privacy interest in controlling information about oneself, an interest that courts have long recognized and the Illinois legislature intended to safeguard. This satisfies the Supreme Court's Article III standing requirements for procedural violations as set forth in *Spokeo, Inc. v. Robins*.[29] As

24. Complaint at 31–32, Am. Civil Liberties Union v. Clearview AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct., Cook Cty., Ch. Div. May 28, 2020), https://www.aclu.org/sites/default/files/field_document/2020.05.28_aclu-clearview_complaint_file_stamped.pdf.

25. In January 2021, New York legislators introduced a bill, the Biometric Privacy Act (A.B. 27), that has been called a "carbon copy" of BIPA. Lydia de la Torre, *A New York BIPA in the Making?*, NAT'L L. REV. (Jan. 28, 2021), https://www.natlawreview.com/article/new-york-bipa-making.

26. In 2020, a bill introduced in the U.S. Senate proposed a National Biometric Information Privacy Act, modeled after BIPA and containing a private right of action. Joseph J. Lazzarotti, *National Biometric Information Privacy Act, Proposed by Sens. Jeff Merkley and Bernie Sanders*, NAT'L L. REV. (Aug. 5, 2020), https://www.natlawreview.com/article/national-biometric-information-privacy-act-proposed-sens-jeff-merkley-and-bernie.

27. The Illinois legislature has itself considered amending BIPA several times in response to the numerous lawsuits brought under the statute. In 2019, a bill was introduced and ultimately abandoned that would have removed BIPA's private right of action. Meghan C. O'Connor, Gary R. Clark & Sarah A. Erdmann, *Illinois Introduces Bills to Amend BIPA Taking Away Private Right of Action and Adding ECGs*, QUARLES & BRADY LLP (Apr. 25, 2019), https://www.quarles.com/publications/illinois-introduces-bills-to-amend-bipa-taking-away-private-right-of-action-and-adding-ecgs. And in March 2021, the Illinois House Judiciary Committee introduced a bill that would (among other amendments) allow electronic consent in place of written consent and create a thirty-day "notice and cure" period before a lawsuit could be brought. Gordon Rees Scully Mansukhani, *Is Illinois Moving Away from its Strict BIPA Law?*, LEXOLOGY (Mar. 15, 2021), https://www.lexology.com/library/detail.aspx?g=27375046-9836-47d3-95de-5f1dadf50144. This bill was motivated by the concern that massive class actions brought under BIPA could harm small businesses in Illinois. *Id.*

28. Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't*, 9 J. INFO. POL'Y 148, 148 (2019).

29. 136 S. Ct. 1540 (2016).

such, plaintiffs alleging section 15(b) violations should not be denied standing in federal court for failure to assert a concrete injury.

Part II of this Note describes BIPA's provisions. Part III explains the current standing landscape of section 15(b) cases in state and federal court. Part IV discusses the privacy interests protected by the statute and then contends that violations of BIPA's notice and consent requirements should amount to concrete injuries for the purposes of Article III standing. Finally, this Note concludes by raising questions about the broader implications of the BIPA standing debate.

II. UNDERSTANDING BIPA'S PROVISIONS

BIPA regulates the collection, use, and disclosure of biometric information. The statute defines a "[b]iometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[30] Biological materials and other medical data, such as x-rays and MRIs, do not fall under the statute.[31] Although BIPA explicitly states that photographs are not biometric identifiers,[32] several courts have either assumed or explicitly held that scans of facial geometry captured from photographs do constitute biometric data.[33] The question of whether information amounts to biometric data under the statute does not depend on how the data is captured.[34] Finally, BIPA only applies to private entities, not government agencies or judicial employees.[35]

BIPA contains five restrictions. First, section 15(b) prohibits companies from collecting data without notice and consent. To "collect, capture, purchase, receive through trade, or otherwise obtain" a data subject's biometric data, a private entity must first (1) give the data subject a written notice explaining that the data is being collected, describing the purpose for collection, and placing a limit on retention; and (2) obtain the subject's written consent.[36] Second, after collection, biometric data must be stored, transmitted, and secured in a commercially reasonable manner.[37] These data security

30. 740 ILL. COMP. STAT. 14/10 (2021).

31. *Id.*

32. *Id.*

33. *See, e.g.*, Patel v. Facebook, Inc., 932 F.3d 1264, 1276 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.); Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1001 (N.D. Ill. 2018), *abrogated on other grounds by* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020); Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017); Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

34. 740 ILL. COMP. STAT. 14/10 (2021).

35. *Id.*

36. *Id.* 14/15(b).

37. *Id.* 14/15(e).

safeguards must be at least as strong as those that the company employs to protect other types of sensitive personal information.[38] Third, a company must destroy biometric data once the purpose for collection is satisfied or once three years have passed since the data subject last interacted with the company, whichever comes first.[39] The company must also maintain a publicly available, written notice describing its retention and destruction policy.[40] Fourth, a company cannot disclose biometric data to a third party without the data subject's consent, unless the disclosure "completes a financial transaction" authorized by the subject or is required by law.[41] And finally, BIPA prohibits companies from profiting off of an individual's biometric identifiers, through sale, lease, or otherwise.[42]

BIPA contains a private right of action, which permits individuals "aggrieved by a violation of [the] Act" to sue a company for violating the statute's provisions.[43] Successful plaintiffs can collect the greater of actual damages or liquidated damages of $1,000 for each negligent violation, and they can collect the greater of actual damages or liquidated damages of $5,000 for each intentional or reckless violation.[44] They can also recover reasonable attorneys' fees and obtain appropriate injunctive relief.[45]

III. THE CURRENT STANDING LANDSCAPE FOR BIPA SECTION 15(B) CASES

Although BIPA provides a private right of action for "aggrieved" Illinois residents, courts have grappled with whether violations of the notice and consent requirements in section 15(b) are sufficient to grant plaintiffs standing without further injury.[46] The debate over standing in Illinois state court, which rested on the statutory interpretation of "aggrieved," was resolved in January 2019, when the state supreme court held that any violation of a right granted

38. *Id.*
39. *Id.* 14/15(a).
40. *Id.*
41. *Id.* 14/15(d).
42. *Id.* 14/15(c).
43. *Id.* 14/20 ("Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party.").
44. *Id.*
45. *Id.*
46. *Compare* Patel v. Facebook, Inc., 932 F.3d 1264, 1267–68 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.), *with* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1014 (N.D. Ill. 2018), *abrogated on other grounds by* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020)..

under BIPA could confer standing.[47] But the approach to answering the standing question is different in federal courts, which are limited in their jurisdiction by Article III of the Constitution and can only hear cases brought by plaintiffs who have suffered a concrete "injury in fact."[48]

This Part describes how state and federal courts have addressed the standing question in section 15(b) lawsuits thus far.

A. STATUTORY STANDING IN ILLINOIS STATE COURT

In 2019, the Illinois Supreme Court decided *Rosenbach v. Six Flags*, which established that plaintiffs can sue in state court for a violation of BIPA's provisions even if they suffer no additional harm.[49] The court held, "[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under [BIPA], in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[50]

Rosenbach involved Six Flags' practice of collecting and storing the fingerprints of visitors with season passes in order to authenticate their identities and grant them access to the amusement park.[51] The plaintiff, a fourteen-year-old named Alexander Rosenbach, went on a school field trip to Six Flags.[52] Because his mother had purchased a season pass for him prior to the outing, he was asked to scan his thumbprint upon arrival at the park.[53] Neither Rosenbach nor his mother received written notice informing them of the fact that fingerprints would be collected, describing the purpose for doing so, or indicating how long the data would be retained.[54] Additionally, they had no opportunity to grant or deny consent in writing.[55] Rosenbach sued under BIPA section 15(b), seeking statutory damages and an injunction requiring Six Flags to adhere to the statute's requirements.[56] Six Flags filed a motion to dismiss, arguing that Rosenbach lacked standing to sue because he had not suffered any real or threatened harm.[57]

47. *See* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186 (2019).
48. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).
49. 2019 IL 123186, ¶ 40.
50. *Id.*
51. *Id.* ¶ 4.
52. *Id.* ¶ 5.
53. *Id.* ¶¶ 5–6.
54. *Id.* ¶¶ 8–9.
55. *Id.* ¶ 8.
56. *Id.* ¶ 11.
57. *Id.* ¶ 12.

Relying first on principles of statutory construction, the court held that the plain meaning of the statute evinced the legislature's intent to allow individuals to sue without showing additional injury.[58] Section 20 states that anyone "aggrieved by a violation" of BIPA's provisions has a right of action.[59] Illinois jurisprudence had previously interpreted "aggrieved" to refer to a person who has suffered an invasion of a legal right,[60] and dictionary definitions were consistent with that understanding.[61] Therefore, the court found that the legislature would have intended "aggrieved" to have this meaning.[62] And because BIPA did grant individuals a legal right—namely, "a right to privacy in and control over their biometric identifiers," safeguarded "by requiring notice before collection and giving them the power to say no by withholding consent"—the legislature must have meant to permit lawsuits for invasions of this right without requiring additional harm.[63]

Second, the court found that procedural violations of BIPA's right to biometric privacy and control are not "merely 'technical' in nature."[64] Rather, it wrote, "When a private entity fails to adhere to the statutory procedures, . . . 'the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.' "[65] Such a harm "is no mere 'technicality' " but a "real and significant" injury.[66] Thus, the court held, plaintiffs suing under BIPA in Illinois state court are not required to allege actual injury beyond a violation of the statute's provisions.[67]

B. ARTICLE III STANDING IN FEDERAL COURT

While plaintiffs have a clear avenue to bring BIPA lawsuits in Illinois state court, federal courts have split on the question of whether violations of section 15(b) confer Article III standing.

1. The Article III Standing Requirement for Intangible Harms

The modern federal standing doctrine has its origins in Article III of the U.S. Constitution, which limits federal courts' jurisdiction to cases and

58. *See id.* ¶¶ 24–25.
59. 740 ILL. COMP. STAT. 14/20 (2021).
60. *Rosenbach*, 2019 IL 123186, ¶¶ 30–31.
61. *Id.* ¶ 32.
62. *Id.*
63. *Id.* ¶¶ 33, 34 (citing Patel v. Facebook Inc., 290 F. Supp. 3d 948, 953 (N.D. Cal. 2018)).
64. *Id.* ¶ 34.
65. *Id.* (quoting *Patel*, 290 F. Supp. 3d at 954).
66. *Id.*
67. *Id.* ¶ 40.

controversies.[68] Although the Constitution is silent on the question of who may bring suit in Article III courts, the Supreme Court has held that the Case or Controversy Clause requires plaintiffs to meet an "irreducible constitutional minimum of standing."[69] Three elements compose this minimum. First, plaintiffs must be able to show that they "suffered an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent."[70] Second, the defendant's actions must have caused the injury.[71] And third, it must be likely that the injury can be remedied by a favorable judicial outcome.[72]

Spokeo, Inc. v. Robins made it clear that even intangible injuries can meet Article III's requirement of concreteness.[73] When intangible harm results from the violation of procedural statutory rights, courts must inquire into the legitimacy of the interests that those rights were designed to protect. *Spokeo* involved a violation of the Fair Credit Reporting Act (FCRA), which, among other things, requires that credit reporting agencies follow certain procedures to ensure that the information they put forth about consumers is as accurate as possible.[74] The Court faced the question of whether the violation of that requirement—an intangible injury—could amount to a concrete harm for the purposes of the Article III analysis. Ultimately, although somewhat opaquely, the Court held that it could. Justice Alito wrote for the majority, "[T]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified."[75] But, "[d]eprivation of a procedural right without some concrete interest that is affected by the deprivation . . . is insufficient to create Article

68. U.S. CONST. art. III, § 2.

69. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

70. *Id.* at 560 (internal quotations, footnote, and citations omitted).

71. *Id.*

72. *Id.* at 561.

73. 136 S. Ct. 1540 (2016).

74. *Id.* at 1545. The defendant, Spokeo, was a reporting agency that sold information about consumers, aggregated from across the internet, to prospective employers, romantic partners, and others wishing to learn about a particular individual. *Id.* at 1546. Robins became aware that his profile on Spokeo's website contained inaccurate information regarding his age, wealth, level of education, and employment status. *Id.* He sued Spokeo for failing to comply with FCRA's accuracy requirement. *Id.* On appeal from the district court, where Robins's claim had been dismissed for lack of standing, the Ninth Circuit held that Robins met the injury in fact requirement because his particular statutory rights had been violated. *Id.* at 1544–45. The Supreme Court remanded the case to the Ninth Circuit to consider whether Robins's injury was concrete as well as particularized. *Id.* at 1545.

75. *Id.* at 1549.

III standing."[76] Put simply, the procedural right infringed upon cannot be *merely* procedural; it must protect a concrete interest.[77]

The Court identified two sources that would help determine whether an intangible statutory violation is sufficiently concrete. First, it directed lower courts to consider common law history. An intangible harm that "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts" is more likely to constitute an injury in fact.[78] Second, the legislature's judgment plays an important role, because lawmakers are well-positioned to identify which harms meet the Article III test.[79] The Court wrote, "Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.' "[80] But, the Court also stated, "Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing."[81]

Scholars have lamented the muddied analysis in *Spokeo*. Lauren E. Willis, a professor, wrote, "The majority opinion in *Spokeo* reads like a bad law student exam . . . . First, it sets forth superficial and facially contradictory statements . . . with no resolution of those conflicts. Second, it never discusses how those rules apply to the facts of this case."[82] Some commentators question whether *Spokeo* changed the legal landscape at all,[83] and judges disagree about whether the case creates a useful framework to guide the standing analysis.[84] The Supreme Court, however, has declined to revisit the question, denying

76. *Id.* (quoting Summers v. Earth Island Inst., 555 U.S. 488, 496 (2009)).

77. The majority gave the example of an incorrect zip code as a "bare" procedural violation. *Id.* at 1550. The dissent contrasted this with the harm that Robins experienced, arguing that incorrect information about his family, employment, and financial status "could affect his fortune in the job market" and thus amounted to a sufficiently concrete harm. *Id.* at 1556 (Ginsburg, J., dissenting).

78. *Id.* at 1549 (majority opinion).

79. *Id.*

80. *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992)).

81. *Id.* at 1547–48 (quoting Raines v. Byrd, 521 U.S. 811, 820 n.3 (1997)).

82. Lauren E. Willis, Spokeo *Misspeaks*, 50 LOY. L. A. L. REV. 233, 238 (2017).

83. *Compare* Thomas v. FTS USA, LLC, 193 F. Supp. 3d 623, 629 (E.D. Va. 2016) ("Spokeo did not change the basic requirements of standing."), *with* Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 452, 457 (2017) (explaining that *Spokeo* "requires the courts to assess the nature and cognizability of harms in a way that the Supreme Court had not been doing before" and labeling its holding a "doctrinal shift").

84. *See* Matthew S. DeLuca, Note, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2456 (2018).

certiorari in several cases involving the lower courts' varying interpretations of *Spokeo*.[85]

Despite *Spokeo*'s lack of clarity, its language and reasoning suggest a series of questions that courts should ask when assessing whether an intangible injury stemming from a statutory violation is sufficiently concrete to establish standing. First, is the statutory provision at issue procedural or substantive? *Spokeo*'s analysis applies only to procedural requirements; the credit reporting agency in the case had to follow certain steps (i.e., a procedure) to assure reasonable accuracy of information.[86] But some statutory provisions establish substantive requirements. For example, in *Eichenberger v. ESPN, Inc.*, the Ninth Circuit wrote that a section of the Video Privacy Protection Act outlawing disclosure of a person's video-viewing data "does not describe a procedure that video service providers must follow. Rather, it protects generally a consumer's substantive privacy interest in his or her video-viewing history."[87] While infringements of both procedural and substantive provisions can result in intangible harms, courts will have an easier time finding a concrete injury when the violated provision is itself substantive.[88]

If the provision is procedural, a second distinction arises: is it a "bare" procedural requirement or one whose violation results in concrete harm?[89] In other words, does the provision protect a concrete interest or not? This is the question the court grappled with in *Spokeo*, and it is where common law history and legislative intent become relevant. In addition to these factors, *Spokeo* also suggests that sometimes the answer depends on factual context. A violation of the same clause might give rise to Article III standing in some cases but not others. For example, if Spokeo's failure to follow reasonable procedures to ensure accuracy resulted in the posting of an incorrect zip code, Robins would have suffered a "bare procedural violation" and would not have had standing.[90]

---

85. *See* Lee J. Plave & John W. Edson, *First Steps in Data Privacy Cases: Article III Standing*, 37 FRANCHISE L.J. 485, 505 (2018).

86. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016).

87. 876 F.3d 979, 983 (9th Cir. 2017).

88. *See id.* ("Accordingly, *every* disclosure of an individual's 'personally identifiable information' and video-viewing history offends the interests that the statute protects.").

89. *See Spokeo*, 136 S. Ct. at 1549 ("[D]eprivation of a procedural right without some concrete interest that is affected by the deprivation . . . is insufficient to create Article III standing." (quoting Summers v. Earth Island Inst., 555 U.S. 488, 496 (2009))). But, "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact." *Id.*

90. *Id.* at 1550. The Court also gives an example of a "bare procedural violation" of FCRA's notice requirement, writing, "[E]ven if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless

But, as the dissent noted and the Ninth Circuit held on remand, failure to verify the accuracy of familial, educational, and financial information implicated Robins's concrete interests through potential effects on his employment prospects, and he therefore had standing to sue.[91]

Although the Supreme Court has not directly stated that *Spokeo* applies to violations of state statutes as well as federal ones, several courts have suggested that it does. Two pre-*Spokeo* cases, one in the Seventh Circuit and one in the Ninth, held that a violation of state law can amount to an injury in fact that grants plaintiffs Article III standing.[92] In 2016, a district court relied on one of those cases in finding that, since "*Spokeo* said nothing about the ability of state legislatures to create rights sufficient to confer Article III standing," precedent recognizing standing for injuries to state legal rights was controlling.[93] And in two cases discussed below, when assessing whether plaintiffs had standing to sue for BIPA violations, the Seventh and Ninth Circuits both unquestioningly applied *Spokeo*'s analysis to the Illinois statute, considering the General Assembly's intent in lieu of Congress's.[94] The Supreme Court had a chance to review the Ninth Circuit's holding, but denied certiorari.[95] Of course, the injury claimed as the result of a state statutory violation must still meet the *Spokeo* requirement of concreteness; a bare procedural infringement of a state statute will never be enough to confer standing.[96]

---

may be entirely accurate" and thus the statutory violation would "result in no harm." *Id.* Note that some have challenged the assertion that the publication of an incorrect zip code causes no harm. *See, e.g.*, Leading Case, *Class Action Standing:* Spokeo, Inc. v. Robins, 130 HARV. L. REV. 437, 444–45 (2016) ("[E]ven incorrect zip codes assuredly cause harm of *some* degree, since insurance and marketing companies often segment by zip code, and individuals are prone to make generalizations about race, religion, or ethnicity based on where somebody lives.").

91. *See Spokeo*, 136 S. Ct. at 1556 (Ginsburg, J., dissenting); Robins v. Spokeo, Inc., 867 F.3d 1108, 1116 (9th Cir. 2017) ("[E]ven if Congress determined that inaccurate credit reporting generally causes real harm to consumers, it cannot be the case that every trivial or meaningless inaccuracy does so.").

92. *See* FMC Corp. v. Boesky, 852 F.2d 981, 993 (7th Cir. 1988) ("Properly pleaded violations of state-created legal rights, therefore, must suffice to satisfy Article III's injury requirement."); Cantrell v. City of Long Beach, 241 F.3d 674, 684 (9th Cir. 2001) ("[S]tate law can create interests that support standing in federal courts.").

93. *See* Matera v. Google Inc., No. 15-CV-04062-LHK, 2016 WL 5339806, at *14 (N.D. Cal. Sept. 23, 2016).

94. *See* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020); Patel v. Facebook, Inc., 932 F.3d 1264, 1273–74 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.).

95. Facebook, Inc. v. Patel, 140 S. Ct. 937 (2020) (mem.).

96. *See* Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 534 (D. Md. 2016) (finding "no authority for the proposition that a state legislature . . . through a state statute or cause of action, can manufacture Article III standing for a litigant who has not suffered a concrete injury").

2. Concrete Injuries in Section 15(b) Litigation

Federal courts have held that some, but not all, violations of BIPA's provisions amount to concrete harms for the purposes of Article III standing. For example, several courts have found that unconsented-to disclosure of biometric data in contravention of section 15(d) constitutes an injury in fact.[97] Some courts have also suggested that failure to comply with BIPA's data security and retention requirements might give rise to standing.[98] But section 15(b) has proven the most contentious, with district courts and circuit courts alike disagreeing about whether plaintiffs can bring suit for violations of the statute's notice and consent requirements in various circumstances. This Section describes cases from the three circuit courts that have addressed the question—the Second, Seventh, and Ninth[99]—as well as some cases from the lower courts that further illuminate how federal judges have reasoned about standing in section 15(b) litigation.

a) Face Scans in the Second Circuit

In 2017, the Second Circuit held in *Santana v. Take-Two Interactive Software, Inc.*—a nonprecedential opinion—that plaintiffs lacked standing to sue a company for collecting their biometrics in violation of section 15(b).[100] In this case, plaintiffs sued Take-Two, the makers of a basketball-oriented video game that allowed players to create avatars based on their own facial geometries.[101] Players were first required to agree to terms and conditions, which read, "Your

97. *See, e.g.*, Dixon v. Wash. & Jane Smith Cmty.–Beverly, No. 17 C 8033, 2018 WL 2445292, at *8–9 (N.D. Ill. May 31, 2018) (finding that an employee had standing to sue her employer for storing her biometric data with a third-party vendor without her consent); Howe v. Speedway LLC, No. 17-CV-07303, 2018 WL 2445541, at *4 (N.D. Ill. May 31, 2018) (holding that plaintiff did not have standing because there was no indication that defendant "has released, or allowed anyone to disseminate, any of the plaintiff's personal information in the company's possession" (quoting Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 912 (7th Cir. 2017))); McGinnis v. U.S. Cold Storage, Inc., 382 F. Supp. 3d 813, 818 (N.D. Ill. 2019) ("To be sure, disclosing a biometric identifier to a third-party might very well constitute a concrete injury to an individual's privacy.").

98. *See, e.g.*, *Howe*, 2018 WL 2445541, at *5 (reasoning that BIPA's data security requirement is a "substantive provision[]" given the purposes of the statute); Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 15–16 (2d Cir. 2017) (summary order) (noting that violations of BIPA's data security requirement could "raise[] a material risk that [plaintiffs'] biometric data will be improperly accessed by third parties"); Miller v. Sw. Airlines Co., 926 F.3d 898, 902 (7th Cir. 2019) ("The longer data are retained . . . the greater the risk of disclosure . . . ."). *But see Bryant*, 958 F.3d at 626 (holding that a company's failure to publicly post a biometric data retention schedule in violation of section 15(a) did not confer standing).

99. *See Santana*, 717 F. App'x at 12; *Miller*, 926 F.3d at 898; *Bryant*, 958 F.3d at 617; *Patel*, 932 F.3d at 1264.

100. 717 F. App'x at 17.

101. *Id.* at 13.

face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay. By proceeding you agree and consent to such uses and other uses pursuant to the End User License Agreement."[102] Then, players had to spend fifteen minutes rotating their heads in front of a camera to generate their avatar.[103] The plaintiffs alleged that Take-Two violated five of BIPA's provisions, including section 15(b), by collecting biometrics "without their informed consent."[104]

The Second Circuit did not conduct a thorough *Spokeo* analysis to assess whether section 15(b)'s procedural notice and consent requirements protected a concrete interest. The court concluded that this question was not at issue because the plaintiffs had conceded that "BIPA [was] implicated only if their biometric data [was] collected or disseminated without their authorization or if a procedural violation create[d] a material risk of such an outcome."[105] The court ultimately rejected the plaintiffs' argument that Take-Two had collected their biometrics without authorization.[106] Instead, the court found that the software had clearly informed the plaintiffs that the game required face scans,[107] and that any reasonable person would have known that the cameras were conducting such a scan.[108] Ultimately, plaintiffs were not harmed by the lack of opportunity to give written consent. Moreover, Take-Two's failure to provide notice describing how long the company would store biometric data did not "present[] a material risk that [plaintiffs'] biometric data [would] be misused or disclosed."[109] As such, the plaintiffs lacked Article III standing.[110]

b) Biometric Photograph Tagging in the Ninth Circuit and the Northern District of Illinois

In 2019, the Ninth Circuit became the first federal appellate court to hold that plaintiffs had standing to sue a company for failure to comply with section 15(b)'s notice and consent requirements.[111] *Patel v. Facebook, Inc.* involved Facebook's Tag Suggestions feature: when users upload photos that contain

102. *Id.* at 13–14.
103. *Id.*
104. *Id.* at 14.
105. *Id.* at 15.
106. *Id.*
107. *Id.* at 15 (holding that the phrasing of the terms and conditions was "sufficient to meet BIPA's mandates under the circumstances here. . . . [T]o the extent that Take-Two departed from BIPA's requirements, it only did so insofar as it omitted the term, 'geometry.' ").
108. *Id.* at 15–16.
109. *Id.* at 16.
110. *Id.* at 17.
111. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1275 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.).

individuals' faces, the application analyzes various geometric points and compares them to a database of face templates.[112] If it finds a match, the application asks the user if they would like to tag that person.[113] Plaintiffs in this case alleged that Facebook violated BIPA's section 15(b) requirements by failing to obtain a written release for the collection of their biometric identifiers, and Facebook sought dismissal for lack of standing.[114]

The Ninth Circuit's analysis closely followed the framework laid out in *Spokeo*. The court first observed, "Privacy rights have long been regarded 'as providing a basis for a lawsuit in English or American courts.' "[115] It discussed the myriad ways in which the law has recognized privacy, from Samuel Warren and Louis Brandeis's pioneering law review article to William Prosser's privacy torts to First and Fourth Amendment jurisprudence.[116] The court concluded that, like these historical rights, BIPA protected the interest in controlling information about oneself.[117] Second, the court found that the Illinois legislature meant for the statute's procedural rights to protect concrete interests, basing much of its reasoning on the Illinois Supreme Court's decision in *Rosenbach*.[118] Because Facebook's Tag Suggestions feature infringed upon the right of individuals to control their biometric information—a right that was not merely procedural and which the Illinois General Assembly intended to protect—Facebook's actions resulted in a concrete injury that gave plaintiffs standing to sue.[119]

But in *Rivera v. Google, Inc.*, a case similar to *Patel* that also involved the tagging of photographs, the Northern District of Illinois held that plaintiffs lacked standing to sue Google for scanning their facial geometries without notice or consent.[120] Although *Rivera*'s conclusion as to standing for section 15(b) violations was abrogated in part by the Seventh Circuit's decision in

112. *Id.* at 1268.
113. *Id.*
114. *Id.* at 1268–69, 1274.
115. *Id.* at 1271 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).
116. *Id.* at 1271–72.
117. *Id.* at 1273.
118. *See id.* at 1273–74.
119. *Id.* at 1274.
120. Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1014 (N.D. Ill. 2018), *abrogated on other grounds by* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020). Rather than creating tag suggestions, Google Photos creates "face groups," which allow users to group photos of certain individuals together. *Id.* at 1001–02. One of the named plaintiffs in this case was a Google user who had uploaded photos of himself; those photos were then grouped together based on analysis of his facial geometry and associated with his user profile. *Id.* at 1002. The second named plaintiff was *not* a Google user; instead, her friend uploaded photos of her to the application and labeled the resulting group with her name. *Id.*

Bryant v. Compass Group USA, Inc., discussed below, it presents a useful comparison to *Patel* and illustrates how different courts have applied *Spokeo* to questions of standing under section 15(b).

Under *Spokeo*'s history prong, the *Rivera* court examined two possible common law analogues: the privacy torts of intrusion upon seclusion and appropriation of likeness.[121] It held that a violation of section 15(b) was not sufficiently similar to either.[122] The alleged injury could not compare to intrusion upon seclusion because the information involved was not private; people expose their faces to others constantly.[123] And since Google did not use plaintiffs' face scans for a commercial purpose, the second tort, appropriation of likeness, was also a poor fit.[124]

The court also found that the legislature's intent did not support a finding of injury in fact. Although the General Assembly emphasized that the permanency of biometric information heightened the risk of identity theft, the court did not believe that every case would present a sufficient risk of disclosure for this potential harm to amount to a concrete injury.[125] The court noted, "[T]here is no legislative finding that explains why the absence of consent gives rise to an injury that is *independent* of the risk of identity theft."[126] While recognizing that the case "presented close legal questions," the district court in *Rivera* ultimately concluded that the violation of section 15(b) did not constitute a concrete injury for the purposes of Article III standing.[127]

c) Fingerprint Scans in the Seventh Circuit and the Northern District of Illinois

The Seventh Circuit has decided two section 15(b) standing cases. Both involved the collection of fingerprints, but the holdings are distinct. While *Miller v. Southwest Airlines Co.*[128] is of limited applicability due to unique facts, *Bryant v. Compass Group USA, Inc.*,[129] opened the federal courts to a much wider range of BIPA cases. *Bryant* also overturned a number of Illinois district court cases involving fingerprint collection and section 15(b) standing.

121. *Id.* at 1011–14.

122. *Id.* at 1013–14. The court acknowledged that *Spokeo* does not require a harm to "square on all fours with a common law privacy tort," but found that the relationship must be sufficiently close. *Id.* at 1011.

123. *Id.* at 1012. The court was not persuaded by plaintiffs' argument that their facial biometrics were private, even if their faces themselves were not. *Id.*

124. *Id.* at 1013–14.

125. *Id.* at 1010.

126. *Id.*

127. *Id.* at 1014.

128. 926 F.3d 898 (7th Cir. 2019).

129. 958 F.3d 617 (7th Cir. 2020).

In *Miller*, the Seventh Circuit held that a class of union members had standing to sue their employers for collecting biometrics without written notice and consent.[130] The plaintiffs worked for airlines that required them to scan their fingerprints when clocking in and out of shifts.[131] As union members, the plaintiffs had the right to bargain over "a material change in [their] terms and conditions of employment," and "there [could] be no doubt that how workers clock in and out is a proper subject of negotiation between unions and employers."[132] In other words, because they were not given the opportunity to consent to biometric data collection, the plaintiffs were denied their right to negotiate an agreement surrounding the collection policy (e.g., their unions could have refused to agree to the policy or pressured employers to raise wages in exchange for its implementation).[133] The Seventh Circuit held that denial of the opportunity to negotiate a benefit was a concrete injury.[134]

The Seventh Circuit also found that a non-union plaintiff had standing to sue for a violation of section 15(b) in *Bryant v. Compass Group USA, Inc.*[135] In this case, the plaintiff's employer, Compass, had installed vending machines whose products could only be purchased by fingerprint.[136] During orientation, Compass instructed the plaintiff and her colleagues to scan their fingerprints into the machine and link a form of payment to create an account.[137] In contravention of section 15(b), Compass failed to (1) give the employees written notice explaining that their biometrics were being collected, describing the purpose for collection, and detailing the length of storage; and (2) obtain their written permission.[138] The plaintiff argued that these violations "denied her the ability to give informed written consent" and resulted "in the loss of the right to control [her] biometric identifiers and information."[139]

Like the Ninth Circuit in *Patel*, the Seventh Circuit used *Spokeo* to guide its standing analysis.[140] Interestingly, however, the court relied primarily on a concurrence by Justice Thomas, who reasoned that the injury in fact analysis should distinguish between private rights (e.g., trespass) and public rights (e.g.,

130. *Miller*, 926 F.3d at 901, 905.
131. *Id.* at 901.
132. *Id.* at 902–03.
133. *Id.*
134. *Id.*
135. 958 F.3d 617, 619 (7th Cir. 2020).
136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.* at 620.
140. *See id.* at 623 ("Our starting point is *Spokeo* itself, which provides substantial guidance about cases alleging the kind of intangible harm to personal interests that Bryant asserts."); Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.).

failure to comply with regulatory laws).[141] In *Bryant*, the Seventh Circuit concluded that the unlawful collection of Bryant's fingerprints was a violation of a private right and was "enough to show injury-in-fact without further tangible consequences."[142] Thus, the court wrote, "This was no bare procedural violation; it was an invasion of her private domain, much like an act of trespass would be."[143]

The court also analyzed the plaintiff's case through the lens of its precedent governing informational injuries—cases where parties fail to comply with statutes that require the disclosure of certain information (e.g., information about public candidates, agency activities, consumer reports, etc.) to enable the recipient to make decisions based on that information.[144] In the Seventh Circuit, "[t]he injury inflicted by nondisclosure is concrete [for the purposes of Article III standing] if the plaintiff establishes that the withholding impaired her ability to use the information in a way the statute envisioned."[145] Here, Compass's failure to disclose information regarding the collection, purpose, and storage of the plaintiff's fingerprints "deprived her of the ability to give the *informed* consent section 15(b) mandates."[146] Because "the informed-consent regime laid out in section 15(b) is the heart of BIPA," the plaintiff's injury was concrete.[147]

Bryant abrogated several cases from the Northern District of Illinois that had denied plaintiffs standing to sue private parties for scanning their fingerprints without notice and consent.[148] For example, in *Howe v. Speedway LLC*, the district court held that a plaintiff could not sue his employer for such a violation of section 15(b).[149] The court found that the goal of BIPA was not

141. *Id.* at 624; Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550–51 (2016) (Thomas, J., concurring) ("Common-law courts more readily entertained suits from private plaintiffs who alleged a violation of their own rights, in contrast to private plaintiffs who asserted claims vindicating public rights.").

142. *Bryant*, 958 F.3d at 624.

143. *Id.* Note that the plaintiff also sued Compass for failing to make publicly available a written data retention schedule, as required by section 15(a); the Seventh Circuit held that this violation did not result in a concrete injury for Article III standing purposes. *Id.* at 626.

144. *Id.*

145. *Id.*

146. *Id.* at 626.

147. *Id.* ("[BIPA's] purpose is to ensure that consumers understand, before providing their biometric data, how that information will be used, who will have access to it, and for how long it will be retained.").

148. *See, e.g.*, Howe v. Speedway LLC, No. 17-CV-07303, 2018 WL 2445541 (N.D. Ill. May 31, 2018); McGinnis v. U.S. Cold Storage, Inc., 382 F. Supp. 3d 813 (N.D. Ill. 2019); McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016); Colon v. Dynacast, LLC, No. 19-CV-4561, 2019 WL 5536834, at *4 (N.D. Ill. Oct. 17, 2019).

149. *Howe*, 2018 WL 2445541, at *7.

to grant individuals a right to informed consent, but to protect and secure their biometric data.[150] It based this conclusion on legislative findings that the permanency of biometrics heightened the risk of identity theft, and that regulation would promote "public welfare, security, and safety."[151] Consequently, the court concluded, BIPA's substantive provisions were those mandating reasonably secure data storage and prohibiting the sale or unauthorized disclosure of biometric information.[152] The notice and consent requirements "operate[d] in support of the data protection goal of the statute" but did not safeguard a concrete right in and of themselves[153]—at least in contexts like fingerprint scanning where plaintiffs had some awareness that their biometrics were being collected.[154]

In *Colon v. Dynacast, LLC*, the Northern District of Illinois noted that it had never found standing for a violation of section 15(b) in cases involving the scanning of fingerprints.[155] The reasoning in this case was similar to the Second Circuit's reasoning in *Santana*. The court wrote that in fingerprint collection cases, "any reasonable person would have known that the respective defendants were collecting, storing, and using biometric data."[156] Like these earlier cases, "the only purported 'violation of privacy' " the plaintiff in *Colon* could assert "was the failure to explain *in writing* that biometric data was being collected—something that would have been obvious to any employee subject to a fingerprint or hand-scan."[157] This obviousness led the court to find that any harm resulting from such collection was negligible and failed to amount to an Article III injury in fact.[158]

While *Howe* and *Colon* provide interesting arguments against the concreteness of section 15(b) injuries, *Bryant* opens the door for plaintiffs in fingerprint collection cases—and cases involving the collection of biometrics in other contexts—to bring suit in the Seventh Circuit and Illinois district courts for violations of BIPA's notice and consent requirements.

150. *Id.* at *5.

151. *Id.* (quoting 740 ILL. COMP. STAT. 14/5(g) (2020)).

152. *Id.*

153. *Id.* (quoting Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 513 (S.D.N.Y.), *vacated in part sub nom.* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12 (2d Cir. 2017)).

154. *Id.* (distinguishing this case from those involving the nonobvious collection of biometrics through the scanning of photographs posted online, including *Patel* and *Rivera*).

155. No. 19-CV-4561, 2019 WL 5536834, at *4 (N.D. Ill. Oct. 17, 2019).

156. *Id.*

157. *Id.* at *5.

158. *Id.*

IV. THE CONCRETENESS OF NOTICE AND CONSENT

This Part presents a theoretical assessment of whether BIPA's notice and consent requirements protect concrete privacy interests, the invasion of which should give rise to Article III standing. It focuses on section 15(b), as opposed to other provisions, for two reasons. First, as just discussed, much of the controversy surrounding BIPA's private right of action has stemmed from disagreements over whether data collection without notice and consent is a sufficiently concrete injury. Second, informed consent provisions are a core element of modern privacy protection, both in the United States and abroad.[159] Resolving the question of whether BIPA's notice and consent requirements are merely procedural, or whether they protect concrete rights in certain contexts, informs the broader conversation surrounding Article III standing in privacy cases.

This Part raises but does not resolve two important questions. First, is notice and consent a good regime for protecting privacy? Since the Organisation for Economic Co-operation and Development first articulated its Privacy Guidelines in the 1980s (also known as Fair Information Practice Principles, or FIPPs), numerous privacy laws around the globe have employed notice and consent as key safeguards.[160] But some scholars argue that such provisions do little to protect privacy, as they are often hidden in lengthy privacy policies, written in a manner that is difficult to understand, and offer a choice only between consenting to data collection or not using a service at all.[161] While the question of notice and consent's effectiveness is hugely important, this Note assumes that BIPA section 15(b) is an important mechanism for securing biometric privacy.

Second, should notice and consent be viewed as one provision with two separate requirements, or two distinct provisions whose violation must be assessed differently within the standing analysis? This Note primarily treats them as one, although it does discuss how violations of each requirement

159. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

160. *See* ORGANISATION FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK 75 (2013); Memorandum regarding The Fair Information Practice Principles from Hugo Teufel III, Chief Privacy Officer, Dep't of Homeland Sec. (Dec. 29, 2008); Notice of Privacy Practices for Protected Health Information, 45 C.F.R § 164.520 (2019); Privacy of Consumer Financial Information, 16 C.F.R. § 313 (2020); Council Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 at art. 7, recital 32.

161. *See, e.g.*, Susser, *supra* note 28, at 43–47.

might independently undermine the right to control one's personal information. But the two could easily be seen as protecting distinct interests. Daniel Susser writes that there can be no meaningful consent without notice, because informed consent requires an understanding of what one is agreeing to; however, he argues that notice does more than offer procedural support for the substantive goals of consent.[162] Rather, notice serves normatively important objectives on its own, such as raising user awareness regarding data collection and encouraging companies to develop articulable privacy policies.[163] Susser claims that critiques about the value of notice and consent (e.g., the impossibility of truly informed consent and lack of meaningful choice) are more properly directed at consent alone.[164] The severability of the two provisions is, again, a deeply interesting question that lies mostly outside the scope of this Note.

This Part asserts that plaintiffs suffer a concrete harm when private entities collect biometric data without notice and consent. Section IV.A describes how BIPA reflects a widely recognized conceptualization of privacy—control theory—which acknowledges that notice and consent protect substantive rights. Section IV.B argues that alleged violations of section 15(b) can quite easily be found concrete under the *Spokeo* analysis. Finally, Section IV.C explains that a finding of concrete harm for these violations serves the standing doctrine's underlying goal of preserving the separation of powers.

A. CONCEPTUALIZING BIOMETRIC PRIVACY THROUGH THE LENS OF CONTROL THEORY

Because privacy is a nebulous term involving a multitude of legal interests, a clearer understanding of the interests that BIPA's notice and consent requirements protect is necessary to determine whether violating section 15(b) infringes upon a concrete right.

Philosopher Judith Jarvis Thomson has remarked, "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."[165] A diverse collection of relatively unrelated laws invoke the concept of privacy, ranging from the Fourth Amendment right to be secure from government intrusion in one's own home[166] to the parental right to control online collection of a child's personal information.[167] Indeed, many academics agree that privacy's indeterminacy stems from the fact that it "seems

162. *See id.* at 52–56.
163. *Id.*
164. *Id.* at 43–47.
165. Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFF. 295, 295 (1975).
166. U.S. CONST. amend. IV.
167. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2018).

to be about everything, and therefore it appears to be nothing."[168] Recognizing that such an amorphous right is difficult to litigate and regulate effectively,[169] scholars have endeavored for decades to understand privacy's myriad meanings in the law.[170] Efforts to classify privacy harms have produced several prominent conceptualizations—i.e., ideas about what privacy actually is—which justify, though do not perfectly mirror, the rights to privacy afforded at law.[171] This Section asserts that BIPA's notice and consent provision reflects the widely accepted "control theory" of privacy. It discusses both the theory's conceptualization of why privacy is important as well as the legal recognitions of privacy reflecting that conceptualization.[172]

1. Foundations of Control Theory

Early control theorist Alan Westin wrote, "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[173] While some scholars suggest that privacy-as-control reflects a liberal focus on the individual as an entity entitled to make his or her own choices,[174] others argue that it can only be understood in the context of societal relations.[175] A person's ability to control the information known about her by others protects her ability to create bonds characterized by essential human values like trust, respect, and love.[176] That is to say, control theory is not about secrecy; it does not presume that people have privacy only in that which they choose not to convey to others at all.[177] Instead, it recognizes that people may wish to share

168. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 479 (2006).

169. *Id.* at 480.

170. Yvonne F. Lindgren, *Personal Autonomy: Towards a New Taxonomy for Privacy Law*, 31 WOMEN'S RTS. L. REP. 447, 450 (2010).

171. Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 36 (1967) ("The law does not determine what privacy is, but only what situations of privacy will be afforded legal protection . . . . Privacy, no less than good reputation or physical safety, is a creature of life in a human community and not the contrivance of a legal system concerned with its protection.").

172. BIPA arguably reflects other theories of privacy as well as control (e.g., personhood). But the discussion in this Note is limited to control theory, which strongly supports the argument that BIPA protects concrete interests and which several courts clearly draw upon in their analyses. *See, e.g.*, Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186; Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.).

173. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

174. *See* Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 862 (2000).

175. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("To refer . . . to the privacy of a lonely man on a desert island would be to engage in irony. The person who enjoys privacy is able to grant or deny access to others.").

176. *Id.* at 477.

177. *See id.* at 483.

aspects of themselves in some contexts but not others, and contends that the right to privacy safeguards their ability to make those determinations.[178] Under this theory, privacy is violated when an individual's ability to control personal information is taken away.

2. Control Theory as Reflected in BIPA Section 15(b)

Several courts have concluded that BIPA protects the right to control one's biometric information.[179] Indeed, section 15(b) clearly reflects the control theory of privacy.

Notice and consent provisions like the one in BIPA are at the heart of control theory, as they give people power to make educated decisions about when, how, and for what purpose others may gather their data. Control theorists recognize that choices about the amount of information to share, and at what level of detail, are highly contextual.[180] BIPA allows people to decide on a case-by-case basis whether a certain company should have access to a certain category of biometrics; consent to one circumstance does not imply consent to others. For example, someone may allow a bank to collect her fingerprint, knowing that it will only be used to grant her access to her financial records. She may feel uncomfortable using the same fingerprint to pay for groceries at a local supermarket, because the store associates all her past purchases with her fingerprint and recommends certain products when she scans it at checkout. Furthermore, she may choose not to consent to any company's collection, use, or storage of her facial geometry. Section 15(b) empowers her to make these contextual decisions.

Choices about whether or not to consent to a certain type of collection are meaningless without knowing to what exactly one is consenting; thus, notice is required if a statute is to guarantee *informed* consent. In this way, as proposed above, notice and consent can be considered separate but inherently intertwined requirements, and a violation of each can infringe upon control. When a company fails to ask for permission before scanning a person's face, then creates a series of data points describing his facial geometry, stores that data on servers for an undetermined amount of time, and uses it for any

178. *Id.* (giving an example of a person who tells a friend he is ill, but does not wish that friend to witness him actually experiencing the symptoms of that illness); *see also* WESTIN, *supra* note 173, at 7 ("[E]ach individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others . . . .").

179. *See, e.g.*, Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186; Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.); Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).

180. Fried, *supra* note 175, at 483; WESTIN, *supra* note 173, at 7.

number of purposes, the company quite clearly takes control over that data away from the subject. But even if the company had sought consent for the original face scan, that consent would be hollow if the subject had no understanding of what would happen to his data after it was collected, as that information might change his decision. Section 15(b)'s required notices explaining purpose, retention, and destruction of data are crucial for informed consent and thus play an important role in preserving individual control.

The fact that control of information mandates informed consent through adequate notice casts doubt on the Second Circuit's conclusion in *Santana* and the Northern District of Illinois's in *Colon* that no concrete injury occurs when an individual is aware that a company is collecting their biometrics. If, like in *Colon*, employees are required to scan their fingerprints to clock in and out of shifts without any idea of how long their employer might store the data or whether it will be used for any other purposes, the employees cannot legitimately be said to have given informed consent.[181] Despite the fact that employees know their biometrics are being collected, they are denied the ability to make a decision based on a clear understanding of what will happen to their data, and they thus suffer a loss of control. This idea challenges the notion that infringement in the context of knowing collection is a bare procedural violation and suggests that the notice provision protects a concrete right despite the individual's awareness. Indeed, the Seventh Circuit appropriately held in *Bryant* that Compass's failure to tell the plaintiff about its collection and storage procedures deprived her of the right to give informed consent and thus injured her concretely.[182]

3. When the Loss of Control Requires Legal Protection

In conjunction with theories about the meaning and import of privacy, some scholars have aimed to classify specific types of privacy harms to better understand which are afforded legal protection. The most prominent example of such an effort is William Prosser's 1960 synthesis of the four privacy torts.[183] Nearly five decades later, Daniel Solove published a taxonomy of privacy that looked beyond tort law to constitutional doctrines, evidentiary privileges, and federal and state statutory protections, ultimately identifying sixteen privacy harms within four categories.[184] Several of the harms discussed in Solove's taxonomy serve as strong examples of how the loss of control over personal

181. *See* Colon v. Dynacast, LLC, No. 19-CV-4561, 2019 WL 5536834 (N.D. Ill. Oct. 17, 2019).

182. *See Bryant*, 958 F.3d at 626.

183. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

184. *See* Solove, *A Taxonomy of Privacy*, *supra* note 168, at 482–83.

information can cause injury; indeed, some early control theorists wrote about the same specific harms within their conceptualizations.[185] Many of these harms have also been acknowledged in the courts.

This Section describes two such harms—identification (and the correlative interest in anonymity) and aggregation—both of which have received legal recognition, and both of which are implicated in BIPA section 15(b).

a) Identification

Identification is the harm that results from a person's loss of control regarding information about who they are. The inverse of identification is anonymity, which Westin calls a "basic state[] of individual privacy . . . . [that] occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance."[186] At its core, Westin says, the value of anonymity is freedom—it allows a person to move about "open spaces and public arenas" without having to conform to societal roles and rules.[187] Anonymity allows people to control whether information about what they do in public will be linked back to them in a way that could compromise their social relationships.

Anonymity has received a significant amount of legal protection in certain contexts. In *McIntyre v. Ohio Elections Commission*, the Supreme Court determined that privacy encompasses a person's right to speak and associate without being forced to identify oneself.[188] The Court wrote, "Anonymity is a shield from the tyranny of the majority. . . . [It] protect[s] unpopular individuals from retaliation . . . at the hand of an intolerant society."[189] Similarly, the Court observed in *NAACP v. Alabama* that "[i]nviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[190] The Court also noted the troubling history of identification in the context of religion.[191]

Without the requirements of notice and consent, many biometric applications could force unwanted identification in spaces that were previously

185. *See* WESTIN, *supra* note 173, at 31 (referring to anonymity as a "state of privacy").
186. *Id.*
187. *Id.*
188. 514 U.S. 334 (1995).
189. *Id.* at 357.
190. 357 U.S. 449, 462 (1958).
191. *Id.* (quoting Am. Commc'ns Ass'n v. Douds, 339 U.S. 382, 402 (1950) ("A requirement that adherents of particular religious faiths or political parties wear identifying arm-bands, for example, is obviously of this nature," i.e., obviously interferes with freedom of assembly.)

anonymous, and, depending on the context, could chill freedoms of speech and association.[192] For example, Nest doorbells have the capacity to capture and analyze face scans of people walking along public streets.[193] If every homeowner in a neighborhood purchased a Nest, people might be deterred from exercising their right to protest in that neighborhood for fear that they would be identified and suffer consequent reprisal. Because of BIPA, Nests sold in Illinois are not equipped with facial recognition (likely because providing the required notice and obtaining consent from every individual who approached a doorbell would be impossible).[194] The provision has thus successfully protected Illinoisans' anonymity. Similarly, as discussed in Part I, some churches use surveillance cameras equipped with facial recognition technology to identify parishioners.[195] Given the right to anonymous association, combined with the great deference religion is given in the United States, obtaining biometrics without consent in this circumstance certainly infringes upon privacy.

Apart from surveillance, Solove argues that de-anonymization can also be harmful in the information privacy context because it "attaches informational baggage to people" and thus removes their control over what others are able to learn about them in a particular circumstance.[196] In this view, biometric identification can result in harm by linking someone's identity to other types of information.[197] Countless biometric applications demonstrate this effect. For example, bank verification can attach an individual's entire financial record to their thumbprint. Employer attendance software connects the same thumbprint with habits of truancy or tardiness. Shoplifter identification systems associate visitors to retail stores with potentially damning information about their past behaviors. And online applications that recognize a person in an uploaded photograph could scour the internet and link that person to a decades-old mugshot. While some of these applications appear more innocuous than others, all can be said to cause harm in that they "inhibit

192. Not all biometric applications threaten anonymity: some are utilized in environments where anonymity is not an option, such as employers' use of thumbprints to track time.

193. Gibbs, *supra* note 4.

194. *See* Amy Korte, *Privacy Law Prevents Illinoisans from Using Google App's Selfie Art Feature*, ILL. POLICY (Jan. 23, 2018), https://www.illinoispolicy.org/privacy-law-prevents-illinoisans-from-using-google-apps-selfie-art-feature.

195. *See Face Recognition App – The Churchix App*, *supra* note 2.

196. Solove, *A Taxonomy of Privacy*, *supra* note 168, at 513 (describing a French case where a transgender person was unable to change her gender on identifying documents).

197. *Id.*

people's ability to change and can prevent their self-development by tying them to a past from which they want to escape."[198]

b) Aggregation

The problem of informational baggage is especially pronounced when applications aggregate many different types of data from many different sources. Solove classifies aggregation as a harm distinct from identification, but recognizes that they are often intertwined.[199] Aggregation can generate highly detailed insights that data subjects could not have envisioned when each individual data point was collected, and identification links those insights to a specific person.[200]

Solove recognizes aggregation as a harm for two reasons. First, it causes a dignitary injury by violating people's expectations that there will be "certain limits on what is known about them and on what others will find out."[201] The Supreme Court voiced a similar concern in *Carpenter v. United States*, a case involving the collection of location data from a cellphone over a period of 127 days.[202] The Court found that the aggregation of many individual location data points—each of which could theoretically be observed by police physically tracking a person in public—could cause harm by violating people's presumptions that "law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual[] . . . for a very long period."[203] Aggregation thus infringed upon the defendant's reasonable expectation of privacy. Second, Solove notes that aggregation can cause a power imbalance when compiled data is used to make crucial decisions about whether someone will receive certain benefits, such as loans and mortgages.[204]

These harms are certainly possible in the context of biometric data collection. Facebook's Tag Suggestions feature, for example, can associate an individual's face template with any photograph uploaded to the site.[205] While someone may expect that he will only be tagged in his friends' photographs, any image uploaded by any stranger that unwittingly captures him in the background can theoretically be linked to his profile. Given that hundreds of

198. *Id.* at 514.

199. *Id.*

200. *Id.* at 507, 514 (explaining that aggregation creates a "digital person" and identification "links the digital person directly to a person in realspace").

201. *Id.* at 508.

202. 138 S. Ct. 2206 (2018).

203. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 430 (2012)).

204. Solove, *A Taxonomy of Privacy*, *supra* note 168, at 508.

205. The Ninth Circuit raises this concern in *Patel*. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.).

millions of photographs are uploaded each day, there is a potential for data aggregation that provides overly detailed insight into what a person does, who he is with, and (through geotagging) where he goes. This may violate that person's expectations for how the Facebook site functions and represents a significant loss of control over the amount and detail of collected information. But providing adequate notice at the collection stage detailing how the data will be used and whether it will be combined with other information can properly orient an individual's expectations regarding the extent of data use. And requiring Facebook to obtain consent gives the individual the power to choose whether the company can create a "digital person"[206] based on the aggregation of the individual's data.

B. NOTICE AND CONSENT UNDER *SPOKEO*

A clearer understanding of how section 15(b) implicates the privacy-as-control theory makes it easier to analyze whether a violation of that provision constitutes a concrete injury under *Spokeo*. The examples discussed above already suggest that failure to provide adequate notice and obtain consent can cause real harms, such as loss of control over highly personal information, infringement of the right to speak and associate anonymously (as well as the potential chilling effect on the exercise of those freedoms), inability to disassociate oneself from past actions or contextually unrelated information, and violation of expectations governing the amount of information known about oneself. So, while section 15(b) may be procedural, it protects undeniably concrete interests, and violations merit a finding of injury in fact. This Section demonstrates how the two prongs of the *Spokeo* analysis support that conclusion.

1. History

Spokeo directs courts to "consider whether an alleged intangible harm has a close relationship" to one historically recognized at common law.[207]

As discussed above, courts throughout history have acknowledged several of the privacy harms that section 15(b) implicates as deserving of legal redress. Some interests are more modern, but others, like that of anonymous speech and association, are First Amendment rights that go back to the country's origins. Moreover, although scholars only began to articulate control theory in the 1960s, they did so in an attempt to extract insight from much older

206. Solove, *A Taxonomy of Privacy*, *supra* note 168, at 508.
207. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

common law cases that established legal protections for privacy rights.[208] So, it can be said that many of the harms examined in Section IV.A, are sufficiently analogous to historically protected harms.

Crucially, *Spokeo*'s "close relationship" between alleged and common law harm does not have to be an exact match; several courts have found general comparisons to be satisfactory.[209] Although some scholars assert that comparing privacy harms to historical analogs is likely to severely diminish standing for privacy cases, since traditional conceptions of privacy do not encompass modern problems,[210] the broad interpretation of the history prong gives courts sufficient leeway to identify old injuries that are sufficiently similar to new ones.

The Ninth Circuit accurately described some of the specific historical interests that BIPA protects in its analysis of common law privacy harms in *Patel*. The court began by broadly acknowledging that the common law protected "a general right to privacy."[211] It discussed this right in the context of Warren and Brandeis's ideas about privacy, Prosser's four privacy torts, and the intertwined constitutional and common law notions regarding "zones of privacy."[212] The court also noted recent Fourth Amendment cases, like *United States v. Jones*,[213] *Carpenter v. United States*,[214] and *Riley v. California*,[215] which found that new technologies introduced significant risks to privacy.[216] While this initial analysis was somewhat vague, the court eventually clarified how the specific interests BIPA protects compared to traditionally recognized harms. First, it wrote, "[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[217] In other words, the statute reflects control theory's conceptualization of privacy. Second, the court discussed how Facebook's Tag

208. WESTIN, *supra* note 173, at 330–64 (describing how privacy rights in American law evolved in the years between 1790 and the mid-twentieth century).

209. DeLuca, *supra* note 84, at 2463–64.

210. *See, e.g.*, Solove, *A Taxonomy of Privacy*, *supra* note 168, at 564 ("[S]ome of the privacy problems we face today are different in nature, and do not track traditional conceptions of privacy.").

211. Patel v. Facebook, Inc., 932 F.3d 1264, 1271 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.) (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890)).

212. *Id.* at 1271–72.

213. 565 U.S. 400 (2012).

214. 138 S. Ct. 2206 (2018).

215. 573 U.S. 373 (2014).

216. *Patel*, 932 F.3d at 1272–73.

217. *Id.* at 1273 (quoting U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989)).

Suggestions feature could obtain "encyclopedic" information and associate a user with "hundreds of millions of photos."[218] This point reflects concerns about data aggregation. The court then noted that Facebook's face scans could be used to identify an individual "from a surveillance photo taken on the streets or in an office building."[219] Here, we see anxiety about the harms of identification in conjunction with surveillance and how it can lead to the loss of anonymity. The court concluded that these harms "invade[] an individual's private affairs,"[220] suggesting that the concrete interest in privacy that BIPA protects is sufficiently similar to the common law's general right to privacy.

On the other hand, the Northern District of Illinois's overly restrictive analysis in *Rivera* failed to acknowledge any possible connection between common law privacy rights and the theory of privacy-as-control underlying BIPA's provisions. In *Rivera*, the court examined whether a violation of section 15(b) bore a sufficiently close relationship to one of two specific privacy torts, intrusion upon seclusion or appropriation of likeness.[221] It concluded that neither was an apt analogue, because several key elements of the torts were not met in the BIPA case.[222] Although the court recognized that *Spokeo* did not require "[an] alleged injury . . . [to] square on all fours with a common law privacy tort," it ultimately held that the differences between the statute and the torts were too great.[223] The *Rivera* court's analysis was thus flawed, in part because it construed *Spokeo*'s "close relationship" guidance as requiring an excessively strict standard. But beyond that, the court assessed how a violation of notice and consent squared with the *elements* of traditional privacy harms, when it should have compared the *interests* that each protects. After all, the overarching purpose of the *Spokeo* analysis is not to find an adequate historical match for a modern statute involving modern technology—it is to determine whether that modern statute protects interests that can rightly be judged as concrete. Because *Rivera*'s factual context was so similar to *Patel*'s, the Northern District of Illinois should have identified all the harms discussed by the Ninth Circuit and found standing as a result.

2. Legislative Intent

Spokeo also held that courts should consider Congress's judgment and assess whether it meant for the statute to protect a concrete interest. The state

218. *Id.*
219. *Id.*
220. *Id.*
221. Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1011 (N.D. Ill. 2018), *abrogated on other grounds by* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).
222. *Id.* at 1012–14.
223. *Id.* at 1011.

legislature's intent is equally instructive when analyzing whether plaintiffs have standing under a state statute.[224]

Federal courts have disagreed over whether the Illinois General Assembly intended for the procedural requirements in section 15(b) to protect an underlying concrete interest. The Northern District of Illinois concluded in *Howe* that the purpose of BIPA is "the protection and security of biometric data"; according to this court, the notice and consent requirements merely "support" those goals and do not in themselves safeguard a concrete interest.[225] The same court came to a similar conclusion in *Rivera*, noting that none of the legislature's findings addressed a harm separate from identity theft.[226] In contrast, the Ninth Circuit, relying heavily on the Illinois Supreme Court's decision in *Rosenbach*, interpreted BIPA as granting a right to control one's personal information and found that notice and consent are integral to preserving true authority over one's data.[227] And in *Bryant*, the Seventh Circuit found that the purpose of the statute was "to ensure that consumers understand, before providing their biometric data, how that information will be used, who will have access to it, and for how long it will be retained."[228] Informed consent and the corresponding right to withhold consent—which the court called "[a] key part of the right to control biometric information"[229]—were at "the heart of BIPA."[230]

The legislature's focus on *proactively* preventing the harms associated with identity theft, as well as its interest in safeguarding the public welfare by regulating data collection, strongly indicates that it intended section 15(b) to protect concrete interests, the violation of which would suffice for standing. After noting the legislative findings regarding identity theft, the Illinois Supreme Court in *Rosenbach* found that BIPA was designed to "head off such problems before they occur," in part by "imposing safeguards to insure that

224. *See supra* text accompanying notes 92–96.

225. Howe v. Speedway LLC, No. 17-CV-07303, 2018 WL 2445541, at *5 (N.D. Ill. May 31, 2018). The court did postulate that, in different factual contexts where plaintiffs were completely unaware that companies were collecting their biometrics, violations of section 15(b) might infringe upon an underlying privacy interest. *Id.* However, the same court seemed to reject that reasoning several months later in *Rivera*, a case where plaintiffs did not know that Google was scanning their photographs to collect their facial geometries. *See* Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1001–02 (N.D. Ill. 2018), *abrogated on other grounds by* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).

226. *See Rivera*, 366 F. Supp. 3d at 1010–11.

227. *See* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 34 (2019); Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020) (mem.).

228. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 626 (7th Cir. 2020).

229. *Id.* at 621.

230. *Id.* at 626.

individuals' . . . rights in their biometric identifiers . . . are properly honored and protected to begin with, before they are or can be compromised."[231] *Patel* cited this language to come to the same conclusion.[232] A failure to find standing in section 15(b) cases would allow plaintiffs to bring suit only in situations where their biometric information was already in a heightened state of risk, because a company either failed to store it securely or disclosed it to a third party without consent. It certainly seems that the legislature was interested not only in preventing identity theft itself but also in preventing (unwanted) increased risk as well. As the Seventh Circuit found in *Bryant*, notice and consent enable informed decisions about whether one wishes to assume such a risk.[233] Thus, when a company violates section 15(b), "the right of the individual to maintain . . . biometric privacy vanishes into thin air [and] [t]he precise harm the Illinois legislature sought to prevent is then realized."[234]

Furthermore, the *Howe* court's judgment that section 15(b)'s notice and consent requirements "support" BIPA's goals does not inevitably lead to the conclusion that those provisions do not protect a concrete interest.[235] Notice and consent supply individuals with control in part by enabling them to exercise other rights encompassed by other provisions. For example, without adequate notice that a company is collecting and storing biometric information, how can anyone sue for the improper storage or disclosure of that data? Absent this knowledge, they may not learn that their information is being held insecurely, or held by a third party, until after it is compromised.

In sum, the Seventh Circuit and Ninth Circuit correctly concluded that the Illinois General Assembly intended BIPA section 15(b) to grant a right to control the collection of one's own biometric data through informed consent, and that that control safeguards concrete interests. Because the provision also prevents harms historically recognized in the Constitution and at common law, the *Spokeo* analysis supports a finding that violations of section 15(b) amount to concrete harms for the purposes of the injury in fact analysis.

231. *Rosenbach*, 2019 IL 123186, ¶ 36.

232. *Patel*, 932 F.3d at 1273.

233. *Bryant*, 958 F.3d at 626 ("The judgment of Illinois's General Assembly is that the sensitivity of biometric information and the risk of identity theft or other privacy or economic harm that may result from its dissemination, necessitates that people be given the opportunity to make informed choices about to whom and for what purpose they will relinquish control of that information.").

234. *Rosenbach*, 2019 IL 123186, ¶ 34 (quoting Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).

235. *See* Howe v. Speedway LLC, No. 17-CV-07303, 2018 WL 2445541, at *5 (N.D. Ill. May 31, 2018).

C. BIPA AND THE GOALS OF STANDING

Finally, interpreting section 15(b) as protecting concrete interests in accordance with the legislature's intent serves the standing doctrine's underlying goal of preserving the separation of powers.

The majority in *Spokeo* wrote that the standing doctrine "developed in our case law to ensure that federal courts do not exceed their authority."[236] Indeed, preserving the separation of powers is one of the most commonly-offered justifications of the doctrine.[237] Justice Antonin Scalia argued in a highly influential article that standing, by requiring plaintiffs to have suffered a concrete and particularized injury, restricts the judiciary to its traditional role of protecting individuals, rather than "prescribing how the other two branches should function."[238] In Justice Scalia's view, this limit is a good thing, both because courts are inherently undemocratic and because judges are "governed by a body of knowledge that values abstract principle above concrete result."[239]

While standing does place important limits on the courts' ability to answer questions better suited for Congress, stringent enforcement of standing requirements can actually undermine the power of the legislature to define and enforce rights.[240] In *The Structure of Standing*, Judge William Fletcher asserts that the balance of powers is likely to tip too far towards the courts when judges are interpreting whether a statutory violation amounts to an injury in fact. He argues, "[T]o limit . . . the power of Congress to create standing . . . is to limit the power of Congress to define and protect against certain kinds of injury that the Court thinks it improper to protect against."[241]

The increasing number of privacy statutes represents a clear effort by federal and state legislatures to define new injuries arising as a result of technological progress. As previously discussed, some of these injuries share characteristics with the privacy torts and older common law claims. But some represent entirely new harms. In Judge Fletcher's view, a restrictive standing requirement that prevents plaintiffs from vindicating rights the legislature has granted violates the separation of powers. Felix Wu makes a similar argument regarding *Spokeo*'s effect on the standing analysis in privacy cases. He writes:

---

236. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).

237. Along with promoting separation of powers, standing also serves the goals of heightened judicial efficiency, improved judicial decision-making, and increased fairness. ERWIN CHEMERINSKY, FEDERAL JURISDICTION 56–57 (7th ed. 2016).

238. Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 894 (1983).

239. *Id.* at 896.

240. William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 233 (1988).

241. *Id.*

> When courts deny standing in [privacy] 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.[242]

In enacting BIPA, the Illinois legislature determined that the unauthorized collection of biometric data by a corporate entity represents a significant harm. Because plaintiffs are suing companies for illegally capturing their unique data, rather than for biometric practices more generally, questions brought to the court will often involve individual rights.[243] Federal courts thus are well within their purview to answer these questions. Indeed, refusing to do so based on an overly strict standing requirement would infringe upon legislative power.

V. CONCLUSION

A clear analysis of the privacy theory underlying BIPA's notice and consent requirements, as well as the harms BIPA prevents, supports the conclusion that section 15(b) protects a concrete right. As the federal courts see more and more BIPA litigation involving violations of section 15(b), they should hold that infringements upon the interests it safeguards meet the requirements of injury in fact for the purposes of Article III standing.

This analysis may also have implications for other privacy statutes that mandate proper notice and informed consent for the collection and use of data. As discussed above, many statutes in the United States and elsewhere rely upon these provisions as key elements of privacy protection. A finding of concreteness for violations of section 15(b) does not necessarily suggest the same conclusion for other privacy statutes; perhaps biometric data should be seen as unique, given the heightened identity theft risks resulting from its permanency, as well as other distinctive characteristics.[244] Regardless, in analyzing the concreteness of similar privacy harms, courts should make a greater effort to clarify the underlying conceptualizations of privacy that a given statute protects. Doing so will preserve the power of federal and state

242. Wu, *supra* note 83, at 458.

243. *See id.* ("The vast majority of privacy and security cases . . . are indeed ones involving individual rights, not merely broad questions of public interest. Almost invariably, privacy plaintiffs are specific individuals who claim that their own personal information has been mishandled in some way.").

244. Here, the personhood theory of privacy, introduced *supra* note 172, could support an argument that BIPA is unique because the biometric data it protects is inextricably tied to the body and the self, while other types of information like addresses and credit card numbers are less intrinsically personal.

legislatures to enact laws like BIPA to ensure that new technologies do not dilute or eliminate important, long-recognized rights to privacy.