UIC Law Review

Volume 57 | Issue 2 Article 5

2024

Illinois BIPA: A Litigation Nightmare for Employers

Andrew Cook

ILLINOIS BIPA: A LITIGATION NIGHTMARE FOR EMPLOYERS

ANDREW COOK*

* Andrew James Cook, Juris Doctor Candidate at the University of Illinois Chicago School of Law. At the forefront, I would like to thank my family, my fiancé Rachel, and her family for their constant love and support throughout my law school journey. I would also like to thank my dearest friends Matt, Muj, Jacob, Brad, Dom, Adam, Robert, and Alexis for giving me constant encouragement and many laughs throughout law school. Lastly, I'd like to thank my mentor and best friend, Patrick Oriedo, who has taught me what it means to be a caring, zealous, and impactful advocate.

I. INTRODUCTION

Biometrics is the measurement and statistical analysis of a person's physical characteristics.[1] These physical characteristics are facial, fingerprint, retina, and iris recognition, called "biometric identifiers."[2] Passwords or social security numbers can be easy to forget and easily guessed or obtained through phishing attacks. At the same time, biometrics are unique to the person, making it extremely difficult to replicate or steal.[3]

The surge in biometric use is a result of advancements in technology.[4] The National Security Agency formed the Biometric Consortium in 1992, which developed numerous working groups to expand the development of biometric technology.[5] In the 2000s, research and development led to substantial innovations in facial recognition, hand geometry, iris recognition, and fingerprint recognition.[6] A study done in 2017 found that fifty-seven percent of companies use biometrics for identity authentication, and another study in 2020 found that eighty percent of active phones in North America were incorporated with biometric authentication systems.[7]

Many states have started implementing biometric privacy laws to protect against the unauthorized use of biometrics.[8] On October 3, 2008, Illinois became the first state to implement a biometrics law.[9] In passing the Biometric Information Privacy Act (BIPA), the Illinois General Assembly found that "[t]he public

---

1. Alexander Gillis et al., *biometrics*, TECHTARGET (July 2021), www.techtarget.com/searchsecurity/definition/biometrics [perma.cc/V9VD-P4AG].

2. *Id.*

3. *Id.*

4. Stephen Mayhew, *History of Biometrics*, BIOMETRICUPDATE.COM (Feb. 1, 2018), www.biometricupdate.com/201802/history-of-biometrics-2 [perma.cc/64SR-4L7L] (explaining that people have used biometrics throughout the history of civilization, such as handprints on caves created by prehistoric men).

5. *Id.*

6. *Id.*

7. *Moving Forward with Cybersecurity and Privacy*, PWC (Oct. 5, 2016), www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf [perma.cc/7BKY-NN7Q]; Justina Alexandra Sava, *Biometric Technologies – Statistics & Facts*, STATISTA (Feb. 17, 2022), www.statista.com/topics/4989/biometric-technologies/#topicOverview [perma.cc/G3KR-YQL7].

8. *Is Biometric Information Protected by Privacy Laws?*, BLOOMBERG L., pro.bloomberglaw.com/brief/biometric-data-privacy-laws/ [perma.cc/RZX4-TVFY] (last visited Feb. 17, 2023) (explaining that Illinois, Texas, and Washington have biometric privacy laws in effect). Additionally, California, Connecticut, Colorado, Utah, and Virginia have passed comprehensive consumer privacy laws that once in effect, will govern the processing of biometric information and other states have enacted data breach notification laws that include biometric data within their scope. *Id.*

9. 740 ILL. COMP. STAT. 14/99 (2008).

welfare, security, and safety will be served by regulating the collection . . . of biometric identifiers."[10] Shortly after, Texas followed suit by enacting the Capture or Use of Biometric Identifiers Act (CUBI).[11]

Employers are suffering detrimental effects from the implementation of BIPA despite the Illinois legislature's good intentions. This comment offers suggestions to make BIPA effective without causing an undue burden on employers. The background in section II discusses how people and businesses use biometrics and discusses the existing biometric laws in Illinois and Texas. The analysis section will compare BIPA's private right of action and CUBI's Attorney General's right of action. It will discuss what it means to be an "aggrieved" person to bring a suit under BIPA, how the federal courts have interpreted BIPA, and strategies plaintiffs use to collect massive damage awards under BIPA. Finally, the proposal suggests that Illinois should eliminate its private right of action and vest the attorney general with the sole discretion to bring a claim under BIPA. It also suggests that the Illinois courts should only allow standing for violations that cause actual harm. Additionally, Illinois should implement a safe harbor provision to protect entities acting in good faith where the entity's violation results in no actual harm to the plaintiff.

II. BACKGROUND

The use of biometric data for security purposes is growing exponentially.[12] Biometrics are used today for identity authentication, mobile access, banking, and business purposes.[13] People use biometric information because it is reliable, secure, and convenient. Companies use biometric technology to enhance security, prevent fraud, improve efficiency, and protect sensitive data.[14] States have implemented laws regulating the use and

10. 740 ILL. COMP. STAT. 14/5(g) (2008).

11. David Oberly, *Beyond BIPA: Mitigating Biometric Data Legal Risks Under Texas and Washington Biometrics Laws*, BIOMETRICUPDATE (Aug. 24, 2022), www.biometricupdate.com/202208/beyond-bipa-mitigating-biometric-data-legal-risks-under-texas-and-washington-biometrics-laws [perma.cc/YG4W-5Y35].

12. *See What is Biometrics? How is it Used in Security?*, KAPERSKY, www.kaspersky.com/resource-center/definitions/biometrics [perma.cc/5HDU-LVW2] (last visited Oct. 8, 2022) (discussing how biometrics are being used for banks, e-passports, phone security systems, and international traveling).

13. *The Top 9 Common Uses of Biometrics in Everyday Life*, NIPPON ELEC. CO. (July 7, 2020), www.nec.co.nz/market-leadership/publications-media/the-top-9-common-uses-of-biometrics-in-everyday-life/ [perma.cc/FU4E-VMC7].

14. Dave Zielinski, *Use of Biometric Data Grows, Though Not Without Legal* Risks, SHRM (Aug. 23, 2018), www.shrm.org/ResourcesAndTools/hr-topics/technology/Pages/biometric-technologies-grow-.aspx [perma.cc/94KM-KCS3].

collection of biometric data.[15] Illinois and Texas were the first to enforce biometric laws.[16]

A. How People Use Biometric Data and the Risks Involved

People use biometric data in a variety of ways. The two most common uses are smartphone security and banking.[17] Major tech companies such as Apple and LG provide biometric scanners on their smartphones, which allow users to scan their faces and fingerprints as a security measure to unlock their phones.[18] Banks such as Wells Fargo enable individuals to access their financial accounts electronically through facial and fingerprint recognition.[19] Biometric systems allow users to unlock their phone or bank account in seconds by placing their finger on a scanner.[20]

People use biometric data because it is reliable, secure, and convenient. Biometrics are reliable because they are unique and highly accurate.[21] No two persons can have the same biometrics.[22] An adult's biometrics, such as fingerprints, voice, retinal patterns, facial recognition, and hand patterns, remain consistent over time.[23] Biometrics allows a person to be identified and authenticated based on recognizable, verifiable, unique, and specific data.[24]

---

15. Oberly, *supra* note 11.

16. *Id*.

17. Robert Smith, *25 Uses of Biometrics in Today's Society*, BIOMETRIC TODAY, biometrictoday.com/uses-of-biometric-technology-today-society/ [perma.cc/R2C9-PJEH] (last visited Oct. 12, 2023).

18. *What is Biometrics? How is it Used in Security?*, *supra* note 12.

19. *See Biometric Authentication*, WELLS FARGO, www.wellsfargo.com/online-banking/biometric/ [perma.cc/CM2L-5S4X] (last visited Oct. 8, 2022) (providing users a downloadable app on their smartphone that allows users to use biometric features such as fingerprint and facial recognition, instead of a username and password, to sign on to the app).

20. *See* Jessica Goopman, *In Biometrics, Security Concerns Span Technical, Legal and Ethical*, TECHTARGET (Jun. 15, 2020), www.techtarget.com/searchsecurity/tip/In-biometrics-security-concerns-span-technical-legal-and-ethical https://www.techtarget.com/searchsecurity/tip/In-biometrics-security-concerns-span-technical-legal-and-ethical [perma.cc/LNB6-8WMS].

21. Keyede Erinfolami, *What Are Biometrics and How Do They Work?*, MAKEUSEOF (Oct. 19, 2021), www.makeuseof.com/what-are-biometrics-how-do-they-work/ [perma.cc/7XFD-SSXA]; Andrew Zarkowsky, *Biometrics: An Evolving Industry With Unique Risks*, HARTFORD (May 20, 2021), www.thehartford.com/insights/technology/biometrics [perma.cc/8MSR-BJHF].

22. *See* Erinfolami, *supra* note 21 (explaining that even biological twins have their own unique biometric different from each other).

23. *Id.*

24. *Biometrics: Definition, Use Cases, Latest* News, THALES (MAY 20, 2023), www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics [perma.cc/73KC-63FJ].

People use biometric data because it is secure. Unlike passwords and PINs, which hackers can easily compromise during a data breach, biometrics are difficult to crack due to the vast amount of unique variations.[25] According to Apple, the probability that two different fingerprints register as a match for Touch ID is 1 in 50,000.[26] In contrast, the odds of guessing a typical 4-digit passcode is 1 in 10,000.[27] Biometric Identifiers are so unique and complex that hackers need advanced tools and distinct data to replicate them.[28] For example, a hacker would have to first hack into a database where fingerprints are stored and then create a synthetic fingerprint or a mold of the fingerprint, which is both time-consuming and difficult.[29]

Additionally, people use biometric data because it is convenient. No memorization is required to use biometrics, biometric systems provide quicker authentication than traditional methods, and the systems are easy to use.[30] Unlike traditional security systems that require users to remember passwords or PINS, biometric systems work with the user's unique physical traits such as fingerprints, palm veins, retina, etc.[31] Individuals do not have to memorize or carry around lengthy passwords when using biometric systems.[32] Biometric systems provide quicker authentication compared to traditional methods.[33] A fingerprint scan or facial recognition can grant access almost instantly.[34] Furthermore, biometric systems are generally user-friendly and easy to use.[35] They can be as simple as taking a selfie, speaking into a microphone, or placing a finger on a scanner.[36]

---

25. *Id*.

26. *About Touch ID Advanced Security Technology*, APPLE (Sep. 11, 2017), www.support.apple.com/en-us/HT204587 [perma.cc/UPZ4-TUJR].

27. *Id.*

28. Mark Smith et al., *Biometric Data Risks: Keep Eyes on Coverage Gaps*, CRC GROUP (Sep. 17, 2020), www.crcgroup.com/Tools-Intel/post/biometric-data-risks-keep-eyes-on-coverage-gaps [perma.cc/9L5H-WKBN].

29. Ryan Toohil, *Fingerprint Identity Theft: How To Keep Your Devices Secure*, AURA (Dec. 19, 2022), www.aura.com/learn/fingerprint-identity-theft. [perma.cc/QEH3-ME6U].

30. Robert Smith, *10 Advantages and Disadvantages of Biometrics System You Should Know*, BIOMETRIC TODAY, biometrictoday.com/10-advantages-disadvantages-biometrics-technology/ [perma.cc/F3NL-TSCK] (last visited Oct. 12, 2023).

31. *Id.*

32. *Id.*

33. *Id.*

34. Stanley Goodner, *What Are Finger Scanners and How Do They Work?*, LIFEWIRE (Aug. 29, 2021), www.lifewire.com/understanding-finger-scanners-4150464 [perma.cc/J5TN-XGHN].

35. Smith, *supra* note 30.

36. *Id.*

B. How Businesses Use Biometric Systems

Companies use biometric technology to enhance security, prevent fraud, improve efficiency, and protect sensitive data.[37] Companies use biometric technologies to provide a more secure way to authenticate employee identity for timekeeping, granting access to sensitive data, and facilitating onboarding and offboarding.[38] Most Information Technology ("IT") and human resource ("HR") information system professionals believe that biometrics are more secure than traditional forms of authentication, such as text-based passwords or personal identification numbers.[39]

Biometric technology helps to prevent fraud.[40] Biometric time clocks that use fingerprint scanning or facial recognition help HR better comply with labor laws by ensuring employees clock in and out accurately and by leaving well-documented audit trails.[41] This practice prevents "buddy punching," in which workers clock in for colleagues who are not present.[42]

Biometric technology improves workplace efficiency.[43] Companies are turning to biometric single sign-on approaches over traditional usernames and passwords.[44] With single sign-on, employees who frequently log into multiple databases can avoid using different passwords to access each system, adding efficiency and enhanced security protection.[45]

Finally, companies use biometric technology to protect sensitive data.[46] The use of default, weak, or even nonexistent passwords is rampant.[47] Biometrics offers a solution to this problem by providing a more secure form of authentication.[48] This protects an employer's sensitive work information from being compromised.[49]

---

37. Zielinski, *supra* note 14.
38. *Id.*
39. *Id.*
40. *5 Ways Biometrics Help Fight Fraud,* IDR&D (Nov. 14, 2021), www.idrnd.ai/5-ways-biometrics-help-fight-fraud/ [perma.cc/893F-N3WR].
41. Zielinski, *supra* note 14.
42. Roy Maurer, *More Employers Are Using Biometric* Authentication, Shrm (Apr. 6, 2018), www.shrm.org/ResourcesAndTools/hr-topics/technology/Pages/Employers-Using-Biometric-Authentication.aspx [perma.cc/54YC-2K4U] (last visited Oct. 31, 2023).
43. Zielinski, *supra* note 14.
44. *Id.*
45. *Id.*
46. Zarkowsky, *supra* note 21.
47. Maurer, *supra* note 42.
48. *Id.*
49. *Id.*

C. State Biometric Laws

On October 3, 2008, Illinois signed the Biometric Information Privacy Act ("BIPA") into law, reasoning that regulating biometric data would serve public welfare, security, and safety.[50] Texas enacted the Capture or Use of Biometric Identifier Act ("CUBI") the following year.[51] As of 2023, Illinois, Texas, and Washington are the only states with enacted biometric privacy legislation.[52] This section will discuss the Illinois and Texas biometric laws.

1. Illinois Biometric Information Privacy Act

Illinois BIPA provides biometric information retention, collection, disclosure, and destruction requirements.[53] Sections a, b, c, d, and e—comprise the retention, collection, disclosure, and destruction sections.[54]

Section (a) establishes that a private entity possessing biometric information must make a written policy available to the public, establishing a retention schedule and destruction guidelines.[55] A private entity must destroy the biometric information once the initial purpose for the collection has been satisfied or within three years, whichever is first.[56]

Section (b) asserts that before a private entity collects, purchases, or obtains biometric data, it must first inform the individual in writing that it is collecting a biometric identifier, list the purpose and length of time the information will be collected, stored, and used, and obtain a signed written release.[57]

Section (c) prohibits private entities from selling, leasing, trading, or profiting from biometric identifiers or information.[58]

Section (d) proscribes the disclosure or dissemination of biometric identifiers or information unless the individual consents, the disclosure completes a financial transaction authorized by the

50. 740 ILL. COMP. STAT. 14/1 – 5 (2008).

51. Molly DiRago, *The Litigation Landscape of Illinois' Biometric Information Privacy Act*, AMERICAN BAR ASS'N (Aug. 20, 2021) www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/the-litigation-landscape/ [perma.cc/D8RU-U6FF].

52. *2023 State Biometric Privacy Law Tracker*, HUSCH BLACKWELL LLP (Feb. 13, 2023), www.huschblackwell.com/2023-state-biometric-privacy-law-tracker [perma.cc/KZM9-GDUM] (listing Arizona, Minnesota, Missouri, Tennessee, Kentucky, New York, Massachusetts, Vermont, and Maryland as states with active biometric privacy law legislation, and Illinois, Texas, and Washington as states with enacted biometric privacy law legislation).

53. 740 ILL. COMP. STAT. 14/15 (2008).

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

individual, or a law or court order requires disclosure.[59]

Furthermore, section (e) requires a private entity possessing biometric information to use a reasonable standard of care when storing the data and to store the information in the same or more protective manner than it stores other confidential information.[60]

A person "aggrieved" by a violation of the statute has a private right of action in state court or federal court if jurisdictional requirements are satisfied.[61] A person aggrieved by a violation of the act may recover liquidated damages of $1000 or actual damages when a private entity negligently violates a provision of the act.[62] The act also provides for recovery of liquidated damages of $5,000 or actual damages against a private entity that intentionally or recklessly violates a provision of the act.[63]

2. Texas Capture or Use of Biometric Identifier Act

In 2009, Texas enacted the Capture or Use of Biometric Identifier Act (CUBI), which regulates the collection and use of biometric information.[64] The act prohibits a person from capturing a biometric identifier for a "commercial purpose" unless the person informs the individual and receives consent to capture the biometric identifier.[65]

A person possessing a biometric identifier captured for commercial purposes may not sell, lease, or disclose a person's biometric identifier unless the individual consents, the disclosure completes a financial transaction authorized by the individual, or a law or court order requires disclosure.[66] The biometric identifier captured for a commercial purpose must be stored and transmitted using reasonable care and in the same manner the person stores other confidential information to protect disclosures.[67] The person must destroy the biometric identifier no later than a year after the

---

59. Daniel A. Cotter, *The Illinois Biometric Information Privacy Act: Emerging Insurance Issues*, HOWARD & HOWARD ATTYS. PLLC (Apr. 4, 2021) www.howardandhoward.com/media/pdf/The%20Illinois%20Biometric%20Information%20Privacy%20Act%20Emerging%20Insurance%20Issues.pdf [perma.cc/5QK2-8TXA].

60. *Id*.

61. *See* 740 ILL. COMP. STAT. 14/20 (2008). *See generally Subject Matter Jurisdiction*, CORNELL L. SCH., www.law.cornell.edu/wex/subject_matter_jurisdiction [perma.cc/46DG-MN9G] (last visited Dec. 18, 2023) (explaining diversity and supplemental jurisdiction).

62. *Id*.

63. *Id*.

64. Chad J. Layton & Peter J. Strelitz, *CUBI: Everything You Need to Know About Texas' Biometric Law and Beyond…*, SEGAL MCCAMBRIDGE (Jan. 28, 2021), www.segalmccambridge.com/blog/cubi-everything-you-need-to-know-about-texas-biometric-law-and-beyond/ [perma.cc/BBE9-XKU8].

65. TEX. BUS. & COM. CODE § 503.001 (2017).

66. *Id*.

67. *Id*.

first collection of the data.[68]

A person who violates the statute is subject to a civil penalty of no more than $25,000 for each violation.[69] Unlike Illinois, CUBI only allows the Texas Attorney General to bring an action to recover the civil penalty for a violation.[70] Until February 2022, there has been little to no enforcement of the statute's provisions.[71]

III. ANALYSIS

The analysis section will compare BIPA's private right of action and CUBI's Attorney General's right of action. Then, it will discuss what it means to be an "aggrieved" person to bring a suit under BIPA and address how the federal courts have interpreted BIPA. Finally, the analysis will address plaintiffs' strategies to collect massive damage awards under BIPA.

A. Private Right of Action vs. Attorney General Right of Action

One critical difference between Illinois BIPA and the Texas biometrics statute is that Illinois BIPA allows individuals a private right of action when a private entity violates the Statute.[72] Texas CUBI only allows the Attorney General to bring suit under the statute.[73]

Under Illinois BIPA, a person "aggrieved" by a violation of the statute has a private right of action in state court or as a supplemental claim in federal court.[74] A private right of action means anyone who believes a person violated their rights under the statute can take legal action and file suit against the alleged violator to seek redress for the alleged harm.[75]

---

68. *Id*.

69. Bart Huffman & Haylie D. Treas, *Texas Enforcement of Biometric Law Focuses on Artificial Intelligence*, HOLLAND & KNIGHT (Nov. 14, 2022), www.hklaw.com/en/insights/publications/2022/11/texas-enforcement-of-biometric-law-focuses-on-artificial-intelligence [perma.cc/B9GT-SQN9].

70. TEX. BUS. & COM. CODE § 503.001 (2017).

71. Mackenzie Wallace et al., *Texas Sues Meta for Alleged Violations of Texas Biometric Law*, THOMPSON COBURN LLP (Feb. 25, 2022), www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2022-02-25/texas-sues-meta-for-alleged-violations-of-texas-biometric-law [perma.cc/2P8Z-MPAU] ("[I]t remains to be seen how aggressively the Texas Attorney General will use CUBI's provisions to penalize private businesses.").

72. 740 ILL. COMP. STAT. 14/20 (2008).

73. TEX. BUS. & COM. CODE § 503.001 (2017).

74. 740 ILL. COMP. STAT. 14/20 (2008).

75. Dmitry Shifrin et al., *Past Present and Future: What's Happening With Illinois' and Other Biometric Privacy Laws*, NAT'L L. REV. (Aug. 10, 2021), www.natlawreview.com/article/past-present-and-future-what-s-happening-illinois-and-other-biometric-privacy-laws-0 [perma.cc/4SSP-3M5X].

In contrast, under the Texas biometric law, only the Attorney General can file a claim against an alleged violator.[76] In Texas, the Attorney General ("AG") identifies violations of CUBI through investigations, referrals by other state agencies, and public reports.[77] After investigation, once the AG identifies a violation, the AG can file a lawsuit against the violating party.[78] In the lawsuit, the AG can seek damages for the alleged violations and an injunction to stop the violating party from continuing to collect information in Texas and to delete any collected information.[79]

B. What is an Aggrieved Person to Bring Suit in Illinois State Courts?

Under Illinois BIPA, A person "aggrieved" by a violation of the act may recover liquidated damages of $1000 or actual damages when a private entity negligently violates a provision.[80] The Illinois Supreme Court's decision in *Rosenbach v. Six Flags Entm't Corp.* explained what it means to be an "aggrieved" person to bring a lawsuit under the statute. [81]

In this case, a mother filed a lawsuit against Six Flags, alleging that it violated BIPA's requirements when Six Flags took her son's fingerprint as part of his purchase of a season pass to its amusement park.[82] She claimed that Six Flags did not inform her or her son of the specific purpose and length of term for which his fingerprint had been collected.[83] She also claimed that neither of them signed any written release regarding the taking of the fingerprint, and neither consented to the collection or use of that biometric information.[84] In response, Six Flags filed a motion to dismiss, arguing that the plaintiff had no actual or threatened injury and, therefore, lacked standing to sue and that the plaintiff's complaint failed to state a

76. TEX. BUS. & COM. CODE § 503.001 (2017).

77. *Id.*; *see* Huffman & Treas, *supra* note 69; *What the Attorney General Can Do for You*, ATT'Y GEN. OF TEX., www2.texasattorneygeneral.gov/agency/what-the-attorney-general-can-do-for-you [perma.cc/9EXX-2QWN] (last visited Oct. 13, 2023); *File a Consumer Complaint*, ATT'Y GEN. OF TEX., www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint. [perma.cc/HL5X-9ZNP] (last visited Oct. 13, 2023).

78. F. Mario Trujillo & Jon Frankel, *Texas Starts Enforcing Its Biometric Law*, ZWILLGENBLOG (Feb. 18, 2022), www.zwillgen.com/privacy/texas-cubi-law-and-biometric-privacy/ [perma.cc/D9V2-4FM8].

79. *Id.*

80. *Id.*

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

82. *Id.* at 1200-01.

83. *Id.*

84. Tae Kim, *Rosenbach v. Six Flags: Illinois Supreme Court Interprets Illinois Biometric Privacy Law*, JOLT DIGEST (Feb. 18, 2019), www.jolt.law.harvard.edu/digest/rosenbach-v-six-flags-illinois-supreme-court-interprets-illinois-biometric-privacy-law [perma.cc/G7DR-QU8B].

cause of action for violation of the Act.[85]

The central issue the court addressed was whether an individual qualifies as an "aggrieved" person and may seek liquidated damages and injunctive relief under BIPA if he or she has not alleged some actual injury or adverse effect beyond a violation of his or her rights under the statute.[86] On review, the Illinois Supreme Court relied on the settled legal meaning of the term aggrieved: "[a] person is prejudiced or aggrieved in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment."[87]

The court found that BIPA conferred upon individuals a right to privacy and control over their biometric information.[88] Thus, the court determined that a person is "aggrieved" within the meaning of BIPA and entitled to seek recovery when a private entity fails to comply with the statute requirements.[89] The court reasoned that the violation impairs or denies the statutory rights of any person whose biometric information is subject to the breach.[90] The court made this finding irrespective of whether the biometric data had been improperly shared or misused.[91]

In other words, the court held that an individual does not need to allege some actual injury or adverse effect beyond the violation of his or her rights under BIPA to qualify as an "aggrieved" person and be entitled to bring a private action under the Act.[92] Therefore, the standing doctrine in Illinois allows an "aggrieved" person to bring suit under BIPA in Illinois State Courts.[93]

C. Federal Court Standing and BIPA

Most plaintiffs bring BIPA claims in Illinois state court.[94]

85. Donald Patrick Eckler & Calvin A. Townsend II, *I'm Still Standing? Development of Standing Doctrine in Illinois Consumer Protection Class Actions*, ILL. ASS'N OF DEFENSE TRIAL COUNS., www.pretzel-stouffer.com/wp-content/uploads/2019/11/Im-Still-Standing.pdf [perma.cc/A7FK-ZA3R] (last visited Nov. 2, 2023).

86. Kim, *supra* note 84.

87. Christine E. Skoczylas & Dana Amato Sarros, *No Harm, No Foul? Not So Fast: Illinois Supreme Court Allows BIPA Lawsuits Without Allegations of Actual Injury*, NAT'L L. REV. (June 5, 2019), www.natlawreview.com/article/no-harm-no-foul-not-so-fast-illinois-supreme-court-allows-bipa-lawsuits-without [perma.cc/WWL6-JAF9].

88. Kim, *supra* note 84.

89. Phillip M. Schreiber, *Illinois Supreme Court Expands Potential Liability Under Biometric Information Privacy Act*, HOLLAND & KNIGHT (Jan. 25, 2019), www.hklaw.com/en/insights/publications/2019/01/illinois-supreme-court-expands-potential-liability [perma.cc/ER2V-38RW].

90. *Id*.

91. Eckler & Townsend, *supra* note 85.

92. *Id.*

93. *Id.*

94. James Shreve et al., *Seventh Circuit Rules That Federal Court Has*

However, defendants often wish to remove them to federal court under the Class Action Fairness Act.[95] The Class Action Fairness Act allows defendant classes to be removed to federal court as long as the case involves at least 100 plaintiffs, one of the plaintiffs is from outside the defendant's home state, and the potential liability is at least $5 million.[96]

Additionally, a plaintiff must have Article III standing for a federal court to have jurisdiction to hear their BIPA case.[97] To establish Article III standing, the party must allege that he personally suffered a concrete and particularized injury that is traceable to the opposing party's allegedly unlawful actions and redressable by a favorable judicial decision.[98] Unlike Illinois state courts, simply qualifying as an "aggrieved" person under the statute does not give the plaintiff automatic standing in federal court.[99] The United States Supreme Court has clarified that a bare procedural violation alone cannot confer Article III standing without pleading a particularized concrete harm.[100] *Bryant v. Compass Group USA, Inc.* and *Fox v. Dakkota Integrated Systems* demonstrate how the Article III standing requirement differs from Illinois' "aggrieved" person requirement.

1. Bryant v. Compass Grp. USA.

In *Bryant*, the central issue was whether the plaintiff employee suffered a concrete injury in fact necessary for Article III standing, which is the right to bring a lawsuit in federal court.[101] A vending machine company installed a Smart Market vending machine in the company's cafeteria.[102] The machines did not accept cash, and users had to create an account using their fingerprints.[103] During orientation, the employer instructed the employee and her

Jurisdiction Over Claims Brought Under BIPA, THOMPSON COBURN LLP (May 11, 2020), www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2020-05-11/seventh-circuit-rules-that-federal-court-has-jurisdiction-over-claims-brought-under-bipa [perma.cc/6PXC-WHAG].

95. *Id.*

96. *Id.*

97. Taylor L. Haran, *Seventh Circuit: BIPA Claims Can Be Heard in Federal Court*, FAEGRE DRINKER (May 6, 2020), www.faegredrinker.com/en/insights/publications/2020/5/seventh-circuit-bipa-claims-can-be-heard-in-federal-court [perma.cc/AN9E-YQFB].

98. *Art. III.S2.C1.6.1 Overview of Standing*, CORNELL L. SCH., www.law.cornell.edu/constitution-conan/article-3/section-2/clause-1/overview-of-standing [perma.cc/G7VN-NEQF] (last visited Oct. 13, 2023).

99. Eckler & Townsend, *supra* note 85.

100. Spokeo, Inc. v. Robins, 578 U.S. 330, 342 (2016) (explaining that a plaintiff must allege an injury that is both concrete and particularized to have standing under Article III of the Constitution).

101. *Id.*

102. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619-20 (7th Cir. 2020).

103. *Id.*

coworkers to scan and register their fingerprints into the vending machine system to establish a user account.[104] Once registered, users could purchase items and add money with a finger scan.[105]

The employee filed a claim in Illinois state court, contending that the vending machine company violated section (a) by not posting publicly a retention schedule and guidelines for destroying the fingerprint information it was collecting.[106] She also alleged a violation of section (b), pleading that the company failed to make the requisite disclosures, denying her the ability to give informed consent required under BIPA.[107] The vending machine company removed the case to federal court under the Class Action Fairness Act.[108] Bryant moved to remand the action to the state court, claiming that the district court did not have subject matter jurisdiction because she lacked the concrete injury necessary to satisfy the federal requirement for Article III standing.[109]

The court denied standing for the employee's section (a) claim, reasoning that the plaintiff failed to show that the statutory violation presented a particularized harm resulting from the violation.[110] The court held that a bare procedural violation without concrete harm does not satisfy the injury requirement for Article III standing.[111]

The court held that the employee's section (b) claim satisfied standing requirements, reasoning that the plaintiff alleged that because Compass failed to provide her with information purportedly required by BIPA, she lost the right to control her biometric identifiers and information. The plaintiff alleged a concrete and particularized harm sufficient to confer Article III standing – the loss of the right to control her information. –

2. Fox v. Dakkota Integrated Sys., LLC

Fox v. Dakkota Integrated Sys., LLC. is a case where a plaintiff alleged a particularized harm resulting from the entity's violation of section 15(a) that satisfied Article III standing.[112]

Here, Fox's employer, Dakkota, required employees to clock in

---

104. *Id.*

105. *Id.*

106. *Id.* at 619.

107. Jonathan S. Kolodner et al., *The Seventh Circuit Holds That Lack of Disclosure and Informed Consent Under Biometric Information Privacy Act Satisfies Article III Standing Requirement*, CLEARLY GOTTLIEB (May 12, 2020), www.clearycyberwatch.com/2020/05/the-seventh-circuit-holds-that-lack-of-disclosure-and-informed-consent-under-biometric-information-privacy-act-satisfies-article-iii-standing-requirement/ [perma.cc/24ZG-VR3H].

108. *Bryant*, 958 F.3d at 620.

109. *Id.*

110. *Id.*

111. *Id.* at 621.

112. Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146 (7th Cir. 2020).

and out by scanning their hands on a biometric timekeeping device.[113] Dakkota used third-party software to capture the data stored in a third-party database.[114] Fox alleged that Dakkota failed to develop, publicly disclose, and implement a data-retention schedule and guidelines for the permanent destruction of its employees' biometric identifiers and failed to permanently destroy her biometric data when she left the company.[115] Fox alleged that the violation resulted in the unlawful retention of her handprint after she left the company and the unlawful sharing of her biometric data with the third-party database administrator.[116] The court held that Fox had Article III standing to litigate her section 15(a) claim in federal court because Fox alleged a concrete and particularized injury - the unlawful collection of her biometric data.[117]

As these cases show, an individual must allege some actual injury or adverse effect beyond violation of his or her rights under BIPA to satisfy Article III Standing and successfully remove the case to federal court.

D. Standing Strategies

Sometimes, Plaintiffs purposely fail to allege a concrete and particularized injury to satisfy Article III standing. *Thornley v. Clearview AI, Inc.*, demonstrates times when plaintiffs purposely fail to satisfy Article III standing by not alleging a concrete and particularized harm resulting from the alleged BIPA violation.

1. Thornley v. Clearview AI, Inc.

Defendant Clearview AI, Inc., an American facial recognition company, used a proprietary algorithm to scrape pictures from social media sites, harvested the pictures' biometric facial scan and associated metadata, and stored the information on a server in New York and New Jersey.[118] The plaintiffs filed their class action in state court, specifically the Circuit Court of Cook County.[119] Thornley's initial complaint asserted violations of three subsections of BIPA: (a), (b), and (c).[120] Clearview removed the case to federal court pursuant to the class action fairness act. However, shortly

113. *Id.* at 1149.
114. *Id.*
115. *Id.* at 1150.
116. *Id.*
117. Brett Doran et al., *Seventh Circuit Finds Article III Standing for (Some) Section 15(a) Violations of the Illinois Biometric Privacy Act*, NAT'L L. REV. (Nov. 30, 2020), www.natlawreview.com/article/seventh-circuit-finds-article-iii-standing-some-section-15a-violations-illinois [perma.cc/TK33-C4U4].
118. Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1242-43 (7th Cir. 2021).
119. *Id.* at 1243.
120. *Id.*

after the removal, Thornley voluntarily dismissed the action.[121] Thornley then returned to the Circuit Court of Cook County with a new, significantly narrowed action against Clearview.[122] The new action only alleged a violation of BIPA §15(c).[123] Clearview again removed the case to federal court, and Thornley filed a motion to remand.[124] Thornley argued that the violation of section 15(c) was only a "bare procedural violation, divorced from any concrete harm," and did not support Article III standing.[125] The district court agreed with her and remanded the case to state court.[126]

On review, the Seventh Circuit Court of Appeals addressed the issue of whether Thornley had standing to pursue the case in federal court.[127] The court concluded that Thornley and her co-plaintiffs did not have Article III standing because they described only a general, regulatory violation in their complaint, not something particularized to them and concrete. [128]

The court noted that plaintiffs, like Thornley, can draft their allegations and scope of the proposed class carefully to steer clear of federal court.[129] The court also noted that plaintiffs may take advantage of the fact that Illinois permits BIPA cases that allege bare statutory violations without any further need to allege or show injury.[130]

2. Why Plaintiffs Prefer Illinois State Courts to Hear Their BIPA Claims

Plaintiffs prefer Illinois State court because of their large damage payouts and low standing requirement. Illinois BIPA allows for statutory damages of up to $1,000 per negligent violation and $5,000 per intentional or reckless violation.[131] As Rosenbach established, a plaintiff is not required to show or even allege actual harm to recover statutory damages; a violation of the statute in itself is sufficient to support the individual's statutory cause of

---

121. *Id.*

122. *Id.*

123. Christopher Ward & Aaron Wegrzyn, 7*th Circ. Ruling Highlights Continuing BIPA Questions*, FOLEY & LARDNER LLP (Jan. 27, 2021), www.foley.com/news/2021/01/7th-circ-ruling-highlights-bipa-questions/ [perma.cc/5UFH-MJ96].

124. *Id.*

125. *Thornley*, 984 F.3d at 1243.

126. *Id.*

127. *Id.* at 1244.

128. *Id.* at 1248.

129. *Id.* at 1248-49; *see also* James F. Bogan III, *BIPA Class Actions: Seventh Circuit Endorses Pleading Strategy Calculated to Avoid Removal to Federal Court*, KILPATRICK (Jan. 29, 2021), www.ktslaw.com/Blog/classaction/2021/1/bipa [perma.cc/M7F5-3TN4] (explaining the pleading strategy calculated to avoid removal to federal court).

130. *Id.*

131. 740 ILL. COMP. STAT. 14/20 (2008).

action.[132] It was not surprising that BIPA-related lawsuits rose 1400% in the year after the *Rosenbach* ruling.[133]

This lack of harm standard and substantial statutory damages that can be assessed for each violation has allowed significant damage awards.[134] *Cothron v. White Castle System, Inc.* portrays how plaintiffs can recover massive damage payouts by simply alleging BIPA violations without actual harm resulting from the violation.[135]

3. Cothron v. White Castle Systems Inc.

Plaintiff, a White Castle employee, filed a class action on behalf of all Illinois White Castle employees.[136] The employee alleged that White Castle violated Sections 15(b) and (d) of BIPA by requiring its employees to scan their fingerprints to access their pay stubs and computers and disclosed their fingerprint scans to a third-party vendor who verified each scan and authorized the employee's access.[137] The employee alleged that White Castle implemented this biometric-collection system without obtaining her consent in violation of the Act.[138] The employee alleged that the fingerprint scanning system was introduced in 2004, four years before the Illinois legislature enacted BIPA.[139]

The plaintiff initially filed the case in Illinois state court, and the defendant removed the case to the Northern District of Illinois under the Class Action Fairness Act.[140] White Castle moved to dismiss the case, arguing that the employee's claims were untimely.[141] They argued that the statute of limitations expired since her claims accrued in 2008, the first time she scanned her

---

132. *Rosenbach*, 129 N.E.3d at 1206.

133. Megan L. Brown, et al., *A Bad Match: Illinois and The Biometric Information Privacy Act*, INST. FOR LEGAL REFORM, www.instituteforlegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf [perma.cc/7ABP-G6GG] (last visited Nov. 2, 2023).

134. David Rice et al., *U.S. District Court Holds That BIPA's Liquidated Damages Are Discretionary*, DAVIS WRIGHT TREMAINE LLP (Aug. 15, 2023), www.dwt.com/blogs/privacy--security-law-blog/2023/08/illinois-bipa-biometrics-privacy-court-ruling [perma.cc/D37C-NUFQ].

135. Danielle Kays & James Nasiri, *Illinois Supreme Court Upholds Per-Scan Damages for BIPA Claims*, JD SUPRA (July 20, 2023), www.jdsupra.com/legalnews/illinois-supreme-court-upholds-per-scan-6420973/ [perma.cc/32GX-SPHZ].

136. Cothron v. White Castle Sys., 216 N.E.3d 918, 920 (Ill. 2023).

137. *Id.* at 920.

138. *Id.*

139. *Id.*

140. *Id.*

141. Hannah Schaller et al., *When Is a BIPA Violation Actionable? White Castle Asks Seventh Circuit to Weigh In*, ZWILLGENBLOG (June 10, 2021), www.zwillgen.com/privacy/bipa-violation-white-castle-seventh-circuit/ [perma.cc/SPS5-AP88].

fingerprint after BIPA was enacted.[142]

The district court concluded that the lawsuit was timely, reasoning that every unauthorized fingerprint scan was a separate violation of the statute and a new claim accrued with each unauthorized scan.[143] The Seventh Circuit referred the case to the Illinois Supreme Court to answer the question of whether BIPA claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?[144]

The court found that the employee's claims under Sections 15(b) and 15(d) accrued every time a private entity collects or disseminates biometric data without prior informed consent.[145] White Castle argued that under Illinois law, a claim accrues when a legal right is first invaded and an injury inflicted, which was not the case here.[146] The court applied *Rosenbach*, noting that a statutory violation alone is a sufficient injury without anything more.[147]

White Castle also argued that interpreting BIPA to allow for repeated accruals of claims by one individual "would constitute annihilative liability not contemplated by the legislature and possibly be unconstitutional."[148] White Castle estimated that if the employee brings claims on behalf of 9,500 current and former White Castle employees, where employees potentially scan their fingerprints multiple times per shift, the damages in her action may exceed $17 billion.[149] The court was unpersuaded by these arguments, concluding that policy-based concerns about potentially excessive damage awards under the Act are best addressed by the Illinois legislature to clarify its intent regarding the assessment of damages under BIPA.[150]

The dissenting opinion in White Castle contended that the majority's interpretation was unsupported by BIPA's plain language and "will lead to consequences that the legislature could not have intended."[151] The dissent argued that a private entity may

142. *Id.*

143. *Cothron*, 216 N.E.3d at 921.

144. *Id.* at 920.

145. Morgan A. Dilbeck & Mitchel D. Torrence, *Illinois Supreme Court Poised To Decide BIPA Claim Accrual Question*, (July 26, 2022) www.clausen.com/illinois-supreme-court-poised-to-decide-bipa-claim-accrual-question/ [perma.cc/84F9-BDMP].

146. *Cothron*, 216 N.E.3d at 927.

147. *Id.* at 928.

148. *Id.*

149. *Id.*

150. *Id.* at 928-29.

151. Nadine C. Abrahams et al., *Illinois Supreme Court Issues Long-Awaited BIPA Decision in Cothron v. White Castle Systems*, JACKSONLEWIS (Feb. 21, 2023), www.jacksonlewis.com/insights/illinois-supreme-court-issues-long-awaited-bipa-decision-cothron-v-white-castle-systems [perma.cc/L5RL-2UK8].

obtain an individual's biometric information in violation of BIPA only once, as there is only one loss of control or privacy, which happens when the entity first obtains the information.[152]

The dissent reasoned that White Castle already had the biometric information, and the court could not consider subsequent scans as obtaining additional information.[153] The dissent highlighted two issues in the majority's decision.[154] First, the majority approach will incentivize plaintiffs to delay bringing their claims as long as possible, thereby impermissibly "racking up damages."[155] Second, in light of the massive damages award White Castle may face, the dissent argued that the majority's interpretation is contrary to legislative intent.[156] The dissent concluded that "[i]mposing punitive, crippling liability on businesses could not have been a goal of the Act, nor did the legislature intend to impose damages wildly exceeding any remotely reasonable estimate of harm."[157]

4. Illinois BIPA Targets Companies Acting in Good Faith Where the Plaintiff Alleges No Actual Harm Resulting from the Violation.

Illinois BIPA has targeted companies acting in good faith where the plaintiff alleges no harm from the alleged violation. Respondus, a company helping students and schools adapt to remote learning during the global COVID-19 pandemic, created software to detect and prevent cheating in online tests.[158] Plaintiffs filed a series of putative class actions against Respondus.[159] They alleged that Respondus's exam software uses student webcams to capture biometric data through scans of students' facial geometry in violation of BIPA.[160] Respondus agreed to a 6.25 million settlement to resolve the class action lawsuit.[161]

---

152. *Cothron*, 216 N.E.3d at 932.

153. *Id.* at 932.

154. *Id* at 933.

155. *Id.*

156. *Id.* at 934.

157. Abrahams et al., *supra* note 151.

158. Shea Swauger, *Software That Monitors Students During Tests Perpetuates Inequality and Violates Their Privacy,* MIT TECH. REV. (Aug. 7, 2020), www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/ [perma.cc/9NKR-XQH8]; *A Bad Match: Illinois and the Biometric Information Privacy Act*, INST. FOR LEGAL REFORM, www.instituteforlegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf [perma.cc/B6P2-6LYT] (last visited Dec. 12, 2023).

159. *Id.*

160. Robert D. Boley et al., *BIPA Class Actions - 2022 Round-Up*, NAT'L L. REV. (Dec. 9, 2022), www.natlawreview.com/article/bipa-class-actions-2022-round [perma.cc/QX7R-Y3ZN].

161. Danny Nguyen, *Respondus Online Exam BIPA Class Action Lawsuit,* HUSTLER MONEY BLOG (Aug. 22, 2023),

Additionally, a truck driver brought a putative class action against Samsara Inc., a facial recognition technology provider for interstate motor carriers that developed a dashboard camera that extracted biometric images of drivers' faces to identify and monitor them for fatigue and distraction.[162] The district court denied Samsara's motion to dismiss, declining to note the uniform scheme of federal regulation of truck safety technology and supported an award of enhanced damages.[163]

Hyatt also settled a class action claim for $1.5 million after collecting employee fingerprints through its biometric time and attendance system, allowing employees to punch in and out to help them accurately get paid for time worked. The plaintiffs argued that Hyatt did not technically comply with the law and offered no actual harm caused by the biometric timekeeping system.

5. Who Gets Compensated?

A study found that plaintiffs' law firms are the largest beneficiaries of BIPA cases.[164] For example, in a Facebook settlement involving the company's facial recognition technology, a federal judge approved a $650 million settlement fund, $97.5 million of which goes to attorneys' fees, with class members receiving around $350 each.[165] In April 2021, an Illinois judge approved a $25 million BIPA class action settlement between a company called ADP and its employees, awarding $8.75 million to plaintiffs' counsel and only $375 to individuals who filed claims under the settlement.[166] Additionally, in May 2021, an Illinois judge approved a $987,850 settlement against a company called Lifespace, where the attorneys were granted almost $329,000 in attorneys' fees and costs, while the employee class members received only $1,150.[167] Further research has revealed that four plaintiffs' law firms made more than $30 million each from consumer-oriented settlements alone.[168]

---

www.hustlermoneyblog.com/respondus-online-exam-bipa-class-action-lawsuit/ [perma.cc/LR8E-KNHW].

162. Boley et al., *supra* note 160.

163. *Id.*; *Class Action BIPA Lawsuit Against Manufacturer of Dashcam Technology Moves Forward In Illinois,* MARKETSCREENER (July 15, 2022), www.marketscreener.com/quote/stock/SAMSARA-INC-130784042/news/Class-Action-BIPA-Lawsuit-Against-Manufacturer-Of-Dashcam-Technology-Moves-Forward-In-Illinois-40991723 [perma.cc/4LU9-WKP8].

164. Kaitlyn Harger, *Who Benefits From BIPA? An Analysis of Cases Brought Under Illinois' State Biometrics Law,* CHAMBER OF PROGRESS (Apr. 2023), www.progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf [perma.cc/3R7K-29ZV].

165. Brown et al., *supra* note 133.

166. *Id.*

167. *Id.*

168. *See* Harger, *supra* note 164 (explaining that the four law firms were

IV. PROPOSAL

Illinois has gone too far by allowing plaintiffs to recover massive damages for mere technical violations that result in no harm. Illinois must eliminate its private right of action and vest the attorney general with the sole discretion to bring a claim under BIPA. The Illinois courts should only allow standing for violations that cause actual harm. Additionally, Illinois should implement a safe harbor provision to protect entities acting in good faith where the entity's violation results in no actual harm to the plaintiff.

A. The Illinois Legislature Should Vest the Attorney General with the Sole Discretion to Bring a Claim Under BIPA

The Attorney General should enforce the biometric law exclusively because they are experts in the best position to enforce complex and technical laws. One of the Illinois Attorney General's primary functions is to help consumers victimized by fraud, deception, or unfair competition.[169] The Illinois Attorney General's Office already has a Consumer Protection Division responsible for protecting consumers and businesses from fraud, deception, and unfair business practices, and is composed of several bureaus.[170] When a consumer is victimized by fraud, deception, or unfair methods of competition, the consumer can file a complaint online. Attorneys, investigators, and other members of the Consumer Protection Division use the information submitted to carry out the functions of the Illinois Attorney General.[171] This division would be the best fit to handle BIPA-related complaints.

Unlike a private right of action where plaintiffs with no legal expertise can file frivolous claims, vesting enforcement rights with the Attorney General ensures knowledgeable and experienced individuals in that particular area of law review the claims and ensure they are meritorious.[172] The Illinois Attorney General has more resources than most private plaintiffs, and vesting exclusive authority in the Attorney General to bring a claim under a biometrics law allows legal experts to bring claims after proper investigation and ensures that the claims brought have legal merit.

Carrol, Rhow, & Fegan, Edelson, P.C., Labaton Sucharow, LLP, and Robins, Gellar, Rudman, & Dowd, LLP).

169. *Protecting Consumers: Filing A Consumer Complaint,* ILLINOIS ATT'Y GEN., www.ag.state.il.us/consumers/ [perma.cc/KSA2-S85X] (last visited Nov. 2, 2023).

170. *Id.*

171. *Id.*

172. *Id.*

Another reason why Illinois should grant the attorney general the sole right to bring a claim under its biometric law is because it allows the attorney general to prioritize important cases. Since CUBI's enactment in 2009, the Texas Attorney General has filed only two claims under the statute.[173] However, the two claims filed were massive against two companies whose violations affected millions of Texans.[174] One claim was against Facebook for collecting millions of user's facial identifiers and sending the information to others for profit without the individuals' consent.[175] The second claim was against Google for collecting facial geometry and storing it on its Google Photos app without gaining consent and collecting voice prints without consent.[176] "Google had human beings listen to the most intimate conversations about everything that people discuss in the safety of their own home including sex, religion, politics, and health."[177]

This process differs from Illinois, where plaintiffs have filed nearly 2,000 lawsuits alleging mere technical violations, targeting small businesses and companies acting in good faith.178 The Attorney General can prioritize significant cases considering the harm caused, the number of people affected, and the violations committed.

B. The Illinois Courts Should Only Allow Standing for Violations that Cause Actual Harm

The Illinois courts should only allow standing for violations that cause actual harm. Allowing mere technical violations without showing any harm to satisfy standing has led to frivolous lawsuits, harmed small businesses, and hindered innovation.

Allowing mere technical violations to satisfy standing without showing actual harm has caused plaintiffs to file lawsuits that would otherwise be frivolous if not for *Rosenbach*. The *Rosenbach* ruling opened the floodgates to mass litigation after eliminating the need to show any actual injury. Since then, plaintiffs have filed over 2,000 claims alleging mere technical violations of BIPA, causing entities to settle and pay damages up to 8 to 9 figures.[179]

Allowing mere technical violations to satisfy standing without

---

173. Huffman & Treas, *supra* note 69.

174. *Id.*

175. *Id.*

176. *Id.*

177. Plaintiff's Original Petition at 21, Texas v. Google LLC, No. cv58999 (Dist. Midland Cnty., Tex. Oct. 20, 2022).

178. Daniel Wiessner, *Illinois Top Court Endorses Five-Year Window for Biometric Privacy Claims,* REUTERS (Feb. 2, 2023), www.reuters.com/legal/litigation/illinois-top-court-endorses-five-year-window-biometric-privacy-claims-2023-02-02/ [perma.cc/V9FN-458Z].

179. Brown et al., *supra* note 133.

showing actual harm has harmed small businesses. 88% of BIPA lawsuits have been employer-employee disputes resulting from biometric timekeeping.[180] Tech giants are not the only private entities getting hit with lawsuits for technical violations.[181] Mostly, small businesses face litigation under BIPA, and because BIPA does not contain a cure period to correct mistakes, small businesses that cannot afford large compliance departments are hit the hardest.[182] Small technical mistakes have resulted in millions of dollars of damages since BIPA allows plaintiffs to recover $1,000 to $5,000 per violation of the statute.[183]

Additionally, allowing mere technical violations to satisfy standing without showing actual harm has forced companies to prioritize not getting sued over safety and innovation.[184] As shown above, companies utilizing cameras to monitor distracted or drowsy truck drivers and companies offering remote proctoring software to help schools adapt to remote learning have been hit with massive lawsuits.[185] Illinois BIPA has punished businesses operating in good faith and deterred them from adopting biometric-based technology that would benefit businesses and consumers. To remedy the harm BIPA caused, Illinois courts should only allow standing for violations that cause actual harm.

C. The Illinois Legislature Should Implement a Safe Harbor Provision to Protect Entities Acting in Good Faith Where the Plaintiff Alleges No Harm Resulting from the Violation

Illinois should implement a safe harbor provision allowing an entity in violation the right to cure their breach where the violation did not result in actual harm to the plaintiff and the entity was acting in good faith. A safe harbor provision grants protection from liability or penalty if the defendant meets certain conditions.[186] The right to

180. Harger, *supra* note 164.

181. Brown et al., *supra* note 133.

182. Jonathan Herpy, *Staying In Compliance With Biometric Privacy Laws As A Business,* FORBES (Apr. 5, 2021), www.forbes.com/sites/forbesbusinesscouncil/2021/04/05/staying-in-compliance-with-biometric-privacy-laws-as-a-business/?sh=116f7f703123 [perma.cc/Y96A-V7XV].

183. Tyler Newby, et al., *BIPA's Per-Scan Damages May Create "Annihilative Liability",* FENWICK & WEST LLP (Mar. 6, 2023), www.fenwick.com/insights/publications/bipas-per-scan-damages-may-create-annihilative-liability [perma.cc/NK8D-KEPK].

184. Megan Hickey, *Illinois biometric data privacy law may be bad for business, some say,* CBS NEWS CHICAGO (Mar. 7, 2023), www.cbsnews.com/chicago/news/illinois-biometric-data-privacy-business/ [perma.cc/YGX3-9DX3].

185. Boley et al., *supra* note 160.

186. *Safe Harbor*, CORNELL L. SCH., www.law.cornell.edu/wex/safe_harbor

cure allows a party to resolve disputes before taking drastic actions.[187] Currently, BIPA does not offer a safe harbor provision. Implementing a safe harbor provision would encourage technological innovation, reduce the burden on the judicial system, and balance privacy with practicality.

A safe harbor provision would encourage technological innovation with biometric technologies by reducing the fear of litigation for unintentional, harmless violations. Providing a safety net for good faith, non-harmful actions can encourage companies to develop new biometric applications without fearing disproportionate legal consequences.

A safe harbor provision can reduce the burden on the judicial system by filtering out cases where there is no allegation of actual harm. This ensures that courts focus on more serious violations that have real impacts on individuals rather than being bogged down with numerous cases of technical non-compliance that cause no actual harm.

Additionally, implementing a safe harbor provision would balance privacy with practicality. The provision would balance protecting individual privacy rights and recognizing the practical challenges businesses face in complying with BIPA. A safe harbor provision acknowledges that while biometric data protection is crucial, absolute compliance in rapidly evolving technological landscapes is challenging, and minor, non-harmful errors should not be unduly penalized.

V. CONCLUSION

Illinois BIPA is an employer's nightmare, holding employers liable for significant damage awards even where they act in good faith and cause no measurable harm to plaintiffs. The current law creates a windfall for plaintiffs' attorneys, clogs the judicial system, and stifles innovation. The Illinois legislature should amend BIPA to vest the Attorney General with the sole discretion to bring a claim under the statute, only allow standing for violations that cause actual harm, and implement a safe harbor provision to protect entities acting in good faith where the plaintiff alleges no harm from the violation.

[perma.cc/WF3G-SV8N] (last visited Nov. 2, 2023).

187. Alex Benarroche, *The Right To Cure - Resolving Disputes Without Claims or Legal Action,* LEVELSET (Feb. 4, 2022), www.levelset.com/blog/right-to-cure/ [perma.cc/6JAR-WYPD].