The John Marshall Law Review

Volume 53 | Issue 1 Article 3

2020

Biometric Privacy: Blending Employment Law with the Growth of Technology, 53 UIC J. Marshall L. Rev. 73 (2020)

Gabrielle Neace

BIOMETRIC PRIVACY: BLENDING EMPLOYMENT LAW WITH THE GROWTH OF TECHNOLOGY

GABRIELLE NEACE*

Abstract

In a highly interconnected world where new technology emerges daily to improve our lives, important privacy implications remain unsettled – what happens to the various types of data collected by entities? What privacy rights do we have to that data? What happens when our employer wants to collect that data from us? In 2008, Illinois enacted this country's first Biometric Privacy Act ("BIPA") to answer some of these emerging questions. This statute has not been amended since 2008, despite various efforts, and remained unnoticed until an influx of litigation arose in 2017. This comment surveys Illinois' BIPA, which is the most stringent Biometric Privacy statute in the United States. It focuses on the

impact BIPA has on employees and employers that largely use biometric collection technology to improve their businesses.

I. INTRODUCTION

Would you sacrifice your privacy to allow law enforcement to catch a serial killer? That is precisely what a user of a genealogy website, GEDmatch, facilitated for the Sacramento County police.[1] After forty years, police matched the DNA of the infamous "Golden State Killer" to DNA provided by his distant relative on GEDmatch.[2] This achievement shows the positive aspect of technological advancement and how biometric data collection can improve our daily lives; it can even solve a cold case. However, the ability to collect biometric data raises the issue of data privacy, which is an unsettled legal area largely governed by state laws, as no federal regulation exists.[3]

Illinois passed the Biometric Information Privacy Act (BIPA) in 2008 to regulate businesses that wanted to use rapidly improving technology to collect consumers' biometric data such as fingerprints.[4] BIPA regulates private entities that collect biometric data from individuals, but it does not apply to government entities.[5] It imposes strict requirements for the collection, sharing, retention, and destruction of such data.[6] The statute went relatively unnoticed until 2017, when a large number of plaintiffs began filing lawsuits against companies for violating BIPA's requirements.[7]

When litigation first arose, plaintiffs typically alleged that the defendants violated BIPA by failing to give plaintiffs notice of the data collection or obtain consent prior to collecting the data.[8]

---

* JD, UIC John Marshall School, 2020. Many thanks to my sister Rebecca Bryant, who both paved the path of excellence as an advocate, and continues to walk beside me, inspiring me to achieve goals that once seemed impossible.

1. Sarah Zhang, *How a Genealogy Website Led to the Alleged Golden State Killer*, THE ATLANTIC (Apr. 27, 2018), www.theatlantic.com/science/archive/2018/04/golden-state-killer-east-area-rapist-dna-genealogy/559070/.

2. *Id.*

3. Michelle Gillette & Josh Thomas Foust, *Genetic Testing Cos. Must Examine Illinois Privacy Law*, LAW360 (Aug. 3, 2018), www.law360.com/articles/1069206/genetic-testing-cos-must-examine-illinois-privacy-law.

4. Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1-99 (2008).

5. 740 ILL. COMP. STAT. 14/10 (2020).

6. 740 ILL. COMP. STAT. 14/15 (2020) (requiring private collect biometric data to comply with strict requirements as it relates to the collection, storage, and destruction of data. Otherwise, the entities face a set amount of damages per each violation).

7. Stephanie Sheridan & Megan Brooks, *Avoid Getting A Plaintiff's Fingerprint Pointed At You*, LAW360 (Feb. 28, 2018), www.law360.com/articles/1015719/avoid-getting-a-plaintiff-s-fingerprint-pointed-at-you.

8. Alan S. Wernick, *Biometric Information – Permanent Personally Identifiable Information Risk*, AM. BAR ASS'N (July 2, 2019), www.americanbar.org/groups/business_law/publications/committee_newsletter

Defendants typically responded to BIPA suits by arguing that plaintiffs lacked standing because plaintiffs had not suffered an injury, as required by Article III of the United States Constitution.[9] BIPA lawsuits originally combated internet giants like Facebook and Google, which allegedly violated BIPA's notice and consent requirements.[10] However, in 2018, employees increasingly filed lawsuits against their employers, particularly those that forced employees to clock-in and clock-out of their work hours using their fingerprints instead of the traditional method of stamping a timecard physically or electronically.[11]

Until 2019, over thirty class action lawsuits had been filed under BIPA, which was considered an influx in litigation.[12] However, the Illinois Supreme Court's decision in *Rosenbach v. Six Flags*[13] opened the floodgates for litigation as BIPA lawsuits filed in Illinois courts have risen to the hundreds since that decision.[14] In *Rosenbach*, the Illinois Supreme Court held that "an 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."[15]

Illinois remains among the most stringent states in biometric privacy protections.[16] Only Washington and Texas have enacted similar statutes.[17] Despite the Illinois Supreme Court's ruling in *Rosenbach*, there is still a split among federal district and circuit courts as to whether an individual claiming a technical violation of a statutory provision within BIPA satisfies Article III Standing under the U.S. Constitution.[18] This comment will focus on BIPA

---

s/bcl/2019/201902/fa_8/.

9. *See e.g.,* Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018) (arguing that "collection of biometric information without notice or consent can never support Article III Standing without 'real-world harms' such as adverse employment impacts or even just 'anxiety.'").

10. Sheridan & Brooks, *supra* note 7.

11. *Id.*

12. *Id. See e.g.,* In re Facebook Biometric Info. Privacy Litig., 2018 U.S. Dist. LEXIS 81044, at *14 (N.D. Cal. May 14, 2018) (articulating the common argument among plaintiffs that the business entity violated BIPA by failing to obtain consent, prior to collecting biometric information, in the argument that Facebook violated BIPA through its "Tag Suggestion" and did not obtain prior consent to using a user's facial recognition).

13. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).

14. Michael J. Bologna, *Law on Hiring Robots Could Trigger Litigation for Employers*, BLOOMBERG L. (Oct. 11, 2019), news.bloomberglaw.com/daily-labor-report/law-on-hiring-robots-could-trigger-litigation-for-employers.

15. *Rosenbach*, 129 N.E.3d at 1207.

16. *Id.*

17. *Id.*; TEX. BUS. & COM. CODE § 503.001 (2009); WASH. REV. CODE (ARCW) § 19.375.020 (2017).

18. *Compare* Patel v. Facebook, Inc., 932 F.3d 1264, 1274 (9th Cir. 2019), *cert. denied*, No. 19-706, 2020 WL 283288 (U.S. Jan. 21, 2020) (holding that "plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article

standing and its impact on employers.

The background section will explore BIPA, differing views on the required standing under the statute, similar statutes in other states, and highlight how employers use biometric data. The analysis section will analyze the U.S. Supreme Court's interpretation of Article III Standing, compare biometric data privacy statutes, highlight the potential future of BIPA, and alternative protections for employees who refuse to disseminate their biometric information. Finally, this Comment proposes that current biometric privacy statutes should be amended to allow a private right of action. Beyond that, other states need to continue to enact these statutes. The courts need to support these efforts and the legislatures' intent by recognizing Article III Standing where an entity has violated any provision of a biometric privacy statute.

II. BACKGROUND

The background section will explore the provisions and requirements in BIPA, the Article III Standing associated with interpreting BIPA, the statutes similar to BIPA in other states, and the reasons employers give for collecting biometric data from employees.

A. BIPA: Illinois' First Step to Protect Data Privacy

Illinois passed BIPA in response to emerging public concern over technologies that could attach biometric identifiers to financial and personal information.[19] The Illinois legislature declared that personal biometric information is "biologically unique to the individual; therefore, once compromised, the individual has no recourse."[20] Specifically, there was concern over "finger-scanning technologies" as a new form of payment method.[21] At the time, many corporations chose Chicago as a testing city for implementing finger-scan technologies in public places, such as gas stations and grocery stores.[22]

In 2008, shortly before BIPA was enacted, a company called "Pay by Touch," which intended to link consumers' fingerprints to

---

III standing," where the defendant failed to obtain written consent prior to its collection, use, and storage of biometric identifiers), *with* Santana v. Take-Two Interactive Software, Inc., 717 Fed. App'x 12, 15-18 (2d Cir. 2017) (holding that a technical violation of the consent provision in BIPA is sufficient to confer Article III Standing).

19. 740 ILL. COMP. STAT. 14/5 (d) (2020).

20. 740 ILL. COMP. STAT. 14/5 (c) (2020) (contrasting biometric data with finances and "other sensitive information," like social security numbers).

21. 740 ILL. COMP. STAT. 14/5 (a) (2020).

22. 740 ILL. COMP. STAT. 14/5 (b)(2020).

their bank accounts, went out of business.[23] In using Pay by Touch, a consumer could have used their fingerprint rather a credit card to make purchases in-store.[24] The failure of Pay by Touch, and its ultimate bankruptcy filing, caused the Illinois legislature to question the impact on collected sensitive information if a company like Pay by Touch went out of business.[25] The legislature was concerned that data might be sold to third parties or shared in bankruptcy proceedings, so customers needed protection.[26] Thus, the Illinois legislature passed BIPA and outlined its intent in doing so: "The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[27]

BIPA regulates the disclosure, collection, retention, and destruction of biometric identifiers by any private entity.[28] It does not regulate state or local governments.[29] A "biometric identifier" covered under the act includes "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[30] The term "biometric identifier" does not include "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."[31] The key BIPA provisions include: (1) obtaining written consent from the individual prior to collecting data; (2) a time limit for storing the data; (3) developing and maintaining a publicly available retention schedule; (4) requiring the entity to protect the data using reasonable care;[32] (5) creating a private cause of action

23. Matt Marshall, *Pay By Touch In Trouble, Founder Filing For Bankruptcy*, VENTURE BEAT (Nov. 12, 2007), venturebeat.com/2007/11/12/pay-by-touch-in-trouble-founder-filing-for-bankruptcy/; Erica Gunderson, *Biometric Data: Are We Safer in Illinois, Or Just Having Less Fun?*, CHI. TONIGHT (Jan. 22, 2018), chicagotonight.wttw.com/2018/01/22/biometric-data-are-we-safer-illinois-or-just-having-less-fun.

24. *Id*.

25. Chris Hoffman, *Seventh Circuit Suggests That Unions Can Negotiate Workers' Biometric Data Privacy Rights With Employers*, AM. BAR ASS'N (Aug. 14, 2019), www.americanbar.org/groups/business_law/publications/committee_newsletters/cyberspace/2019/201908/unions/.

26. *Cf.* Darcy Reddan, *Kroger Unit Fired Contaminated-Test Whistleblower, Suit Says*, LAW360 (June 13, 2017), www.law360.com/articles/933696/kroger-unit-fired-contaminated-test-whistleblower-suit-says (noting that Pay by Touch filed for bankruptcy and that, as a result of the filing, it became clear that sensitive information was going to be sold, distributed, or shared in the proceedings).

27. 740 ILL. COMP. STAT. 14/5 (g) (2020).

28. 740 ILL. COMP. STAT. 14/10 (2020).

29. *Id*.

30. *Id*.

31. *Id*.

32. The reasonable care requirement leads to the question, "what happens when an employer declares bankruptcy or merges with another company?"

for individuals; and (6) allowing individuals to recover liquidated damages depending on the level of intent or to prove higher damages.[33]

As applied to the context of employers, an employee must give written consent or release[34] to the employer before the employer can collect, capture, purchase, or receive an employee's "biometric identifier."[35] BIPA also requires that destruction of an employee's biometric data occur either when the reason for collection no longer exists or within three years of the employee's last interaction with the employer.[36] An employer, or any other private entity that possesses biometric data, must use the "reasonable standard of care within the private entity's industry" to store, transmit, and protect the data.[37] That is, an employer must exercise care that is the same as or more protective than the care it uses to handle other confidential and sensitive information.[38] An employer cannot sell, lease, trade, or otherwise use an employee's biometric data for profit.[39] There is no exception in the statutory language of BIPA to the prohibition on selling data, such as consent.

Many employers fear a high monetary judgment against them in a potential BIPA lawsuit due to the liquidated damages that can accumulate for each violation, which applies per person.[40] For example, in the recently settled BIPA lawsuit against Facebook, it was estimated that the social media giant could have faced a $35 billion judgment due to its BIPA violations.[41] Facebook ultimately

---

Becky Yerak, *Mariano's, Kimpton Hotels Sued Over Alleged Collection Of Biometric Data: 'It's Something Very Personal'*, CHI. TRIB. (July 21, 2017), www.chicagotribune.com/business/ct-employers-biometrics-lawsuits-0723-biz-20170720-story.html.

33. 740 ILL. COMP. STAT. 14/15 (2020); John G. Browning, *Department: Technology: The Battle Over Biometrics*, 81 TEX. B. J. 674 (2018).

34. 740 ILL. COMP. STAT. 14/10 (2020). "Written release means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." *Id.*

35. 740 ILL. COMP. STAT. 14/15 (2020). "A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." *Id.*

36. 740 ILL. COMP. STAT. 14/15 (e)(1) (2020).

37. *Id.*

38. *Id.*

39. 740 ILL. COMP. STAT. 14/15(c) (2020); Alastair Johnson, *Fighting Biometric Fraud On The Blockchain*, LAW.COM (Oct. 26, 2018), www.law.com/legaltechnews/2018/10/26/fighting-biometric-fraud-on-the-blockchain/.

40. Susan Lorenc, Jim Shreve, & Ryan Gehbauer, *BIPA Litigation Offers No Legislative Reprieve To Employers – Yet*, THOMPSON COBURN LLP (June 10, 2019), www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2019-06-10/bipa-litigation-offers-no-legislative-reprieve-to-employers-yet.

41. Devin Coldewey, *Facebook Will Pay $550 Million to Settle Class Action Lawsuit Over Privacy Violations*, TECHCRUNCH (Jan. 29, 2020),

settled the lawsuit by agreeing to pay $550 million to the class of BIPA plaintiffs, which includes up to seven million Facebook users.[42] Under BIPA, a prevailing party may recover liquidated damages or actual damages, whichever is greater.[43] Liquidated damages include recovery of $1,000 for each negligent violation or $5,000 for each intentional or reckless violation.[44] Reasonable attorney's fees and costs may be recoverable, as well.[45] Additionally, a state or federal court may order an injunction to prevent an employer or entity from collecting any further data from the employee seeking redress.[46]

B. Who Is An "Aggrieved Person?" - Article III Standing

Prior to the Illinois Supreme Court's decision in *Rosenbach*, the main controversy surrounding BIPA had been the interpretation of the meaning of the term "aggrieved person" under the statute, and whether Article III Standing under the U.S. Constitution is satisfied.[47] In considering Article III Standing under BIPA, this section will highlight the following: the historical interpretation of Article III Standing; Illinois' interpretation of the term "aggrieved" under BIPA; Article III Standing in the Federal District Courts of Illinois; Article III Standing in the Federal District and Circuit Courts of California; Article III Standing in the Second Circuit Court of Appeals; and the Dormant Commerce Clause.

1. Historical Interpretation of Article III Standing

As a general concept, the U.S. Supreme Court has long held that Article III Standing requires that a plaintiff suffer an injury to a legally protected interest that is casually connected to the defendant's conduct, and such injury will be redressed by a court's

---

www.techcrunch. com/2020/01/29/facebook-will-pay-550-million-to-settle-class-action-lawsuit-over-privacy-violations/; Nicholas Iovino, *Ninth Circuit Advances $35 Billion Privacy Suit Against Facebook*, COURTHOUSE NEWS SERV. (Aug. 9, 2019), www.courthousenews.com/ninth-circuit-advances-35-billion-privacy-suit-against-facebook/.

42. Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html.

43. 740 ILL. COMP. STAT. 14/20 (2020).

44. *Id.* For example, in applying the threshold for each violation, a small employer with 100 employees that fails to comply with BIPA could be liable for a $100,000-500,000 verdict if the employer fails to obtain consent prior to data collection. Conversely, a large employer with 10,000 employees could be liable for a verdict of $10-50 million for the same type of violation if it applied to the employer's interactions with all of its employees.

45. *Id.*

46. *Id.*

47. Sheridan & Brooks, *supra* note 7.

decision.[48] Federal courts only have jurisdiction over actual cases and controversies, so standing is essential for a plaintiff to be heard in federal court.[49] The U.S. Supreme Court has not interpreted standing as applied to Illinois' BIPA statute or any other state biometric privacy statute. Nor has Congress passed any laws regulating the collection of biometric data.

The Article III Standing debate under BIPA has centered on federal district, federal appellate, and Illinois state courts' interpretations of the U.S. Supreme Court's 2016 decision in *Spokeo, Inc. v. Robins*. In *Spokeo*, the Court reiterated that a plaintiff must show that he or she suffered an "injury-in-fact" which is "fairly traceable" to the defendant's conduct.[50] The Court has long held that an injury "must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'"[51]

Under the first element of injury-in-fact framework, the injury must be concrete, particularized, and actual or imminent.[52] The Court noted that Congress has the power to define what constitutes an "injury," but Article III Standing requires a concrete injury for statutory violations, as well.[53] The injury must be "actual or imminent, not conjectural or hypothetical," but the injury does not need to be "tangible."[54] However, the existence of a statutory right on its face does not necessarily qualify a procedural violation as a concrete injury.[55]

---

48. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992); Los Angeles v. Lyons, 461 U.S. 95, 102 (1983); Warth v. Seldin, 422 U.S. 490, 508 (1975); Sierra Club v. Morton, 405 U.S. 727, 740-741 (1972).

49. Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1542-48 (2016) (holding that the appellate court failed in analyzing standing for suit brought under the Fair Credit Reporting Act of 1970, because it did not distinguish between "concreteness and particularization," where Plaintiff alleged that a consumer reporting agency generated inaccurate information for his Spokeo profile).

50. *Id.* at 1547.

51. *Lujan*, 504 U.S. at 560-61. The Court held that plaintiff wildlife organizations lacked standing because they failed to show causation of their injury and failed to show redressability. *Id.* The Court reiterated that there are three pongs to Article III Standing that must be satisfied. *Id.*

52. *Spokeo Inc.*, 136 S. Ct. at 1548.

53. *Id.* at 1549.

54. *Id.* at 1548. Despite the Court's holding in *Spokeo*, it did not determine the ultimate issue as to whether the plaintiff actually had Article III Standing. *Id.* at 1550. Rather, the Court remanded the case to the Ninth Circuit Court of Appeals fully address standing but analyzing "distinction between concreteness and particularization." *Id.*

55. Meyers v. Nicolet Rest. of De Pere, LLC, 843 F.3d 724, 727 (7th Cir. 2016). The court held that that plaintiff failed to allege a concrete injury for a violation under 15 U.S.C.S. § 1681c(g)(1) of the Fair and Accurate Credit Transactions Act. *Id.* Even though the restaurant printed his credit expiration date on his receipt in violation of 15 U.S.C.S. § 1681c(g)(1), the violation did not create an "appreciable risk of harm" or identity theft because no other person saw the receipt. *Id.*

2. Illinois' Interpretation Of "Aggrieved" Under BIPA

In regards to BIPA and standing, Illinois allows a private right of action from an individual or class of individuals.[56] The Illinois Attorney General may also enforce the statute, but litigation so far has been limited to class actions suits where the damages are much higher due to the stacking of a large number of plaintiffs.[57] BIPA states, "[a]ny person aggrieved by a violation of this Act shall have a right of action."[58] However, Illinois state, federal district, and federal appellate courts have grappled with determining whether the word "aggrieved" means even a "technical violation," such as a notice violation, is actionable.[59] In BIPA lawsuits, plaintiffs typically allege in their complaint that an entity violated the BIPA provisions requiring notice and consent.[60] Typically, defendants respond to the suit by filing a motion to dismiss and arguing the plaintiffs lack standing for failure to allege an actual injury resulting from such violation.[61] The statute does not explicitly define "aggrieved" in its definition section, so courts have discretion to interpret the term.[62]

The Illinois Appellate Court's 2017 ruling in *Rosenbach v. Six Flags Entertainment Corp.* initially made it more difficult for plaintiffs to survive a motion to dismiss, before the Illinois Supreme Court ruled on standing under BIPA in 2019.[63] In *Rosenbach*, the plaintiff alleged that the defendant-corporation violated BIPA's notice and consent requirement by collecting her son's thumbprint when he purchased a season pass at the theme park, without first obtaining his parent's written consent.[64] The plaintiff alleged "she would have never purchased a season pass for her son" had she known the defendant was going to collect the data.[65] The Illinois Appellate Court held that the plaintiff in *Rosenbach* failed to allege that she suffered an actual harm outside of the defendant violating a BIPA provision.[66] Therefore, the plaintiff did not meet the requirement of "aggrieved" as outlined by BIPA and could not

56. 740 ILL. COMP. STAT. 14/20 (2020).
57. Sheridan & Brooks, *supra* note 7.
58. 740 ILL. COMP. STAT. 14/20 (2020).
59. *Rosenbach,* 2017 IL App (2d) 170317, at ¶ 22.
60. *Id.*
61. *Id.* at ¶ 10.
62. *Id.* at ¶ 4.
63. Jeffrey D. Neuburger, *Illinois Appellate Court Reinstates Biometric Privacy Action, Finding Potential Harm In Alleged Disclosure Of Fingerprint To Outside Vendor*, NAT. L. REV. (Oct. 16, 2018), www.natlawreview.com/article/illinois-appellate-court-reinstates-biometric-privacy-action-finding-potential-harm.
64. *Rosenbach*, 2017 IL App (2d) 170317 at ¶ 10.
65. *Id.* at ¶ 28.
66. *Id.*

recover or receive liquidated damages based on the alleged technical violation.[67]

The Illinois Appellate Court's opinion in *Rosenbach* hinged upon the interpretation of the word "aggrieved."[68] The court declared that if every technical violation was actionable, the requirement that a person be "aggrieved by a violation of the Act" would effectively "render the word 'aggrieved' superfluous."[69] The court also noted that it was appropriate to assign the meaning of an undefined term in a statute using Black's Law Dictionary.[70] It found that the definition of "aggrieved" presupposed an actual harm or adverse effect.[71] It declared that, "if the Illinois legislature intended to allow for a private cause of action for every technical violation of the Act, it could have omitted the word 'aggrieved' and stated that every violation was actionable."[72] Thus, a plaintiff who alleges a technical violation must also allege some tangible or intangible adverse effect.[73]

On May 30, 2018, the Illinois Supreme Court granted the plaintiff's petition for leave of appeal.[74] The court issued its opinion on January 25, 2019, which reversed the lower court's opinion.[75] The Illinois Supreme Court described the defendant's position as "untenable" with the legislature's intent in enacting BIPA.[76] It quoted century-old precedent to find that "aggrieved simply 'means having a substantial grievance; a denial of some personal or property right.'"[77] The court presumed that the legislature understood this precedent in enacting BIPA, and, therefore, "aggrieved" means that a legal right was adversely affected.[78]

Further, the Illinois Supreme Court found that the General Assembly created a legal right when it "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information."[79] A "violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach."[80] As such, no additional harm needs to be

67. *Id*. *Cf* Sekura v. Krishna Schaumburg Tan, Inc., 115 N.E.3d 1080 (Ill. App. 1st 2018), *appeal denied*, 119 N.E.3d 1034 (Ill. 2019) (holding that the plaintiff was not required to show an additional beyond a technical violation of BIPA).

68. Neuburger, *supra* note 63.

69. *Rosenbach*, 2017 IL App (2d) 170317, at ¶ 23.

70. *Id.* at ¶ 20.

71. *Id*.

72. *Id.* at ¶ 23.

73. *Id.* at ¶ 28.

74. Neuburger, *supra* note 63.

75. *Rosenbach*, 129 N.E.3d at 1207.

76. *Id.* at 1204.

77. *Id.* at 1205 (quoting Glos v. People, 102 N.E. 763 (Ill. 1913)).

78. *Id*.

79. *Id.* at 1206.

80. *Id*.

plead or proven by the plaintiff.[81] If an entity does not comply with Section 15 of BIPA (retention, collection, disclosure, destruction), then the entity has committed a violation, thus entitling a plaintiff to recovery, as Article III Standing has been met.[82]

3. Article III Standing in the Federal District Courts of Illinois

A number of employees have collectively sued their employers in class action suits, often in the Federal District Courts of Illinois.[83] In 2017 and 2018, there were twelve BIPA cases in Illinois filed against employers.[84] The District Court for the Northern District of Illinois first weighed in on Article III Standing in the BIPA context in 2018.[85] A federal court has an independent obligation to determine whether it has subject matter jurisdiction over a claim.[86] "[S]tate law cannot create Article III Standing where none exists under [] federal precedents."[87] In *Johnson v. United Air Lines, Inc.*, an employee sued United Airlines because the airline required fingerprint scans as an employment condition, but failed to obtain the employee's consent prior to collection.[88] The court dismissed the claim because a collective bargaining agreement preempted the court from hearing the claim.[89] However, the court felt obligated to address the employee's lack of standing in its opinion.[90] It reiterated that BIPA was enacted "to protect '[t]he public welfare, security, and safety.'"[91] A consent violation did not prove there was risk of

81. *Id.*

82. *Id.*

83. Sheridan & Brooks, *supra* note 7.

84. Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499 (S.D. N.Y. Jan. 27, 2017); Barnes v. ARYZTA, LLC, 288 F. Supp. 3d 834 (N.D. Ill. Dec. 20, 2017); Kiefer v. Bob Evans Farms, LLC, 313 F. Supp. 3d 966 (N.D. Ill. May 23, 2018); Dixon v. Washington & Jane Smith Cmty., 2018 U.S. Dist. LEXIS 90344 (N.D. Ill. May 31, 2018); Howe v. Speedway LLC, 2018 U.S. Dist. LEXIS 90342 (N.D. Ill. May 31, 2018); Goings v. UGN, Inc., 2018 U.S. Dist. LEXIS 99273 (N.D. Ill. June 13, 2018); Johnson v. United Air Lines, Inc., 2018 U.S. Dist. LEXIS 127959 (N.D. Ill. July 30, 2018); Aguilar v. Rexnord LLC, 2018 U.S. Dist. LEXIS 110765 (N.D. Ill. July 3, 2018); Miller v. Southwest Airlines Co., 2018 U.S. Dist. LEXIS 143369 (N.D. Ill. August 23, 2018); White vs. Hegewisch Development Corp., 2018 WL 3772630, at *1 (Ill. Cir. Ct. 2018); Bryant v. Loews Chicago Hotel Inc. et al., 2018 WL 3712874, at *1 (Ill. Cir. Ct. 2018).

85. Johnson v. United Air Lines, Inc., No. 17 C 08858 2018 U.S. Dist. LEXIS 127959, at *1 (N.D. Ill. July 30, 2018).

86. Cook v. Winfrey, 141 F.3d 322, 325 (7th Cir. 1998).

87. *Patel*, 290 F. Supp. 3d at 952–53 (highlighting that federal courts require Article III Standing regardless of whether a state court has found standing on the same issue).

88. *Johnson,* No. 17 C 08858 2018 U.S. Dist. LEXIS 127959, at *3.

89. *Id.*

90. *Id.* at *10.

91. *Id.* at *11 (quoting 740 ILL. COMP. STAT. 14/5(g) (2020)) (alteration in original).

disclosure, so plaintiff needed to establish an actual injury based on "subsequent disclosure."[92]

In 2018, the Northern District of Illinois clarified whether there is standing when biometric data is shared with a third party in the case *Dixon v. Washington & Jane Smith Cmty*.[93] An employer, Smith Senior Living, disclosed an employee's fingerprint information to a third party—out-of-state vendor Kronos, which supplied fingerprint scanners the employer used for biometric timekeeping.[94] In contrast to previous cases that failed to allege a concrete injury, the employee in *Dixon* showed an actual harm, according to the court.[95] The court found that the employee met the standing requirement because the employer did, in fact, "disclose" the biometric information to a third party vendor without the employee's consent, which resulted in an injury.[96] Specifically, the court clarified the employee met Article III Standing because her privacy injury was "fairly traceable to the BIPA violations alleged, and it may be redressed by at least some of the relief that [Plaintiff] seeks."[97] The holding in *Dixon* opened the door to a large area of liability for large employers that use a third party to maintain their employee's biometric timecards.[98]

The court in *Dixon* also noted the employer's defense—that the employee alleged "a bare procedural violation of BIPA"—was synonymous with attacking Article III Standing.[99] The employer argued that it did not trigger the burden to show Article III Standing because neither party challenged subject matter jurisdiction.[100] The court rejected this argument because the employer used authority that directly challenged Article III.[101] Similar to the defendant in *Dixon*, in *Roberts v. Dart Container Corp. of Illinois*, the defendants removed the case to federal court pursuant to the Class Action Fairness Act,[102] and then argued the

92. *Id.* at *11-12.

93. Dixon v. Washington & Jane Smith Cmty., No. 17 C 8033, 2018 U.S. Dist. LEXIS 90344, at *1 (N.D. Ill. May 31, 2018) (discussing an employee that sued its employer by alleging the employer violated their privacy rights under BIPA for disclosing biometric data to a third party, Kronos, which is a company that handles timekeeping for employers without the employer or Kronos obtaining written consent for the data).

94. *Id.* at *2-3.

95. *Id.* at *30.

96. *Id.* at *39.

97. *Id.* at *33.

98. *See* 740 ILL. COMP. STAT. 14/15 (2020) (noting that a private entity cannot profit from a person's biometric data collection).

99. *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *10.

100. *Id.*

101. *Id.* at *12 (citing Robins v. Spokeo, Inc., 867 F.3d at 1108, 1112-18 (9th Cir. 2017) [hereinafter *Spokeo II*]; Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 911-13 (7th Cir. 2017); Monroy v. Shutterfly, Inc., No. 16 C10984, 2017 WL 4099846, at *8 n.5 (N.D. Ill. Sept. 15, 2017); *Vigil*, 235 F. Supp. 3d at 507-19).

102. The Class Action Fairness Act of 2005, 119 Stat. 4 (2005), 28 USC 1711,

plaintiff did not have standing.[103] Furthermore, the U.S. Supreme Court has held that a defendant undoubtedly triggers the burden to show federal jurisdiction when the defendant removes a case to federal court, regardless of other considerations.[104]

4. Article III Standing in the Federal Courts of California

Similar to the Illinois Supreme Court's holding in *Rosenbach*, the Ninth Circuit became the first federal circuit to hold that a plaintiff who alleges a technical violation under BIPA has Article III Standing in *Patel v. Facebook, Inc*.[105] Prior to the Ninth Circuit's holding in *Patel*, the U.S. District Court for the Northern District of California addressed standing under BIPA and found that a technical violation satisfied standing because it is a concrete harm.[106] There, a Facebook user alleged that Facebook's "tag suggestions" program violated BIPA's notice and consent provision.[107] Facebook used software designed to match the faces of people in photos with the names of the Facebook users in the photos, thereby harvesting biometric data from millions of users without gaining prior consent.[108] The court held that BIPA does not require additional proof of an actual harm or financial loss because the privacy right violation is sufficient.[109] Additionally, it rejected the defendant's argument that BIPA only regulates "live" facial geometry scans, rather than photographs, such that photographic information from facial recognition software is excluded from

---

states:

> (b) In General. -- A class action may be removed to a district court of the United States in accordance with section 1446 (except that the 1-year limitation under section 1446(b) shall not apply), without regard to whether any defendant is a citizen of the State in which the action is brought, except that such action may be removed by any defendant without the consent of all defendants. (c) Review of Remand Orders.-- (1) In general.-- Section 1447 shall apply to any removal of a case under this section, except that notwithstanding section 1447(d), a court of appeals may accept an appeal from an order of a district court granting or denying a motion to remand a class action to the State court from which it was removed if application is made to the court of appeals not less than 7 days after entry of the order.

103. Roberts v. Dart Container Corp. of Illinois, No. 17 C 9295, 2018 WL 3015793, at *1 (N.D. Ill. Mar. 12, 2018).

104. *Lujan*, 504 U.S. at 561.

105. *Patel*, 932 F.3d at 1274; Michael E. Brewer, William F. Dugan & Jenna Neumann, *The Ninth Circuit Clears The Way For BIPA Class Actions*, BAKER & MCKENZIE LLP (Aug. 13, 2019), www.theemployerreport.com/2019/08/the-ninth-circuit-clears-the-way-for-bipa-class-actions/.

106. *In re Facebook*, 2018 U.S. Dist. LEXIS 81044, at *5.

107. *Id.* at *3.

108. Singer & Isaac, *supra* note 42.

109. *In re Facebook*, 2018 U.S. Dist. LEXIS 81044, at *5.

BIPA's protections.[110]

In the preceding class certification order, the Northern District of California Court reached its holding by interpreting the Illinois Appellate Court's finding in *Rosenbach*, BIPA's plain language, and the legislative intent behind the Act.[111] The court determined that, had the plaintiff in *Rosenbach* alleged a privacy right violation in her complaint instead of a BIPA notice and consent violation, then she would have standing.[112] Accordingly, the court determined that the holding in *Rosenbach* meant that a privacy right injury qualified as an injury, for standing purposes.[113] Even if "*Rosenbach* might be read differently, the [c]ourt would part company with it" because Illinois law is not binding on California.[114] This commentary demonstrates that, while the Illinois Supreme Court has weighed in on standing, federal courts still require Article III Standing, therefore federal courts can still weigh in on the standing issue.

The Northern District of California Court concluded a BIPA notice and consent violation was the exact harm that the legislature intended to prevent.[115] The Illinois legislature could have used language in BIPA that required an "actual" injury, as it has in other statutes, but it did not.[116] The Northern District of California pointed out that the Illinois Appellate Court in *Rosenbach* did not address the Illinois Supreme Court's precedent established in *Jones*—even though it is still good law.[117] In *Jones*, the Illinois Supreme Court held that a statutory "aggrieved" party includes "a direct, immediate and substantial interest rather than a speculative, theoretical, inconsequential or remote interest."[118]

On appeal, the Ninth Circuit Court of Appeals weighed in on Article III Standing under BIPA in *Patel*.[119] Relying on the U.S. Supreme Court's recent Fourth Amendment jurisprudence, the Ninth Circuit concluded the U.S. Supreme Court viewed technological advances as "increas[ing] the potential for

110. *Id.* at *15.

111. *In re Facebook*, 2018 U.S. Dist. LEXIS 63930, at *19.

112. *Id.* at *18.

113. *Id.*

114. *Id.*

115. *Id.* at *19-20.

116. *Id.* at *20. See e.g., Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. 505/10a (2007) (stating that a private right of action is limited to person who suffers "actual" damage).

117. *In re Facebook*, 2018 U.S. Dist. LEXIS 63930, at *21 (pointing out, "Rosenbach omits any discussion of Jones, and Facebook also does not address it in its papers. That is a concern because Jones is good law in Illinois and is actively cited today by other federal courts and Illinois state courts, significantly in the BIPA context").

118. *Id.* at *20 (quoting Am. Sur. Co. v. Jones, 51 N.E.2d 122, 126 (Ill. 1943) (holding that aggrieved refers to a substantial personal or property interest is violated) (internal quotations omitted).

119. *Patel*, 932 F.3d at 1268.

unreasonable intrusions into personal privacy."[120] By concluding that a biometric privacy right qualified as a closely-related traditional harm recognized by courts, the Ninth Circuit pointed out the consequences of Facebook's "tag suggestions," when it stated:

> Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who are present in the photo.[121]

The court found that developing a face template from facial recognition technology "invades an individual's private affairs and concrete interests."[122] For example, "a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cellphone."[123] Therefore, the court held that "plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article III standing" when they prove that the defendant failed to obtain written consent, prior to collecting, using, and storing biometric identifiers.[124]

Following the Ninth Circuit's refusal to grant the defendant's motion to dismiss for lack of standing in *Patel*, and the U.S. Supreme Court's refusal to grant certiorari to review of the case, Facebook settled with the plaintiffs for $550 million.[125] Some have heralded the settlement as landmark and record-breaking, while others have pointed out that the settlement is dismal when compared to Facebook's potential liability of $35 billion.[126] In comparing the settlement and the potential liability, Facebook's settlement only amounted to slightly less than 1.5% of its liability under BIPA, had the case proceeded to trial and a verdict was entered against Facebook. The settlement is made more miniscule by the fact that Facebook made over $70 billion in revenue in 2019, largely from digital advertisements.[127] Thus, a $550 million

120. *Id.* at 1273 (citing Carpenter v. United States, 138 S. Ct. 2206 (2018); United States v. Jones, 565 U.S. 400, 416 (2012); Riley v. California, 573 U.S. 373, 386 (2014); Kyllo v. United States, 533 U.S. 27, 34 (2001)).

121. *Id.*

122. *Id.* Privacy rights have long been actionable at common law and "privacy torts do not always require additional consequences to be actionable." *Id.* at 1274 (quoting Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017)).

123. *Id.*

124. *Id.* at 1274.

125. Kamran Salour & Melinda L. McLellan, *Following SCOTUS Cert Denial, Facebook Settles BIPA Case for $550 Million*, BAKERHOSTETLER (Jan. 31, 2020), www.dataprivacymonitor.com/biometrics/following-scotus-cert-denial-facebook-settles-bipa-case-for-550-million/.

126. Coldewey, *supra* note 41.

127. J. Clement, *Facebook: Annual Revenue 2009-2019*, STATISTA (Feb. 3,

settlement is miniscule in that regard.

5. Article III Standing in the Second Circuit Court of Appeals

Other federal circuit courts have also weighed in on BIPA, and these cases are actively cited by federal district courts. In *Santana v. Take-Two Interactive Software*, the U.S. Court of Appeals for the Second Circuit came to the same conclusion as the Illinois Appellate Court's interpretation in *Rosenbach*, agreeing that a technical violation did not satisfy standing without additional actual harm.[128] In *Santana*, the court held that a plaintiff failed to show that violating a provision of BIPA created a material risk of harm.[129] It also noted that a reasonable person would have been on notice that defendant was collecting biometric data, due to the invasive nature of the collection.[130] Plaintiff's fear of participating in other biometric transactions did not qualify as an injury-in-fact.[131] The Second Circuit emphasized that the Illinois legislature already clarified that a "consumers' withdrawal from biometric-facilitated transactions" only arises when data has been "collected or disclosed without his or her authorization."[132] While the *Santana* opinion in 2017 predated the Illinois Supreme Court's ruling in *Rosenbach* in 2019,[133] that does not necessarily mean the outcome in *Santana* would have differed, had it post-dated *Rosenbach*, because the Second Circuit could have reached the same conclusion by relying on the Dormant Commerce Clause.

6. The Dormant Commerce Clause

Defendants in at least two federal district court cases claimed

---

2020), www.statista.com/statistics/268604/annual-revenue-of-facebook/.

128. *Santana*, 717 Fed. App'x at 15-17. Video game users sued a company that used their biometric data in a 3D mapping process to create an avatar. *Id.* at 14. The game displayed the following terms and conditions: "Your face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay." *Id*. "By proceeding you agree and consent to such uses and other uses pursuant to the End User License Agreement. www.take2games.com/eula." *Id*. The game would not proceed unless the users clicked continue. *Id*. The players sued for failure to gain their written consent prior to data collection under BIPA. *Id*. The court dismissed the claim because the players failed to allege Article III Standing. *Id*. at 17-18.

129. *Id.* at 17.

130. *Id.* at 15-16.

131. *Id.* at 17.

132. *Id.*

133. *Rosenbach*, 129 N.E.3d at 1207 (holding "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.").

that subjecting out-of-state defendants to BIPA is a violation of the Dormant Commerce Clause.[134] The Dormant Commerce Clause precludes a state from regulating or controlling economic activity, when that activity is conducted solely outside of its border.[135] In BIPA cases, defendants have argued that subjecting them to BIPA regulations violates the Dormant Commerce Clause because Illinois would be attempting to unduly burden interstate commerce.[136] Therefore, the defendants argue that it is unconstitutional for Illinois to regulate out-of-state businesses' collection of biometric data.[137] The Ninth Circuit has rejected defendants' argument.[138] The court reasoned the lawsuit was based on a violation of an Illinois state statute, on behalf of Illinois residents, who used Facebook in Illinois, and the economic activity occurred within Illinois only.[139] BIPA would not force Facebook to adjust its practices in any other state, and Facebook could easily cease its interaction with Illinois users.[140]

C. Biometric Privacy Protections in Other States

The above case analysis only covers the interpretation of Illinois' BIPA. Similar to most privacy laws in the United States, biometric data protection is a patchwork of state law.[141] Other states are free to enact their own statutes. However, only a few states have actually enacted biometric data privacy statutes.[142] Illinois, Texas, and Washington are the only states that have passed comprehensive statutes prohibiting entities from collecting biometric data without a person's prior consent.[143] Additionally, the California Consumer Privacy Act (CCPA)[144] became effective on

134. *In re Facebook,* 2018 U.S. Dist. LEXIS 81044, at *12; Monroy v. Shutterfly, Inc., No. 16 C 10984 (N.D. Ill. Sept. 15, 2017).

135. Healy v. Beer Inst., Inc., 491 U.S. 324, 336-37 (1989).

136. *In re Facebook,* 2018 U.S. Dist. LEXIS 81044, at *13-14.

137. *Id.* at *13.

138. *Id.*

139. *Id.* at *14.

140. *Id.*

141. Sharon Roberg-Perez, *The Future Is Now: Biometric Information And Data Privacy*, 31 ANTITRUST 60, 63 (2017); W. Gregory Voss & Kimberly A. Houser, *Personal Data And The Gdpr: Providing A Competitive Advantage For U.S. Companies*, 56 AM. BUS. L.J. 287, 340 (2019).

142. *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across The United States*, NAT'L L. REV. (Mar. 25, 2019), www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.

143. Sheridan & Brooks, *supra* note 7. Additionally, in California, the California Consumer Privacy Act (CCPA) regulates how employers use biometric data. *The Latest on California's Approach to Biometrics in the Workplace,* NAT'L L. REV. (Oct. 10, 2019), www. natlawreview.com/article/latest-california-s-approach-to-biometrics-workplace.

144. California Consumer Privacy Act of 2018 1.81.5 CAL. CIV. CODE §

January 1, 2020, and it regulates some biometric data collection, but not to the same extent as BIPA.[145]

Texas became the second state to enact a biometric privacy law in 2009.[146] Texas defines a "biometric identifier" as "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[147] The Texas statute does not protect the broad umbrella of "biometric *information*" that Illinois protects.[148] Written authorization prior to collection is not required, but notice and consent must be given.[149] Any data collection under this statute's protection must be destroyed within a "reasonable time," up to a year, after which the data is no longer needed.[150] The penalty is $25,000 per violation, but only the attorney general may bring an action rather than an individual or class.[151]

Washington passed its Biometric Privacy Law under HB 1493 on April 11, 2017, which became effective on July 23, 2017.[152] Washington's definition of "biometric identifier" includes "an individual's retina or iris scan, fingerprint, voiceprint, DNA, or scan of hand or face geometry."[153] It does not include photographs or audio recordings.[154] The Washington law does not regulate employers that collect biometric data for timekeeping.[155] The employer exemption exists because the Washington statute only applies to commercial collectors of biometric identifiers.[156] A "Commercial Purpose" is defined as "a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier."[157] Additionally, only the attorney general can sue to enforce the statute for a

---

1798.100 - 199. Due to the timing the CCPA's enactment and effective date in 2020, it is not discussed at length in this comment.

145. Anthony Zaller, *Employee Biometric Data Issues Under California Law*, CAL. EMP'T L. REP. (Feb. 7, 2020), www.californiaemploymentlawreport.com/2020/02/employee-biometric-data-issues-under-california-law/.

146. TEX. BUS. & COM. CODE § 503.001 (2009).

147. *Id.*

148. *See* Browning, *supra* note 33, at 676 (clarifying that Texas' statute does not include the data that "is converted into a code or template" and stored based upon a person's actual fingerprint for example).

149. *Id.*

150. TEX. BUS. & COM. CODE § 503.001(c)(3) (2020).

151. TEX. BUS. & COM. CODE § 503.001(d) (2020).

152. WASH. REV. CODE § 19.375.020 (2017).

153. WASH. REV. CODE § 19.375.010 (2020).

154. *Id.*

155. Annemaria Duran, *Learn How Washington's New Biometric Privacy Law Affects Businesses*, SWIPECLOCK WORKFORCE MGMT. (Jan. 3, 2018), www3.swipeclock.com/blog/learn-washingtons-new-biometric-privacy-law-affects-businesses/.

156. *Id.*

157. WASH. REV. CODE § 19.375.010 (2020).

violation.[158]

At least eight other states have attempted to pass biometric privacy laws, but these attempts have failed.[159] The proposed bills in Connecticut, Massachusetts, and New York did not allow an individual right of action.[160] The states that have attempted to pass or have biometric privacy bills pending, include: Alaska, Arizona, Delaware, Florida, Hawaii, Idaho, Montana, New Hampshire, New Jersey, Oregon, and Rhode Island.[161]

Some states that failed to pass comprehensive biometric data privacy bills have been able to pass other statutory protections. For example, in New York, the expansion of New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD), which requires notice if there is biometric information that has been accessed by an unauthorized entity and requires safeguards for protecting biometric information, became effective in February 2020.[162] Similarly, Arkansas updated its data breach response law, which requires individuals and businesses to maintain reasonable measures to protect biometric data from unauthorized access and disclosure.[163] If biometric data is breached, then businesses and individuals are required to disclose it to the Attorney General when the breach affects more than 1,000 individuals and there is a "reasonable likelihood of harm to consumers."[164]

D. Employer Data Collection

An understanding of the volume of hourly employees in the United States is crucial to appreciate the impact of BIPA for both employers and employees. The Department of Labor estimated that 79.9 million hourly employees worked in the United States in 2016.[165] Some employers are transitioning to the use of biometric data collection to track employee timecards in lieu of identification badges, which primarily affects hourly workers.[166] Additionally,

158. *Id.*

159. Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth Of Illinois Cousin*, BLOOMBERG L. (July 18, 2017), www.bna.com/washington-biometric-privacy-n73014461920/.

160. *Id.*

161. *Id.*; *State Biometric Privacy Legislation: What You Need to Know*, THOMPSON HINE LLP (Sept. 5, 2019), www.thompsonhine.com/publications/state-biometric-privacy-legislation-what-you-need-to-know.

162. THOMPSON HINE LLP, *supra* note 148.

163. *Consumer Protection Security Or Data Breach*, ARK. ATT'Y GEN., www.arkansasag.gov/consumer-protection/identity/column-one/security-or-data-breach/ (last visited Mar. 19, 2020).

164. *Id.*

165. *Characteristics Of Minimum Wage Workers*, BLS (Apr. 2017), www.bls.gov/opub/reports/minimum-wage/2016/home.htm.

166. Lauraann Wood, *Ill. Lighting Co. Sued In Latest Biometric Privacy Action*, LAW360 (Oct. 1, 2018), www.law360.com/articles/1088059/ill-lighting-

employers use biometrics to secure business areas or devices, control access to information, trace employee trainings, and even track employees' attendance in wellness programs promoting preventative health measures.[167] Many employers also use biometric collection to prevent timekeeping theft through "buddy clocking" where an employee clocks in for another employee.[168] Under BIPA, employers are required to publish a written plan of collecting, storing, and safeguarding the information.[169]

Employee BIPA plaintiffs typically sue employers for violating the informed consent requirement.[170] For instance, ramp and operations employees at Midway Airport in Chicago sued their employer, Southwest Airlines ("Southwest") in 2017 for violating their "substantive privacy rights" under BIPA.[171] In *Miller v. Southwest Airlines*, after Southwest had implemented a finger-scanning biometric timekeeping system, which also assisted with payroll, the system became the subject of plaintiffs' suit.[172] The employees alleged that Southwest failed to comply with three BIPA requirements: (1) provide notice about the timekeeping program; (2) obtain written consent to collect data and transmit it to third parties; and (3) publish data retention schedules.[173] The employees asserted they "would not have agreed to work for [Southwest]" at their salaries, had they known Southwest was going to collect their biometric data.[174] The court agreed and found that Southwest owed the employees additional compensation for taking the employees' data without compensation.[175] The employees requested "compensation for the commercial value of their biometric information."[176] *Miller v. Southwest Airlines* is a prime example of how employers are utilizing biometric data and why employees are suing employers.

Beyond timekeeping, there is another rising technology that could be implicated by BIPA: artificial intelligence facial analytics.[177] Employers have begun to use "hiring robots" to

---

co-sued-in-latest-biometric-privacy-action.

167. Annemaria Duran, *Understanding the Illinois Biometric Information Privacy Act & Its Relation to Employers,* SWIPECLOCK WORKFORCE MANAGEMENT (Dec. 27, 2017), www3.swipeclock.com/blog/understanding-illinois-biometric-information-privacy-act-relation-employers/.

168. Hannah Meisel, *United Airlines Latest To Be Sued Under Ill. Biometrics Law,* LAW360 (Nov. 8, 2017), www.law360.com/articles/983384/united-airlines-latest-to-be-sued-under-ill-biometrics-law.

169. 740 ILL. COMP. STAT.14/5 (2020).

170. Wood, *supra* note 148.

171. Miller v. Southwest Airlines Co., No. 18 C 86, 2018 U.S. Dist. LEXIS 143369, at *2-3 (N.D. Ill. Aug. 23, 2018).

172. *Id.* at *2.

173. *Id.*

174. *Id.*

175. *Id.* at *4, 15.

176. *Id.* at *15.

177. For a fuller discussion of this technology and Illinois' attempt to

interview applicants through pre-recorded videos submitted to the employer by applicants.[178] The robots "analyze facial expressions, gestures, and word choice to evaluate qualities such as honesty, reliability, and professionalism."[179] Some attorneys predict that this technology will be subject to litigation under BIPA because employers are using biometric facial data to analyze the applicants.[180] In this context, employers using interview robots would need to gain consent from applicants prior to data collection, in order to comply with BIPA.[181]

III. ANALYSIS

The main controversy surrounding BIPA has been what type of injury a plaintiff must allege to have Article III Standing to sue a private entity that collected or distributed a plaintiff's biometric data. This section will analyze Article III Standing then compare various state biometric privacy statutes. This section will also analyze the privacy impact on employees and potential for retaliatory discharge. It will include the financial impact on employers, statutory provisions in BIPA that have not been addressed by Illinois courts and legislature, and areas wherein BIPA claims could grow.

A. Interpreting Article III Standing

"[T]he U.S. Supreme Court has noted that 'both common law and the literal understanding of privacy encompass the individual's

---

regulate the notice aspect of it to applicants, see Gabrielle Neace, *AIVIA: A Step Towards Protecting Data Privacy Or A Continuation Of The Push For Individuals To Trade Their Privacy Rights For Employment?*, UIC J. MARSHALL L. REV. (Feb. 20, 2020), lawreview.jmls.uic.edu/aivia-a-step-towards-protecting-data-privacy-or-a-continuation-of-the-push-for-individuals-to-trade-their-privacy-rights-for-employment/.

178. Michael J. Bologna, *Law On Hiring Robots Could Trigger Litigation For Employers*, BLOOMBERG L. (Oct. 11, 2019), news.bloomberglaw.com/daily-labor-report/law-on-hiring-robots-could-trigger-litigation-for-employers.

179. *Id.*

180. Erin Bolan Hines, *Illinois Employers Using AI To Screen Applicants Could Face Litigation, Bloomberg Reports*, SHOOK, HARDY, & BACON LLP (Oct. 12, 2019), www.shb.com/news/2019/10/hines-bolan-aivia-act-bloomberg; Katherine P. Sandberg & Robert T. Quackenboss, *Illinois Enacts AI Interview Law Amid an International Trend Toward Regulation*, HUNTON ANDREWS & KURTH (Nov. 18, 2019), www.huntonlaborblog.com/2019/11/articles/legislative-federal-state-developments/illinois-enacts-ai-interview-law-amid-an-international-trend-toward-regulation/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HuntonEmploymentLaborLawPerspectives+(Hunton+Employment+%26+Labor+Law+Perspectives)#page=1.

181. 740 ILL. COMP. STAT. 14/15 (2020).

control of information concerning his or her person.'"[182] Historically, a personal privacy right qualifies as an intangible injury-in-fact under Article III.[183] Moreover, Illinois law has recognized a violation of privacy rights as a valid tort claim for decades.[184] In *Spokeo*, the U.S. Supreme Court held that two additional considerations are made when determining whether an "intangible" injury qualifies as concrete harm.[185] The first consideration is "whether an alleged intangible harm *has a close relationship* to a harm that has traditionally been regarded as providing a basis for a lawsuit."[186] The second is whether Congress has recognized the "legally cognizable injuries [as] concrete."[187] However, the U.S. Supreme Court has not been clear as to what intangible injuries qualify for Article III Standing.[188]

Even though BIPA is not a federal statute, the Court never distinguished state statutes as less important than federal ones.[189] "[T]here is no good reason why the judgment of a state legislature should be treated as less important than that of Congress in deciding when the violation of a statutory grant in itself amounts to a real and concrete injury."[190] The Illinois legislature's recognition of the injury should be considered in defining an intangible harm just as a federal statute would be used.[191] By enacting BIPA, the Illinois legislature intended to protect a citizen's right to control their own biometric data, which suggests that any violation was meant to be a cognizable injury.[192] Further, remedies have long been awarded to address "invasions of privacy, intrusion upon seclusion, and nuisance[,]" all of which qualify as intangible injuries.[193] In considering the U.S. Supreme Court and Illinois Supreme Court's historical recognition of privacy rights as well as the Illinois legislature's intent in enacting BIPA, Article III Standing should be

182. Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017) (quoting U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) (holding that disclosing an FBI rap sheet to a third-party "could reasonably be expected to constitute an unwarranted invasion of personal privacy.")).

183. *Id.*

184. Leopold v. Levin, 259 N.E.2d 250, 254 (Ill. 1970); Lovgren v. Citizens First Nat. Bank of Princeton, 534 N.E.2d 987, 990 (Ill. 1989).

185. *Spokeo*, Inc., 136 S. Ct. at 1549.

186. *Id.* (emphasis added).

187. *Id.* (alteration added).

188. Matthew B. Kugler, *From Identification To Identity Theft: Public Perceptions Of Biometric Privacy Harms*, 10 UC IRVINE L. REV. 107, 143 (2019).

189. *See* Perlin v. Time Inc., 237 F. Supp. 3d 623, 639-42 (E.D. Mich. 2017) (holding that a customer had standing because their information was disclosed in a violation of Michigan's Video Rental Privacy Act).

190. *Patel*, 290 F. Supp. 3d at 953.

191. *Id.*

192. 740 ILL. COMP. STAT. 14/5 (2020).

193. Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037, 1043 (9th Cir. 2017) (citing Restatement (Second) of Torts § 652(B)); *Patel*, 290 F. Supp. 3d at 954.

satisfied when a plaintiff brings suit for a violation of BIPA in state or federal court. A biometric data privacy interest is just as important as other common law privacy interests.

It could be strategic for a BIPA defendant to remove the case to federal court, but if a defendant removes a case, it may acquire the burden to show the plaintiff had standing.[194] The "party" asserting federal jurisdiction bears the burden to show that Article III Standing existed at the time the suit was removed to federal court.[195] The Northern District of Illinois has noted that defendants cannot argue in one motion that standing does not exist, then argue for removal in another motion.[196] A court may remand a case even if the defendant only indirectly casts doubt on jurisdiction.[197] The Seventh Circuit has noted that courts should construe "the removal statute[198] narrowly, resolving any doubt in favor of the plaintiff's choice of forum in state court."[199] Therefore, BIPA suits that begin in state court will likely remain in state court because defendants' central arguments have attacked standing.

B. Comparing Illinois' BIPA with Other State Privacy Statutes

BIPA is considered the strongest biometric privacy act among the states because Illinois is the only state that allows an individual to sue for a violation.[200] Neither Texas nor Washington allow for a "private right of action," rather only the attorney general can enforce a violation in those states.[201] Aside from that distinction, there are multiple similarities and differences between the statutes in Illinois and Texas.[202] Texas and Illinois both require employers to use "reasonable care" to protect data; destroy data that is no longer needed; give notice to the employee; and gain consent from

194. Collier v. SP Plus Corp., 889 F.3d 894, 895 (7th Cir. 2018) (per curiam) (remanding a case back to the district court to return it to state court because it was unremovable due to plaintiff's lack of standing).

195. *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *10; *Collier,* 889 F.3d at 896.

196. Mocek v. Allsaints USA Ltd., 220 F. Supp. 3d 910, 914-15 (N.D. Ill. 2016).

197. *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *6 (quoting Zhirovetskiy v. Zayo Group, LLC, No. 17 C 5876, dkt. no. 49 (N.D. Ill. Mar. 7, 2018)) (holding that the "the spirit" of defendant's argument indirectly casted doubt on Article III Standing so remand was granted).

198. 28 U.S.C. § 1447 (2018) (describing "if at any time before final judgment it appears that the district court lacks subject matter jurisdiction, the case shall be remanded.").

199. *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *3 (quoting Schur v. L.A. Weight Loss Centers, Inc., 577 F.3d 752, 758 (7th Cir. 2009)).

200. Shukovsky, *supra* note 159.

201. *Id.*

202. Sheridan & Brooks, *supra* note 7.

the employee.[203]

The Texas statute is only more stringent than Illinois in two very limited areas: the time limit to destroy data is shorter and the liquidated damages are higher.[204] The possibility of a lawsuit is much higher in a state where every private person can sue compared to a state where only the attorney general can sue.[205] Illinois is more stringent overall because it requires "written" consent, rather than verbal consent.[206] It also covers "biometric information,"[207] which is broader than Texas' "biometric identifier" categorization.[208] Illinois does not specify the content or format of the written release, so presumably the release could be obtained electronically with a simple "accept" button, rather than a signature.[209] As the statute is silent, the courts may interpret this meaning "[i]n light of the legislature's intent."[210]

C. BIPA Statutory Interpretation, Failed Amendments, and Potential Areas of Litigation

In looking to the language of BIPA itself, there are issues that have not been addressed by the Illinois legislature or interpreted by Illinois courts. As to statutory interpretation, the Illinois Supreme Court has held that legislative intent from the language of a statute is essential to its interpretation.[211] The statute should be read as a whole, including "its nature, its object and the consequences that would result from construing it one way or the other."[212]

Other Illinois employment statutes could help determine the legislative intent surrounding BIPA and the form of the required written consent.[213] BIPA does mention that "[w]ritten release'

---

203. Browning, *supra* note 33, at 676.

204. *See id*. (explaining that under Texas statute, the company retaining biometric data must destroy it within a year after the data is no longer needed. Additionally, the liquidated damages in Texas are $25,000 per violation).

205. *See id*. (noting that only the attorney general can enforce the Texas statute to recover damages or other remedies). *See also* United States v. Goodwin, 457 U.S. 368, 380, n. 11 (1982) (holding that the attorney general retains broad discretion to determine which claims to prosecute).

206. 740 ILL. COMP. STAT. 14/10 (2020).

207. Browning, *supra* note 33, at 675 (describing that Texas does not include data that "is converted into a code or template").

208. *Id.*

209. *Id.*

210. *See* People v. Garcia, N.E.2d 32, 36 (Ill. 2011) (relying on legislative intent to interpret a statute).

211. People v. Fort, 88 N.E.3d 718, 723-24 (Ill. 2017).

212. Fumarolo v. Chicago Bd. of Educ., 566 N.E.2d 1283, 1302 (Ill. 1990).

213. *Compare* 740 ILL. COMP. STAT. 14/10 *with* Employee Retirement Income Security Act of 1974 ("ERISA"), 29 U.S.C. ch. 18 § 1001, *et seq*. (1974) (governing employee benefits and requiring that an employer generally cannot force an employee to receive the "employee benefits plan" documents via

means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment."[214] In looking to the Illinois Wage Payment and Collection Act, the statute specifies that the employer may obtain "written or electronic consent" to disburse an employee's wages via payroll card.[215] In that same statue, the employer cannot deduct funds from an employee's paycheck unless the employer obtains "express written consent of the employee, given freely at the time the deduction is made."[216] Therefore, BIPA may require paper form, as legislators could have easily specified the form, as shown through the Wage Payment and Collection Act .[217]

BIPA does not contain a defined statute of limitations, so BIPA may be subject to different interpretations, based upon other Illinois statutes.[218] For example, if biometric privacy rights fall under the same privacy rights like slander or libel, then the limitation would be one year from the date of the injury or violation.[219] That rationale was applied to the Illinois Right to Privacy Act, which does not have a limitation period, but Illinois courts have interpreted it to have a one-year limitation.[220] On the other hand, BIPA violation could have a three-year limitation if a claim is categorized as a negligence claim considering one of the categories of damages is based upon a "negligent violation."[221] This rationale has merit because BIPA imposes a *reasonable duty of care*, which is the crux of a negligence claim.[222] If neither the one- nor three-year limitation apply, BIPA could also fall under the general five year limitation for civil actions

---

electronic delivery unless the employer meets certain requirements). *See also When Can Employers Use Electronic Delivery of Benefit Plan Documents*, EMP. BENEFITS CORP. (Sep. 21, 2016), www.ebcflex.com/Education/ComplianceBuzz/tabid/1140/ArticleID/377/When-Can-Employers-Use-Electronic-Delivery-of-Benefit-Plan-Documents.aspx; Disclosure, 29 CFR 2520.104b-1 (2002). The employee must have regular access to a computer provided by the employer that is not a central computer or kiosk. *Id*. There is an exception if the employee provides an email to receive electronic notification and completes an electronic consent form. *Id*. Similar to an employee benefits plan, biometric data contains sensitive information important to an individual's livelihood. *Id*. Therefore, in considering how employee benefits plans are regulated, it seems appropriate that consent should be available in both electronic and written format.

214. *Id*.

215. Illinois Wage Payment and Collection Act, 820 ILL. COMP. STAT. 115/14.5(2)(c) (2020) (governing employer's payment of wages to employees and deductions that an employer may take from an employees' paycheck).

216. 820 ILL. COMP. STAT. 115/9 (2020).

217. *Id.*

218. 740 ILL. COMP. STAT. 14/20 (2020).

219. Defamation – Privacy, 735 ILL. COMP. STAT. 5/13-201 (2018).

220. *See* Blair v. Nev. Landing P'ship, 369 Ill. App. 3d 318 (2006) (finding that a violation of the Illinois Right of Publicity Act, 765 Ill. Comp. Stat. 1075/1 had a one-year limitation).

221. 735 ILL. COMP. STAT. 5/13-202 (2020).

222. 740 ILL. COMP. STAT. 14/15 (2020).

because it allows for a private civil right of action against entities that violate BIPA.[223]

There have been many failed attempts to amend BIPA.[224] For example, there was a proposed amendment ("SB3053") in the Illinois senate, which would have limited BIPA by carving out exceptions.[225] Under the proposed exceptions, entities that do not retain biometric data for more than 24 hours would be exempt from BIPA requirements as would entities collecting biometric data for employment purposes.[226] Additionally, SB3053 sought to limit the "biometric identifier[s]" and "biometric information" protected under BIPA, which would exclude facial recognition.[227] However, SB3053 was too limiting, and failed just as similar bills have failed in the past.[228] In supporting an amendment like SB3053, it could be argued that exempting employers from BIPA entities could have promoted employers to implement advanced tracking systems to reduce time theft.

In addition to the statutory ambiguities that Illinois courts have not addressed, there are other provisions in BIPA that may be litigated in future cases, as well. For example, in late 2019, an

---

223. 735 ILL. COMP. STAT. 5/13-205 (2020).

224. Lorenc, et al, *supra* note 40.

225. The Proposed Amendment to 740 ILL. COMP. STAT. 14/25, S.B. 3053, 100th Gen. Assemb. (Ill. 2018), states:

> (f) Nothing in this Act shall be deemed to apply to a private entity collecting, storing, or transmitting biometric information if: (1) the biometric information is used exclusively for: (A) employment, human resources, compliance, identification, or authentication purposes; (B) preventing or investigating acts of terrorism, human trafficking, kidnapping, or violence; or (C) safety, security, or fraud prevention purposes; (2) the private entity does not sell, lease, or trade the biometric identifier or biometric information collected; and (3) the private entity documents a process and time frame to delete any biometric information used for the purposes identified in paragraph (1).

Id.

226. *Id.*

227. Jeffrey Neuburger, *Illinois Considering Amendments to Biometric Privacy Law (BIPA) That Would Create Major Exemptions to Its Scope*, PROSKAUER (Apr. 17, 2018), newmedialaw.proskauer.com/2018/04/17/illinois-considering-amendments-to-biometric-privacy-law-bipa-that-would-create-major-exemptions-to-its-scope/.

228. *See* Amy Korte, *A Proposed Amendment to The Illinois Biometric Information Privacy Act That Would Exclude Facial-Recognition Technology Used By Facebook From The Privacy Protections of The Act Has Been Postponed After Privacy Advocates and The Illinois Attorney General Raised Concerns*, ILL. POL'Y (June 17, 2016), www.illinoispolicy.org/amendment-to-exclude-facebook-facial-recognition-technology-from-illinois-privacy-law-put-on-hold/ (reporting that in 2016, the amendment was put on hold after privacy advocates and the Illinois Attorney General expressed concern regarding the limitations in the bill that would hinder claims against social media giants, like Facebook, for tag suggestions). *See also* Wernick, *supra* note 8 (reporting that SB3053 failed to pass into law).

Illinois federal district court addressed a plaintiff's claim that the defendant failed to have a publicly available disclosure policy as required by BIPA, and the court reviewed conduct that a plaintiff must allege for a BIPA violation to qualify as reckless or intentional intent.[229]

Interestingly, there has not been litigation regarding the BIPA prohibition on selling or profiting from biometric information. BIPA states, "No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."[230] In comparison, other provisions in BIPA allow an entity to take certain actions, so long as the entity obtains consent—among other requirements.[231] However, the profit prohibition does not outline any exceptions that allow an entity to sell information. This is significant because data brokers, who collect and sell personal information, represent a huge industry in the United States.[232] While the brokers' data collection has, historically, not ventured into selling biometric data, it is possible that it could as technology continues to grow, which would in turn implicate BIPA.[233]

There could be a new area of BIPA litigation if employees start suing larger employers that use third parties to process and maintain biometric data. BIPA requires employers to obtain consent from an employee before disclosing a biometric identifier or information to another entity.[234] That regulation does not exempt an employer that discloses the information to the company facilitating the timecards, nor does it exempt the third party from obtaining consent for its use of employees' data.[235] This is exactly what happened in *Dixon*: the employer and third party timekeeping company violated BIPA because the employee never consented to either biometric data collection by the employer or third party.[236] The employee's knowledge that her fingerprint was scanned did not waive the BIPA requirement for consent to later disclose that information.[237] Based on *Dixon*, an employee and its third party

229. Rogers v. CSX Intermodal Terminals, Inc., 409 F. Supp. 3d 612, 617-18 (N.D. Ill. 2019).

230. 740 ILL. COMP. STAT. 14/15(c) (2020).

231. For examples of exceptions, see 740 ILL. COMP. STAT. 14/15(b)(1)-(3) (2020), and 740 ILL. COMP. STAT. 14/15(d)(1)-(4) (2020).

232. Michal Wlosik, *What Is a Data Broker and How Does It Work?*, CLEARCODE, www.clearcode.cc/blog/what-is-data-broker/ (last visited Mar. 16, 2020) (estimating that data brokerage accounts for $200 billion in revenue annually).

233. *See id.* (highlighting that data brokers collect personal information using social media accounts, internet browser history, purchase history, credit card information, and government records).

234. 740 ILL. COMP. STAT. 14/15(d) (2020).

235. *Id.*

236. *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *10.

237. *Id.*

vendor both need independent consent from the employee for the disclosure and the storage.[238]

D. Employer Biometric Data Collection

Biometric timekeeping has become an increasingly popular way to combat employee misconduct and errors, but the payroll savings invites a risk for high damages.[239] For example, a class action BIPA suit was filed against Roundy's Grocery, which employed "more than 10,000 Illinois workers" in 2017.[240] If 100% of those employees joined the class action suit, then Roundy's could be liable for ten million dollars.[241] Alternatively, a company facing a BIPA suit may choose to settle, regardless of liability, to avoid further legal fees. For example, L.A. Tan Enterprises settled for $1.5 million to customers in a lawsuit after the company shared fingerprint scans to an out-of-state vendor.[242] This settlement shows how costly BIPA litigation can be, as the settlement included the $600,000 that it cost the plaintiff class in attorney fees.[243]

Conversely, employers that do not implement better timekeeping risk employees "stealing" time under traditional timekeeping methods.[244] Hourly employees have a responsibility to clock in and out of their shifts and a duty to accurately report.[245] According to American Payroll Association, "buddy clocking"[246] affects 75% of businesses and the average employee steals 4.5 hours through general "time theft."[247] Time theft includes timesheet fraud, rounding up hours, "buddy clocking," unauthorized paid breaks, and not working while clocked in.[248] A recent survey given to hourly employees concluded that 16 percent of the employees

238. *See id.* at *33 (denying the third-party vendor's request to be dismissed from the BIPA suit).

239. Christopher G. Ward, *Using Biometric Timekeeping? Be Aware of Potential Compliance Risks*, FOLER & LARDNER LLP (Oct. 23, 2017), www.foley.com/en/insights/publications/2017/10/using-biometric-timekeeping-be-aware-of-potential.

240. Yerak, *supra* note 32.

241. *Id.*

242. *Id.*

243. Michael J. Bologna, *Biometric Workplace Privacy Suits Erupt in Illinois State Court*, BLOOMBERG L. (Oct. 25, 2017), news.bloomberglaw.com/daily-labor-report/biometric-workplace-privacy-suits-erupt-in-illinois-state-court.

244. Ashik Ahmed, *How To Insure Against Time Theft*, FORBES (Jan. 19, 2018), www.forbes.com/sites/ashikahmed/2018/01/19/how-to-insure-against-time-theft/#55dcc0c15ac8.

245. Ward, *supra* note 239.

246. *Id*. (explaining that Buddy Clocking occurs when an employee signs for another employee such as an employee that clocks-in for their co-worker who is running late).

247. *Id.*

248. *Id.*

admitted to clocking-in for a co-worker.[249] The survey also found the most common error employees made in timesheet submissions was adding an extra 15 minutes.[250] Based on this survey[251] and the estimated 78.2 million hourly workers,[252] U.S. employers lose a total of $373 million annually due to "buddy clocking."[253]

E. Alternative Forms of Relief for Employees

With increasing BIPA litigation, employees may rebel against biometric timekeeping and risk losing their employment when they refuse to relinquish their biometric data. If such an event happens, employees may be able to sue for retaliatory discharge.[254] However, Illinois narrowly interprets the tort of retaliatory discharge.[255] In Illinois, a plaintiff must prove three elements: (1) the employee was discharged; (2) the discharge was in retaliation to the employee's activities; and (3) the discharge "violates a clear mandate of public policy."[256]

The main restriction in a retaliatory discharge claim is that Illinois law has not defined what qualifies as a public policy violation.[257] Instead, the Illinois Courts have articulated that retaliatory discharge "must strike at the heart of a [1] citizen's social rights, [2] duties, and [3] responsibilities before the tort will be allowed," rather than a private grievance.[258] The heart of BIPA protects the privacy rights of citizens.[259] There is no

249. *What Is Buddy Punching And How To Prevent It*, TSHEETS BY QUICKBOOKS, www.tsheets.com/resources/prevent-buddy-punching (last visited Feb. 8, 2020) (describing a data collection by TSheets commissioned PollFish that surveyed 1,000 U.S. Workers that were at least 18 years old).

250. *Id.*

251. *Id.* (declaring that 16% of employees admitted to buddy clocking and the most common error was adding 15 minutes a timesheet).

252. BLS, *supra* note 165 (basing its finding on hourly employees that making an average hourly wage of $22.97).

253. The finding used the following equations: 16% of 78.2 million = 1,251,200 and 25% (15 minutes) of $22.57 (average hourly wage) = $5.74. Then, $5.74 x 1,251,200 workers = $7,185,016 per week. *Id.* Therefore, the annual total is $7,185,016 x 52 weeks = $373,458,176. *Id.*

254. Jacobson v. Knepper & Moga, P.C., 706 N.E.2d 491, 491-92 (Ill. 1998) (holding that employee needed to show that he was discharged in retaliation to his activities and the discharge violated public policy).

255. *Id.* at 492.

256. Blount v. Stroud, 904 N.E.2d 1, 9 (Ill. 2009) (noting that retaliatory discharge was first recognized in 1978 and it is an exception to the rule of an "at-will" employee, who can normally be terminated at any time) (citing Hinthorn v. Roland's of Bloomington, Inc., 529 N.E.2d 909 (1988)).

257. *See* Trochuck v. Patterson Cos., 851 F. Supp. 2d 1147, 1150 (S.D. Ill. 2012) (holding that retaliatory discharge cannot be based on Illinois Wage Payment and Collection Act because the policy reason was too vague).

258. Palmateer v. International Harvester Co., 421 N.E.2d 876, 878-79 (Ill. 1981) (alteration added).

259. 740 ILL. COMP. STAT. 14/5 (2020).

recourse for an individual's whose biologically-unique data has been stolen, whereas there is recourse for victims of credit card or identity theft.[260] Thus, the court's lack of a definition creates an opportunity for Illinois to broaden its interpretation to include privacy rights in one's biometric data.

While Illinois has not defined a "mandated public policy," Illinois courts have narrowly recognized retaliatory discharge as violating public policy in only two circumstances.[261] The first is when an employee asserts a "right to file a workers' compensation claim" pursuant to the Workers' Compensation Act.[262] The second instance includes an employee who is discharged for "whistle blowing,"[263] which refers to reporting an employer's illegal activity to law enforcement.[264] In the vein of whistle blowing, retaliatory discharge has been recognized when an employee refuses to violate a statue such as refusing to commit perjury[265] or reporting to safety violations to a federal administrative agency.[266] In interpreting of a whistleblowing action, the U.S. Seventh Circuit Court of Appeals noted that employers should not force their employees into violating laws, which could subject the employee to liability.[267] While it does not seem like an employee could be subject to liability under BIPA, an employer is effectively trying to get an employee to help the employer evade the law by forgoing the requirements of BIPA.

Some employees have other reasons for withholding their biometric data from employers, which may be subject to protection in alternative causes of action.[268] For instance, a mining worker in West Virginia refused to comply with his employer's fingerprint collection because compliance would violate his religious beliefs by giving him the "mark of the beast."[269] Subsequently, the worker was forced to quit because he refused to comply and his employer would not make accommodations.[270] The trial court found that the worker was discriminated against and constructively discharged.[271]

---

260. *Id.*

261. *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *51.

262. *See* Kelsay v. Motorola, Inc., 384 N.E.2d 353, 357 (Ill. 1978) (holding, as matter of policy, an employer should not have absolute power to terminate an at-will employee).

263. Whistleblower Act, 740 ILL. COMP. STAT. 174/1 (2004).

264. *Id.*

265. *Palmateer*, 421 N.E.2d at 879 (citing Petermann v. Int'l Bhd. of Teamsters, Chauffeurs, Warehousemen & Helpers of Am., Local 396, 174 Cal. App. 2d 184 (Cal. 1959)).

266. Gaffney v. Riverboat Servs., 451 F.3d 424, 447 (7th Cir. 2006).

267. *Id.* at 455.

268. *See* United States EEOC v. Consol Energy, Inc., No. 1:13CV215, 2015 U.S. Dist. LEXIS 1326, at *2-3 (N.D. W. Va. Jan. 7, 2015) (allowing a cause of action under Title VII when an employer required its employees to use hand scanners).

269. *Id.*

270. *Id.* at *3-4.

271. United States EEOC v. Consol Energy Inc., 860 F.3d 131, 137 (4th Cir.

A similar case could easily arise in Illinois, but an employee may have a better chance obtaining relief under the broader federal statute against retaliatory discharge rather than Illinois' narrow interpretation of retaliatory discharge.[272] There could also be relief under a federal statute that protects employee organizations and collective bargaining.[273] If employees collectively combat BIPA, either as a union or non-union group through a "concerted effort,"[274] then they could qualify for protection under 29 U.S.C.S. § 157.[275]

For example, if an employee who refused to use the biometric timekeeping because the employer was violating BIPA, then solicited other employees to join in withholding their biometric data, it could be considered a concerted effort.[276] In that case, if the employer terminates the employees for their collective effort, the group of employees may be afforded protection because the bases for termination could constitute an unfair labor practice.[277] In light of the broad definition of a concerted effort, which has grown with technology, employees could be afforded protection under 29 U.S.C.S. § 157.

2016).

272. *See* Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e *et seq.* (2018) (offering protection to employees who are members of protected classes).

273. 29 U.S.C.S. § 157 (2018), states:

> Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all of such activities except to the extent that such right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 8(a)(3) [29 USCS 158(a)(3)].

Id.

274. An activity is concerted if it arises from prior group activity and an employee acts on behalf of the groups or an employee contacts other employees to join in the effort. Inova Health Sys. v. N.L.R.B., 795 F.3d 68, 74 (D.C. Cir. 2015) (first quoting Tradesmen Int'l, Inc. v. NLRB, 275 F.3d 1137, 1141 (D.C. Cir. 2002), then quoting N.L.R.B. v. Wash. Aluminum Co., 370 U.S. 9, 14 (1962)) (noting that other concerted activities may be protected under the National Labor Relations Act "if they 'relate to legitimate employee concerns about employment-related matters' to 'protect[s] the right of workers to act together to better their working conditions.'").

275. *Wash. Aluminum Co.*, 370 U.S. at 14-15.

276. *Id. ; see also* Three D, LLC v. N.L.R.B., 629 F. App'x 33, 37 (2d Cir. 2015) (highlighting that the definition of concerted has evolved with technology, as an employee's "like" on Facebook qualifies for protection because it seeks to provide support for a group action).

277. *See id.* (holding that the employee's social media activity supported the group action complaining about tax liability due to their workplace. The statements were not made to disparage the employer and the employer discharged employees because of their Facebook activity which violated 29 U.S.C.S. § 157).

F. The Impact of Biometric Data Breaches

The annual increase in identity theft resulting from data breaches demonstrates how insurmountable a data breach of a server housing biometric data could be to individuals.[278] Illinois had the seventh highest per capita rate of identity theft complaints in 2017 out of all the states.[279] Additionally, almost 158 million Social Security numbers and 14.2 million credit card numbers were exposed in the United States in 2017 during data breaches.[280]

A newer scam targets W-2 records from employers through "email phishing."[281] In this scheme, the scammer sends an email to a member of the payroll department from an email address that appears to be that of an existing executive of the company stating that the email is a follow up to a W-2 records request which now asks for a wire transfer.[282] The scam has resulted in thousands of dollars lost.[283] In the same way that the W-2 forms were obtained, cybercriminals could start requesting biometric data from the employer while veiling themselves as the third-party vendor that maintains the employer's biometric data.

There is a myriad of offenses that cybercriminals could commit with biometric data. A criminal could enter a secured building with an employee's biometric credentials.[284] A criminal could expand the use of "deepfake" technology from facial recognition to feign a video of virtual anyone whose data the criminal can obtain.[285] Considering

278. *See 2017 Data Breaches*, IDENTITY THEFT RESOURCE CTR. 1, 3 (Jan. 22, 2018), www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (collecting data breaches annually, reflecting 1,579 breaches in 2017, a 44.7 percent increase from 2016).

279. Matt Tatham, *Identity Theft Statistics*, EXPERIAN (Mar. 15, 2018), www.experian.com/blogs/ask-experian/identity-theft-statistics/ (describing that cybercrimes have increased for all different types of employments and W-2 incident reports increased from 100 in 2016 to 900 in 2017).

280. *Id.*

281. *Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others*, IRS (Feb. 2, 2017), www.irs.gov/newsroom/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others (illustrating a new scam wherein the cybercriminal sends an email to a payroll or human resources personnel as though the email is from an executive, then requests a list of all employees the W-2 forms).

282. *Id.*

283. *Id.*

284. Steve Symanovich, *Biometric Data Breach: Database Exposes Fingerprints, Facial Recognition Data Of 1 Million People*, NORTON, us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html (last visited Jan. 25, 2020).

285. *See* Donie O'Sullivan, *When Seeing Is No Longer Believing - Inside The Pentagon's Race Against Deepfake Videos*, CNN (Jan. 28, 2019), www.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/. A "Deepfake" is the use of artificial intelligence to create "convincing fake audio

that individuals are now able to use their fingerprints to access their cellphones and passwords, a criminal could gain access to an individual's personal messages, photos, and payment methods—such as, bank accounts or credit cards—after accessing the individual's biometric data.[286] Even further, this could impact employers that give employees cellphones for work, if the phone requires biometric data to access it. If the phone and biometric data were obtained, it would grant the criminal access to an employer's sensitive business information.

These data breaches are already happening in the private sector. In early August 2019, outside security researchers discovered that Suprema's internationally-utilized "Biostar 2" security platform was breached.[287] Among other data, the breach notably included the fingerprint data of at least 1 million people.[288] Biostar 2 is utilized in the United States and the company recently announced its integration into a separate security system which is used in 83 countries, by entities including governments and banks.[289] In its worst forms, these types of breaches can lead to cyberwarfare.[290]

In considering the impact on employees and data breaches, it is worth noting that BIPA does not apply to the government's biometric data collection.[291] Despite the common misconception that the government has better data protection mechanisms and resources in place than the average company, hackers stole 5.6 million federal employee fingerprint records in 2015 alone.[292] No federal statute exists that addresses or regulates biometric

---

and video" that make a person "appear to say or do something" that has not actually occurred in reality. *Id*. Typically, videos have been created from public appearances by an individual and used for political purposes. *Id*.

286. *See Are You One Of The Million People Whose Biometric Data Has Been Exposed?,* ENTERPRISE MGMT. 360 (Aug. 15, 2019), www.em360tech.com /continuity/tech-news/opinion-piece/biometric-data/ (among other sensitive information, a team was able to access "personal details, including employee home addresses, emails and start dates" after a data breach).

287. Jon Porter, *Huge Security Flaw Exposes Biometric Data Of More Than A Million Users,* VERGE (Aug. 14. 2019), www.theverge.com /2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data.

288. *Id*.

289. *Id*.

290. *See* Jeff Wichman, *As Attacks On Biometric Data Rise, Risk And Identity-Defined Security Become Paramount*, INFO SECURITY (Sept. 24, 2019), www.infosecurity-magazine.com/opinions/biometric-identity-risk/ (describing "cyber ware" as one of the motives behind targeting biometric data: "For individuals in government, law enforcement and the military, the impact of a breach of this nature could be catastrophic – even life threatening.").

291. 740 ILL. COMP. STAT. 14/15 (2020).

292. *U.S. Government Hack Stole Fingerprints Of 5.6 Million Federal Employees*, THE GUARDIAN (Sep. 23, 2015), www.theguardian.com /technology/2015/sep/23/us-government-hack-stole-fingerprints.

collection.[293] With no federal protection, those 5.6 million employees lack any fundamental recourse.[294] Even if recourse was available, it would probably not apply to government employees, only private employees, as BIPA does not apply to government employers.[295] A federal statute would likely be the only way to protect individuals biometric data from governmental entities.

G. Alternative Employer Approaches to BIPA Suits

Supermarket giant Roundy's attempted to avoid liability for BIPA violations when it argued that it only used "a portion of an employee's finger" rather than an entire fingerprint.[296] Roundy's used Kronos for finger scanning technology to maintain biometric timecards.[297] Roundy's reasoned "[i]t's not possible to construct a biometric identifier such as a fingerprint from the data," so BIPA is not implicated.[298] In response to employee privacy concerns, Kronos claims that it does not store photos of fingerprints, but rather converts a fingerprint into a mathematical equation that cannot recreate the fingerprint.[299] Out-of-state defendants could pursue the argument that subjecting them to BIPA regulations violates the Dormant Commerce Clause because Illinois attempts to unduly burden interstate commerce.[300] Presently, BIPA has potential to burden interstate commerce because the statute does not explicitly state that the data collection must occur within Illinois.

Defendants could challenge class certification rather than challenging standing upon removal to federal court. Plaintiffs bear the burden to prove all four requirements for class certification under Federal Rule of Civil Procedure 23 ("Rule 23").[301] Defendants could spend more resources combating a class certification because the plaintiff has the burden of proof at this stage in litigation.[302]

---

293. Kathi Walker, *Biometric Authentication In The Workplace*, NEW FOCUS HR (July 9, 2018), www.newfocushr.com/2018/07/12/biometric-authentication-workplace/.

294. *U.S. Government Hack Stole Fingerprints of 5.6 Million Federal Employees, supra* note 292.

295. *See* 740 ILL. COMP. STAT. 14/10 (2020). "A [p]rivate entity means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency." *Id*.

296. Yerak, *supra* note 32.

297. *Ease Employees' Privacy Concerns About Kronos Biometric Technology*, KRONOS INC. 1 (2005), www.gc4me.com/information_technology/docs/Fingerscan_privacy_concerns.pdf [hereinafter *Ease Employees' Privacy Concerns*].

298. Yerak, *supra* note 32.

299. *Ease Employees' Privacy Concerns About Kronos Biometric Technology*, *supra* note 297, at 2.

300. *In re Facebook*, 2018 U.S. Dist. LEXIS 81044, at *13.

301. Mazza v. Am. Honda Motor Co., 666 F.3d 581, 588 (9th Cir. 2012).

302. Rule 23 Class Actions, Fed. R. Civ. P. 23(a)(1)-(4) (2018). The Rule

Some BIPA defendants removed the suit to federal court under the Class Action Fairness Act ("CAFA")[303] but ended up back in state court under a granted motion to remand.[304] CAFA does not explicitly state additional jurisdictional requirements must be met to remove a case. However, federal courts have an independent obligation to remand for lack of subject matter jurisdiction.[305] Some district courts have even dismissed CAFA class actions for lack of Article III Standing, but there is a trend to remand rather than dismiss.[306]

Instead of removing a case, defendants could argue that the class cannot be certified under Rule 23 because plaintiffs lack an actual injury, thus failing commonality and typicality.[307] Based on *Spokeo* and the Seventh's Circuit recent decision in *Collier v. SP Plus Corp.*, defendants could cite precedential cases from the forum court that held bare procedural violations did not satisfy an injury.[308] Otherwise, BIPA defendants will be stuck in Illinois state courts if defendants challenge Article III Standing.[309] Additionally, a defendant would save money because a court can award a plaintiff costs and attorney fees if the plaintiff wins its motion to remand

---

states:

> (a) Prerequisites. One or more members of a class may sue or be sued as representative parties on behalf of all members only if: (1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class.

Id.

303. 28 U.S.C. § 1332(d)(2)(A) (2011) (granting federal district courts "original jurisdiction of any civil action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which . . . [a]ny member of a class of plaintiffs is a citizen of a State different from any defendant.").

304. Barnes v. Aryzta, LLC*,* 288 F. Supp. 3d 834, 836 (N.D. Ill. Dec. 20, 2017).

305. *Id.*

306. Matthew Mall, *District Court: CAFA Class Actions Lacking Article III Standing Must Be Remanded to State Court, Not Dismissed*, AM. BAR ASS'N (Oct. 27, 2016), www.americanbar.org/groups/litigation/committees/class-actions/practice/2016/cafa-class-actions-lacking-article-iii-standing-must-be-remanded-to-state-court/.

307. John E. Goodman, *The Standing Trap: Will a Spokeo Challenge Lock a Class Action Defendant into a State Court Forum?*, BRADLEY ARANT BOULT CUMMINGS LLP (May 29, 2018), www.classactiondeclassified.com /2018/05/standing-trap-will-spokeo-challenge-lock-class-action-defendant-state-court-forum/.

308. *Collier*, 889 F.3d at 895 (holding that the suit should have been remanded rather than dismissed due to plaintiff's lack of standing by only showing a bare statutory violation).

309. Mall, *supra* note 306.

after the defendant removed the case.[310]

IV. PROPOSAL

This proposal addresses various steps that could be taken in state and federal legislatures, federal courts, and among employers. As BIPA surpasses its tenth anniversary, it should continue to remain in full force without diminishing any of its protections by adopting legislative amendments. Illinois enacted BIPA at a time where the progression of biometric data collection and technological protections were unknown.[311] The legislature even emphasized, "[t]he full ramifications of biometric technology are not fully known" when it enacted BIPA.[312] There have been extensive technological changes in the last decade; annual smartphones sales exploded from $139 million in 2008 to $1.4 billion in 2016, and Facebook users grew from 100 million in 2008 to 1.79 billion in 2016.[313] In 2008, there were no iPads, GPS on smart phones,[314] ride-sharing apps,[315] mobile payment services,[316] 4G networks, dating applications, or music streaming applications.[317] These products have become daily essentials for many Americans and technology continues to grow. Alongside these technological advancements, there have been extensive data breaches in both the private and public sector.[318] The

310. Mocek v. Allsaints USA Ltd., 220 F. Supp. 3d 910, 914 (N.D. Ill. Dec. 7, 2016); § 1447(c).

311. 740 ILL. COMP. STAT. 14/5(d)-(f) (2020) (outlining that the legislature's intent for enacting BIPA was "an overwhelming majority of members of the public are weary of the use of biometrics" and"[t]he full ramifications of biometric technology are not fully known").

312. 740 ILL. COMP. STAT. 14/5(f) (2020).

313. Jefferson Graham, *5 Top Ways Tech Has Changed Since 2008*, USA TODAY (Nov. 13, 2016), www.usatoday.com/story/tech/2016/11/13/5-top-ways-tech-has-changed-since-2008/93527624/.

314. Avery Hartmans, *These 18 Incredible Products Didn't Exist 10 Years Ago*, BUS. INSIDER (Aug. 23, 2018), www.businessinsider.com/18-tech-products-that-didnt-exist-10-years-ago-2017-7 (providing an example that GPS was invented in 1978 and available for commercial use in 1993 but it was not available on cellphones until Apple introduced it in 2008).

315. Isobel Asher Hamilton, *Uber's Biggest Rival Has Raised New Funding And Doubled In Valuation To $15 billion*, BUS. INSIDER (June 28, 2018), www.businessinsider.com/lyft-doubled-valuation-15-billion-2018-6 (depicting that Lyft launched in 2012, currently valued at $15.1 billion, and provided 375 million trips to passengers in 2017 meanwhile Uber launched in 2009, currently valued at $62 billion and provided $4 billion trips in 2017).

316. Emmett Higdon, *Mobile Online Retail Payments 2016*, JAVELIN STRATEGY & RES. (Oct. 6, 2016), www.javelinstrategy.com/coverage-area/mobile-online-retail-payments-2016 (finding that mobile retail payments in the U.S. grew 60% from 2014 to 2015 ($180 billion) and are expected to reach $320 billion by 2020).

317. Hartmans, *supra* note 314.

318. Porter, *supra* note 287; *U.S. Government Hack Stole Fingerprints Of 5.6 Million Federal Employees, supra* note 292.

full ramifications of technology continue to remain unknown, which is why protections like BIPA are imperative.

As it relates to the statute itself, any amendment that seeks to limit BIPA should be rejected. Illinois should adopt a three-year statute of limitations for BIPA injuries in line with a negligence claim as the standard of care seems to boil down to "reasonable care." Employers should be required to disclose their intention to collect data at the time the employer hires the employee in a separate disclosure form rather than a clause embedded in an employment agreement. Currently, BIPA does not define how the written release is administered.[319] The intent behind BIPA is similar to an employer-sponsored employee benefits plan, which also seeks to protect sensitive data.[320] If BIPA followed the same rationale as the Illinois wage statute, then employers should not be able force employees into using their biometric data for timekeeping, especially considering the employee is not receiving any benefit. An employer cannot force employees to receive their paychecks electronically via direct deposit.[321]

The doctrine of unconscionability under Illinois law should apply to the consent requirement under BIPA.[322] For example, the consent provision should be easily viewable and understandable under the circumstances at the time the document is signed.[323] If the provision is unconscionable, then it is unenforceable and a BIPA violation would arise because consent is lacking. Adding the layer of unconscionability would prompt the employer to be clear in its disclosure.

While employers may not initially collect biometric data for commercial purposes, agreeing to employment is different than choosing a product, which collects biometric data. Further, data breaches continue to become more prevalent among private companies.[324] "A person cannot obtain new DNA or new fingerprints or new eyeballs for iris recognition . . . Replacing a biometric identifier is not like replacing a lost key or a misplaced identification card or a stolen access code."[325] Employees generally do not have much bargaining power against an employer who wants to collect their data. Employees should not have to choose between earning a living and giving up their privacy rights. Further, employers need more education on BIPA and its impact, which the

319. 740 ILL. COMP. STAT. 14/10 (2020).

320. 29 U.S.C. CH. 18 § 1001, *et seq*. (2019) (noting that an employer cannot force an employee to receive the "employee benefits plan" documents via electronic delivery unless the employee meets certain requirements).

321. 820 ILL. COMP. STAT. 115/1 (2020).

322. Cognitest Corp. v. Riverside Publ'g Co., 107 F.3d 493, 499 (7th Cir. 1997).

323. We Care Hair Dev., Inc. v. Engen, 180 F.3d 838, 843 (7th Cir. 1999).

324. Porter, *supra* note 287.

325. Sekura v. Krishna Schaumburg Tan, Inc., 115 N.E.3d 1080, 1093, *appeal denied*, 119 N.E.3d 1034 (Ill. App. 1st 2019).

Department of Labor should assist in implementing.

If the U.S. Supreme Court weighs in on the issue of Article III Standing under BIPA, it would promote uniformity among the circuits and deter forum shopping. The Supreme Court should find that a technical violation is actionable due to the sensitive nature of the data and potential of evolving technology, which can diminish a person's privacy rights. Disclosing biometric data without prior consent to a third party should always qualify as a concrete injury and even allow for higher damages.[326] There must be safeguards to protect sensitive data, which becomes more vulnerable as technology progresses. Biometric privacy acts could affect interstate commerce, if states continue to enact similar statues and those states have different requirements. If the Supreme Court weighed in on standing, it would allow other states to move forward with enacting similar biometric privacy acts and harmonize varying state interpretations. Although, this would not solve biometric privacy issues and pitfalls, it would solidify the recognition of this type of injury.

Congress could also enact a similar federal statute to regulate biometric data collection, but it should not preempt state law. Instead, it should establish a minimal baseline. It could be a matter of national security if cybercriminals obtain a citizens' DNA data. Other states are planning to enact biometric privacy statutes, so Congress may eventually need to take action to ensure uniformity, especially because technology often crosses state lines.[327] Any statute that Congress enacts should include recourse in the event that the entity violates a technical provision, such as notice and consent, and allow a private right of action.

Other states should continue to enact biometric privacy statutes. Like BIPA, those statutes must include a private right of action. Biometric data privacy should be a nationally recognized privacy right, similar to common law privacy claims that have been long-held actionable by the courts.[328]

V. CONCLUSION

The growth of technology is inevitable – state and federal levels of government should grow with it by protecting individuals' privacy rights, especially employees. Data breaches threaten national security far beyond the borders of a state, as seen in recent years.[329]

---

326. *See e.g.*, *Dixon*, 2018 U.S. Dist. LEXIS 90344, at *39 (employer physically shipped hard drives with biometric data to its third-party vendor of timecards without any protection).

327. *See e.g., In re Facebook,* 2018 U.S. Dist. LEXIS 81044, at *12 (where Facebook was sued by Illinois citizens for its use of facial recognition).

328. *Patel*, 932 F.3d at 1273; *Eichenberger*, 876 F.3d at 983.

329. *See U.S. Government Hack Stole Fingerprints Of 5.6 Million Federal Employees*, *supra* note 292 (revealing international hackers stole 5.6 million

The recognition of data privacy rights requires accountability at different government levels and among employers to ensure safety for all employees. Employers need to be held accountable for protecting their employees' data, so they should not be treated differently under a non-commercial entity exception.

BIPA remains the gold standard in the United States for biometric data collection, despite the efforts to erode its protections. Other states should continue to enact similar statutes and grant individuals the private right to protect and adjudicate offenses against their data. The Illinois legislature's intent holds true: "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[330] This urgency only continues to grow as technology advances; the recognition and protection of data privacy rights must growth with it.

federal employee fingerprint records in 2015). *See also* Tatham, *supra* note 279 (estimating that 158 million Social Security numbers and 14 million credit card numbers were exposed in the United States in 2017 during data breaches).

330. 740 ILL. COMP. STAT. 14/5(g) (2020).