DePaul Law Review

Volume 71
Issue 3 *Summer 2022*

Article 9

The Illinois Biometric Privacy Act Post-Rosenbach: Disposing of Actual Harm Inflicts Limitless Harm Onto Businesses

James Nasiri

THE ILLINOIS BIOMETRIC PRIVACY ACT POST-*ROSENBACH*: DISPOSING OF ACTUAL HARM INFLICTS LIMITLESS HARM ONTO BUSINESSES

I. Introduction

In our ever-evolving digital age, advancements in technology have made the majority of Americans feel that their personal privacy is less private than ever.[1] Company-wide data breaches are an unfortunately common occurrence. In Illinois, one notable company's data breach led to the passage of the Illinois Biometric Information Privacy Act (BIPA), which regulates the collection and retention of biometric data.[2] However, in the years since its passage, BIPA's scope has been extended to a point where the majority of BIPA lawsuits now seek to punish employers for mere procedural violations of the law.[3] From a practical perspective, this punitive shift in the law exposes businesses to expensive class action litigation where the business itself caused no current or future risk of harm to an individual's personal privacy interests.

This Comment begins by providing a background on biometric data and how novel biometric technologies inspired the passage of BIPA.[4] After briefly discussing the early BIPA landscape in Illinois, Part II offers an overview of the Illinois Supreme Court's landmark decision in *Rosenbach v. Six Flags Entertainment Corp*.[5] Finally, Part II concludes with a summary of how the *Rosenbach* decision has impacted BIPA litigation.[6]

Part III first discusses the variety of new legal issues rooted in the *Rosenbach* decision.[7] Next, this Part examines how BIPA jurisprudence aligns with federal and state standing principles, thereby high-

1. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, Pew Res. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

2. Charles N. Insler, *How to Ride the Litigation Rollercoaster Driven by The Biometric Information Privacy Act*, 43 S. Ill. U. L.J. 819, 819–20 (2019) [hereinafter Insler, *How to Ride the Litigation Rollercoaster*].

3. *Id.* at 821–22.

4. *See generally infra* Part II.

5. *See infra* Part II.D.

6. *See infra* Part II.E.

7. *See infra* Part III.A.

lighting one major issue with *Rosenbach* and its progeny.[8] Additionally, this Part analyzes a group of new BIPA defense theories to highlight the law's vague nature and then concludes with a suggested legislative measure to resolve the statute's ambiguities.[9]

Part IV of this Comment suggests that, without a legislative amendment to address BIPA's unclear and punitive nature, the statute will continue causing substantial harm to businesses for mere procedural violations.[10] However, should the Illinois General Assembly take legislative action with respect to certain key aspects of BIPA, this Part suggests that the law can be better tailored so that only entities that caused actual, concrete harm to individual privacy interests are held accountable in the court system.[11]

II. BACKGROUND

In 2008, the Illinois General Assembly enacted the Illinois Biometric Privacy Act, a first-of-its-kind privacy statute offering a private right of action to aggrieved individuals.[12] In the years since BIPA's enactment, biometric identifiers like fingerprints, retinal scans, and facial recognition patterns have become increasingly common in the workplace.[13] Employers use these forms of unique data to protect their databases, secure building access, ensure accurate employee timekeeping, and more.[14] In acknowledgment of the widespread use of biometric data, plaintiff's-side class action firms in Illinois began a BIPA "filing frenzy" that was further fueled by a 2019 Illinois Supreme Court decision holding that plaintiffs need not suffer actual damage to have standing under the law.[15] The result has been a court system packed with ongoing biometric privacy class actions, a variety of unanswered legal questions concerning the scope of BIPA, and a

8. *See infra* Part III.B.

9. *See infra* Part III.D.

10. *See generally infra* Part IV.

11. *See infra* Part IV.B.

12. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 821.

13. *See generally* Roy Maurer, *More Employers Are Using Biometric Authentication*, SOC'Y FOR HUM. RES. MGMT. (Apr. 6, 2018), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employers-using-biometric-authentication.aspx.

14. Ana Tagvoryan et al., *Learn the Rules on Employers' Use of Biometric Data*, SOC'Y FOR HUM. RES. MGMT. (Apr. 1, 2019), https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/regulation-employer-use-biometric-data.aspx.

15. Gerald L. Maatman, Jr. et al., *Copy-Cat Class Actions Meet Copy-Cat Legislation: Illinois' BIPA Spurs New Biometric Privacy Legislation Across the Nation*, SEYFARTH SHAW WORKPLACE CLASS ACTION BLOG (July 11, 2019), https://www.workplaceclassaction.com/2019/07/copy-cat-class-actions-meet-copy-cat-legislation-illinois-bipa-spurs-new-biometric-privacy-legislation-across-the-nation/ [hereinafter Maatman, Jr. et al., *Copy-Cat Class Actions*].

business landscape in which employers of all sizes are forced to defend complex class action lawsuits with high potential damages.

A. What are Biometrics?

The world has made, and continues to make, tremendous strides in terms of technological innovation. In a setting that would have been virtually unimaginable twenty to thirty years ago, people are now able to communicate, work, make financial decisions, and purchase almost any conceivable item or service in an instant from their computers and mobile devices.[16] These novel advancements have connected global markets and eased the flow of information, but they are also accompanied by several negative effects.[17] Namely, an individual's personal information is now more accessible than ever, leading the majority of Americans to believe that their data is less secure than it has ever been.[18]

Put simply, "[b]iometrics" are "unique physical characteristics . . . that can be used for automated recognition."[19] Common "biometric identifiers" include fingerprints, retinal scans, facial patterns, and voice recognition.[20] In today's technology-reliant environment, a litany of businesses across several industries use biometric technology to simplify processes such as timekeeping, identification, mobile payment, and more.[21] Businesses and government entities are increasingly using biometric technology rather than other identifiers (such as passwords and ID cards) because biometrics are unique to the individual, harder to steal, and generally more reliable.[22]

Entities that use biometrics for timekeeping and identification purposes typically do so through biometric recognition systems.[23] These systems recognize patterns of biometric data and store this data

16. *See generally* Kevin Webb, *From the Internet to the iPhone, Here Are the 20 Most Important Inventions of the Last 30 Years*, BUS. INSIDER (May 17, 2019, 6:17 PM), https://www.businessinsider.com/most-important-inventions-of-last-30-years-internet-iphone-netflix-facebook-google-2019-5.

17. Emily A. Vogels et al., *Tech Causes More Problems Than It Solves*, PEW RES. CTR. (June 30, 2020), https://www.pewresearch.org/internet/2020/06/30/tech-causes-more-problems-than-it-solves/.

18. Auxier et al., *supra* note 1.

19. *Biometrics*, DEP'T OF HOMELAND SEC. (Dec. 14, 2021), https://www.dhs.gov/biometrics.

20. Maria Korolov, *What Is Biometrics? 10 Physical and Behavioral Identifiers that Can Be Used for Authentication*, CSO (Feb. 12, 2019, 3:00 AM), https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html.

21. *What Is Biometrics*, MICH. ST. UNIV. DEP'T OF COMPUT. SCI. & ENG'G, http://biometrics.cse.msu.edu/info/index.html (last visited May 4, 2022).

22. *Id.*

23. *Id.*

through a two-step process: (1) the system first "enrolls" a user's biometric data by extracting a representation of the user's identifier and storing it as a template for future use; and (2) the system then recognizes a similar representation, which is then compared to the template through a computer algorithm; if the representation is adequately similar to the template, access is granted.[24]

Fingerprint time clocks use this second step to create an anonymous fingerprint template, which is then stored for future identification purposes.[25] However, the biometric timekeeping systems themselves never store the actual fingerprint data.[26] Once an individual scans in with his fingerprint, his print is immediately discarded.[27] Thus, the only data stored on the system is the anonymous template, which cannot be used for nefarious purposes by unauthorized third parties.[28]

B. The Illinois Biometric Information Privacy Act

BIPA was enacted in 2008 to govern the collection, storage, safeguarding, and use of biometrics, especially within the business and security screening industries.[29] The Illinois General Assembly enacted BIPA shortly after Pay By Touch went bankrupt, which (at the time) was the largest fingerprint scanning company in the state.[30] BIPA's section dedicated to legislative intent highlights that "major national corporations" are increasingly utilizing biometric technology, and that "[a]n overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information."[31] This section concludes by noting that the full extent of biometric technology use within this context is not yet known.[32]

BIPA explicitly regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[33] Examples of biometric identifiers include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[34] BIPA further defines "biometric information" as "any information, re-

24. *Id.*
25. *H*ow Do Fingerprint Biometric Time Clocks Work?, JOURNYX (Dec. 22, 2021), https://acumendatasystems.com/how-fingerprint-biometric-time-clocks-work/.
26. *Id.*
27. *Id.*
28. *Id.*
29. 740 ILL. COMP. STAT. 14/5(a) (2008).
30. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 819.
31. 740 ILL. COMP. STAT. 14/5(d).
32. *Id.* § 5(f).
33. *Id.* § 5(g).
34. *Id.* § 10.

gardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[35]

In terms of its application to civil litigation, BIPA has two relevant provisions: the written policy requirement and the informed consent requirement.[36] Section 15(a), also known as the written policy requirement, requires entities collecting biometric information to establish a publicly available written policy containing a retention schedule and procedures for permanently destroying biometric data.[37] Section 15(b), also known as the informed consent requirement, sets out the necessary steps an entity must take before collecting biometric information.[38] Specifically, before obtaining a person's biometric identifiers, an entity must: (1) inform the individual in writing of the proposed collection; (2) inform the individual in writing "of the specific purpose and length of term for which a biometric identifier . . . is being collected . . . ."; and (3) receive the individual's written release allowing collection of their biometric data.[39]

By passing BIPA, Illinois became the first state to enact its own biometric privacy statute.[40] While Texas[41] and Washington have since enacted their own biometric privacy statutes,[42] Illinois stood out from its counterpart states by including a private cause of action in BIPA.[43] To that end, BIPA provides that any "aggrieved" individual may recover $1,000 *per each negligent violation* and $5,000 *per each intentional or reckless violation* of the law.[44]

---

35. *Id.*

36. *See generally id.* § 15(a)–(b); *see also* Steven J. Pearlman & Edward C. Young, *Seventh Circuit Finds Article III Standing for an Illinois BIPA Claim*, NAT'L L. REV. (May 11, 2020), https://www.natlawreview.com/article/seventh-circuit-finds-article-iii-standing-illinois-bipa-claim.

37. 740 ILL. COMP. STAT. 14/15(a).

38. *Id.* § 15(b).

39. *Id.*

40. Gabrielle Neace, *Biometric Privacy: Blending Employment Law with the Growth of Technology*, 53 U. ILL. CHI. JOHN MARSHALL L. REV. 73, 73 (2019).

41. Alhough Texas's biometric privacy law has been in place since 2009, the Texas Attorney General made news in March 2022 when it lodged the first ever enforcement action under the law and sued Meta (formerly Facebook). Thomas E. Ahlering & Andrew Cockroft, *All Eyes on Texas After Filing First Enforcement Action Under State's Biometric Privacy Law*, KING & SPALDING (Mar. 15, 2022), https://www.kslaw.com/news-and-insights/all-eyes-on-texas-after-filing-first-enforcement-action-under-states-biometric-privacy-law. The lawsuit generally alleged that Meta violated Texas state privacy law by collecting Texas residents' biometric information via Facebook photo uploads without users' consent. *Id.*

42. *See generally* TEX. BUS. & COM. CODE § 503.001 (2009); *see also* WASH. REV. CODE § 19.375.010 (2017).

43. Neace, *supr*a note 40, at 77.

44. 740 ILL. COMP. STAT. 14/20.

C. Explosion in BIPA Class Action Filings

Civil lawsuit filings under BIPA were completely idle from its enactment in 2008 up until 2015, when the first BIPA case was filed against social media giant Facebook.[45] In this class action lawsuit, a Cook County man alleged that Facebook violated BIPA by capturing users' biometric data through the social network's facial recognition software without proper notification or storage procedures.[46] Despite this high-profile filing under the Act, there were only fifteen BIPA class action lawsuits in total from 2015 to 2016.[47]

Beginning in 2017, though, BIPA class action filings saw a significant spike.[48] In fact, according to one law firm's research, approximately 148 BIPA class actions were reported between 2017 and 2018.[49] This class action "explosion" was fueled by a deluge of punch clock lawsuits, which alleged BIPA violations related to an employer's use of fingerprinting for timekeeping purposes.[50] Other defining characteristics of the boom in BIPA class actions include a consistent pattern of "cookie-cutter" complaints with a small group of Chicago-area plaintiff's-side law firms filing the heavy majority of claims.[51]

D. Rosenbach v. Six Flags Entertainment Corp.

The most influential BIPA-related decision rendered to date in Illinois—*Rosenbach v. Six Flags Entertainment Corp.*—began with a teenager's class field trip to Six Flags Great America.[52] Specifically, Stacy Rosenbach, the class representative plaintiff, purchased a Six Flags Great America season pass for her son, fourteen-year-old Alexander Rosenbach, in advance of his field trip.[53] Upon arriving at the theme park, Six Flags Great America scanned Alexander Rosenbach's

45. Kathleen Foody, *Unique Illinois Privacy Law Leads to $550M Facebook Deal*, AP NEWS (Feb. 9, 2020), https://apnews.com/article/d9a58a7e656023b4ebef612f71c8c1c5.

46. Tony Briscoe, *Suit: Facebook Facial Recognition Technology Violates Illinois Privacy Laws*, CHI. TRIBUNE (Apr. 1, 2015), https://www.chicagotribune.com/news/breaking/ct-facebook-facial-recognition-lawsuit-met-story.html.

47. Gerald L. Maatman, Jr. et al., *Biometric Privacy Class Actions by The Numbers: Analyzing Illinois' Hottest Class Action Trend*, SEYFARTH SHAW WORKPLACE CLASS ACTION BLOG (June 28, 2019), https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/ [hereinafter Maatman, Jr. et al., *Biometric Privacy Class Actions*].

48. *Id.*

49. *Id.*

50. Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. B. J. 34, 36 (2018).

51. Maatman, Jr. et al., *Copy-Cat Class Actions*, *supra* note 15; Maatman, Jr. et al., *Biometric Privacy Class Actions*, *supra* note 47.

52. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1200 (Ill. 2019).

53. *Id.*

fingerprint, which could then be used to gain access to the park as a season pass holder.[54] Neither the plaintiff nor her son were ever provided with any paperwork in connection with the collection of Alexander's fingerprint.[55] The plaintiff, individually and on behalf of all similarly situated persons, subsequently sued Six Flags Great America asserting violations of BIPA.[56] Importantly, the plaintiff did not allege an actual injury; rather she stated that "had she known of [the] defendants' conduct, 'she never would have purchased a season pass for her son.'"[57]

1. Appellate Court Sides with Six Flags Entertainment Corp.

The defendant moved to dismiss the complaint on the basis that the plaintiff did not suffer actual harm—and thus was not "aggrieved" as required by traditional Article III standing principles—but the trial court denied the defendant's motion.[58] The defendant appealed, and the Second District Appellate Court reviewed the trial court's decision by assessing "whether a 'person aggrieved by a violation of [BIPA] must allege some actual harm."[59] As to this central question, the appellate court held that an aggrieved party must allege some actual harm to proceed under BIPA.[60]

The appellate court first discussed the plain meaning of the phrase "aggrieved party," emphasizing that the definitions of this term suggest that there must be some adverse effect to be aggrieved.[61] Next, the court highlighted several decisions holding that an "aggrieved party" must allege actual harm.[62] Namely, the United States District Court for the Northern District of Illinois determined that mere technical violations did not provide plaintiffs with a cause of action under BIPA, and the United States District Court for the Southern District of New York concurred in a subsequent decision.[63] A Wisconsin ap-

54. *Id.*
55. *Id.*
56. *Id.* at 1201.
57. *Id.* at 128.
58. Rosenbach v. Six Flags Entm't Corp., 147 N.E.3d 125, 127 (Ill. App. Ct. 2017).
59. *Id.* at 126–27.
60. *Id.* at 127.
61. *Id.* at 129 (While noting that the statute does not define "aggrieved," the appellate court reviewed several dictionary definitions of the phrase "aggrieved party," ultimately finding that these definitions together "suggest[ed] that there must be an actual injury, adverse effect, or harm in order for the person to be 'aggrieved.'").
62. *Id.* at 130.
63. *Id.* at 130; *see* McCollough v. Smarte Carte, Inc., No. 16-C-03777, 2016 WL 4077108, at *3 (N.D. Ill. Aug. 1, 2016); *see also* Vigil v. Take–Two Interactive Software, Inc., 235 F. Supp. 3d 499, 519–20 (S.D.N.Y. 2017).

pellate court also reasoned that, under similar circumstances concerning consumer disclosures by a mortgage broker, the plaintiff was not aggrieved by the broker's failure to provide him with a proper consumer disclosure.[64]

2. Illinois Supreme Court Answers Key BIPA Standing Question

The plaintiff appealed the Second District Appellate Court's holding, and on appeal, the Illinois Supreme Court reversed, finding that plaintiffs need not have suffered any actual damage beyond mere technical violations of BIPA in order to file suit under the law.[65] The Illinois Supreme Court focused on legislative intent by comparing BIPA's statutory language to that of the AIDS Confidentiality Act, which also requires no proof of actual damage.[66] The Illinois Supreme Court also emphasized the Illinois General Assembly's words regarding how biometric—in contrast to other identifiers—are unique to the individual and "once compromised, the individual has no recourse . . . ."[67]

With respect to the interpretation of the term "aggrieved," the Illinois Supreme Court also relied on dictionary definitions (which were different than those used by the appellate court) and cited a historic principle that "aggrieved" merely "means . . . a denial of some personal or property right."[68] In furtherance of its interpretation of BIPA, the Illinois Supreme Court relied on *Patel v. Facebook Inc.*, in which a California federal court analyzed the Illinois General Assembly's legislative intent and noted how technical violations of BIPA are the "precise harm the Illinois legislature sought to prevent . . . ."[69] The Illinois Supreme Court thus concluded that, since BIPA's private right of action is the only enforcement measure in the statute, the legislature must have intended for it to punish entities for failure to comply.[70]

---

64. *Rosenbach*, 147 N.E.3d at 130-31; *see* Avudria v. McGlone Mortg. Co., 802 N.W.2d 524, 527 (Wis. Ct. App. 2011).

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

66. *Id.* at 1204.

67. *Id.* at 1206.

68. *Id.* at 1205 (The Illinois Supreme Court based its interpretation on a 1913 case holding that "aggrieved" denotes "having a substantial grievance [or] a denial of some personal or property right." The Court then supported its interpretation with two dictionary definitions maintaining that "aggrieved" generally means infringement upon a legal right.); *see* Glos v. People, 102 N.E. 763, 766 (Ill. 1913).

69. *Rosenbach*, 129 N.E.3d at 1206; *see* Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018).

70. *Rosenbach*, 129 N.E.3d at 1207. More than two years after the Illinois Supreme Court's holding in *Rosenbach*, Six Flags agreed to resolve this class action for $36 million. The settlement

E. The Biometric Privacy Landscape Since Rosenbach

No case has had a more significant impact on the biometric privacy space than the *Rosenbach* decision.[71] On the litigation front, *Rosenbach* has emboldened the plaintiff's class action bar to file even more BIPA class actions regardless of the harm—or lack thereof—caused to the plaintiff.[72] *Rosenbach* has also spurred a series of new legal issues as defendants have adopted several novel defense theories in an attempt to evade BIPA liability, albeit with varying success.[73] Outside of the courtroom, lawmakers around the country are becoming increasingly interested in regulating biometric data as more private and public entities continue to utilize biometric technology.[74]

1. Status of the Class Action Space Following Rosenbach

The Illinois Supreme Court's decision in *Rosenbach* "opened the doors" to a flood of class action litigation against Illinois businesses.[75] In the decade-plus preceding *Rosenbach*, plaintiffs filed approximately 173 total class action lawsuits in Illinois courts.[76] Conversely, within just five months of the *Rosenbach* decision, there were at least 151 BIPA class action lawsuits filed.[77] This surge in filings shows no signs of slowing down either, as Illinois employers continue to face BIPA class actions in both federal and state court.[78]

Since *Rosenbach*, other Illinois courts—both federal and state—have begun analyzing additional questions regarding BIPA's scope

---

was paid to a class of Six Flags visitors between October 2013 and December 2018 whose fingerprints were scanned as they entered the theme park. Celeste Bott, *Six Flags Strikes $36M Deal To End Finger Scan Privacy Row*, Law360 (June 14, 2021, 7:20 PM) https://www.law360.com/articles/1393447/six-flags-strikes-36m-deal-to-end-finger-scan-privacy-row.

71. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 825–26.

72. Maatman, Jr. et al., *Biometric Privacy Class Actions*, *supra* note 47.

73. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 822–25.

74. Allison Grande, *NY Lawmakers Float Bill to Allow Biometric Privacy Suits*, Law360 (Jan. 6, 2021, 9:56 PM), https://www.law360.com/articles/1342347/ny-lawmakers-float-bill-to-allow-biometric-privacy-suits.

75. Maatman, Jr. et al., *Biometric Privacy Class Actions*, *supra* note 47.

76. *Id.*

77. *Id.*

78. Kristin L. Bryan & Aaron C. Garavaglia, *New BIPA Lawsuit Confirms that Employers Will Continue to "Face" Litigation Regarding the Collection of Employees' Biometric Information*, Nat'l L. Rev. (Nov. 17, 2020), https://www.natlawreview.com/article/new-bipa-lawsuit-confirms-employers-will-continue-to-face-litigation-regarding; *see also* Jennifer Marsh, *ANALYSIS: Biometrics Privacy Class Actions Increase This Year*, Bloomberg L. (Nov. 6, 2020, 4:18 AM), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-biometrics-privacy-class-actions-increase-this-year.

and applicability. With respect to standing,[79] the Seventh Circuit issued a somewhat surprising holding in *Bryant v. Compass Group USA, Inc.* when it split BIPA's two major statutory requirements for purposes of Article III standing.[80] The plaintiff in *Bryant* asserted violations of both BIPA's written policy requirement and its informed consent requirement.[81] After the defendant removed the case to federal court, the Seventh Circuit took up the question of whether the plaintiff's injuries were sufficiently concrete and particularized to warrant Article III standing.[82] While the Seventh Circuit did reason that the plaintiff's claims under § 15(b) were sufficient to confer Article III standing, it also held that the claims concerning the Act's public disclosure requirements under § 15(a) were not sufficiently concrete and particularized.[83]

In the months following the Seventh Circuit's decision in *Bryant*, plaintiffs' lawyers began to send their BIPA § 15(a) public disclosure claims back to Illinois state court, which is generally considered to be more plaintiff-friendly.[84] However, in November 2020, the Seventh Circuit questioned the applicability of *Bryant* in another BIPA class action lawsuit that concerned claims under § 15(a).[85] Namely, in *Fox v. Dakkota Integrated Systems*, the Seventh Circuit contradicted *Bryant* by holding that the plaintiff's § 15(a) claims actually belonged in federal court.[86] The Seventh Circuit noted that the plaintiff's § 15(a) claims in *Fox* regarding allegedly unlawful retention were farther reaching than the public disclosure claims in *Bryant* and further emphasized the presence of union preemption questions in *Fox*.[87]

Given the Seventh Circuit's somewhat conflicting holdings in *Fox* and *Bryant*, battles over BIPA standing and venue-shopping are sure

79. On the topic of standing, the U.S. District Court for the Central District of Illinois also refused to apply *Rosenbach* to a class action filed under BIPA. *See* Pruitt v. Par-A-Dice Hotel Casino, No. 1:20-cv-1084-JES-JEH, 2020 WL 5118035, at *2 (C.D. Ill. Aug. 31, 2020).

However, this refusal was mainly based on factual differences between the two cases, and the district court did not offer its own analysis of *Rosenbach*'s general applicability. *Id.*

80. *See generally* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).

81. *Id.* at 619–20.

82. *Id.* at 620–21.

83. *Id.* at 626.

84. Jonathan Bilyk & Scott Holland, *Appeals Panel: Judge Misapplied Decision Often Used by Biometrics Class Action Plaintiffs to Skip Out of Federal Court*, Cook Cty. Rec. (Nov. 18, 2020), https://cookcountyrecord.com/stories/565414533-appeals-panel-judge-misapplied-decision-often-used-by-biometrics-class-action-plaintiffs-to-skip-out-of-federal-court.

85. *See generally* Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146 (7th Cir. 2020).

86. *Id.* at 1156.

87. *Id.* at 1154, 1156.

to persist in the near future.[88] To complicate this issue even further, BIPA plaintiffs have started framing their complaints in a way that confers standing only in the preferential state-court venue.[89] For example, a group of Illinois residents sued technology company Clearview AI alleging that it profited from unlawfully collecting the plaintiffs' biometric identifiers and notably stating that the plaintiffs "suffered no injury" from the company's BIPA violation.[90] While acknowledging the bizarre nature of the plaintiffs' pleading strategy, the Seventh Circuit nevertheless allowed the case to proceed in state court, noting that the plaintiffs "may take advantage of the fact that Illinois permits BIPA cases that allege bare statutory violations."[91] Business advocates have expressed concern with this pleading strategy, arguing that Illinois courts have created a landscape in which the flood of BIPA class action claims will continue while defendants will face increased pressure to simply settle claims.[92]

With the plethora of ongoing BIPA class action litigation in Illinois, defendants have also started to offer unique defenses concerning the Act's practical limitations.[93] For instance, in Illinois state court, a nursing home facing BIPA claims contended that the plaintiffs' allegations were preempted by the Illinois Workers' Compensation Act, which traditionally serves as the "exclusive" remedy for employees to recover for work-related harm.[94] Relying on *Rosenbach*'s holding regarding "actual damage," Illinois' First District Appellate Court rejected the defendants' argument since the Workers' Compensation Act primarily concerns assertions of actual harm.[95] The Illinois Supreme Court subsequently affirmed, finding that, in contrast to BIPA's unique application to "personal and societal injuries," the Workers' Compensation Act is designed to address only physical and psychological workplace injuries.[96]

88. Doug Meal et al., *7th Cir. Privacy Ruling Could Expand Article III Standing*, LAW360 (Jan. 8, 2021, 4:43 PM), https://www.law360.com/articles/1341578.

89. Celeste Bott, *Biggest Illinois Decisions of 2021*, Law360 (Dec. 22, 2021, 8:54 AM), https://www.law360.com/articles/1449232/biggest-illinois-decisions-of-2021 [hereinafter Bott, *Biggest Illinois Decisions of 2021*].

90. Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1246 (7th Cir. 2021).

91. *Id.* at 1242, 1248–49.

92. Bott, *Biggest Illinois Decisions of 2021*, *supra* note 92.

93. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 822–25.

94. McDonald v. Symphony Bronzeville Park LLC, 174 N.E.3d 578, 580 (Ill. App. Ct. 2020).

95. *Id.* at 586. However, the Illinois Supreme Court did agree in late January 2021 to hear the defendant's appeal of the First District Appellate Court's ruling in *McDonald*. Celeste Bott, *Ill. Justices To Weigh Workers' Comp Effect on BIPA*, LAW360 (Jan. 28, 2021, 6:40 PM), https://www.law360.com/articles/1349597/ill-justices-to-weigh-workers-comp-effect-on-bipa [hereinafter Bott, *Ill. Justices To Weigh Workers' Comp Effect On BIPA*].

96. McDonald v. Symphony Bronzeville Park LLC, 2022 WL 318649, at *9 (Ill. Feb. 3, 2022).

Separately, the presence of labor unions invokes unique legal defenses which, as of early 2022, have accounted for rare BIPA victories for defendants. For example, in a BIPA class action filed by employees of United Airlines who were subject to a collective bargaining agreement (CBA), the defendant removed the action to federal court on the grounds of federal preemption by the Railway Labor Act (RLA).[97] The Seventh Circuit agreed with the defendant's position, finding that—when a dispute is governed by a CBA—"[a] state cannot remove a topic from the union's purview and require direct bargaining between individual workers and management."[98] In reliance on this Seventh Circuit decision, an Illinois appellate court recently held that a labor union member's BIPA claims against her university employer were also preempted by the Labor Management Relations Act (LMRA), thereby opening the door to forced arbitration of BIPA claims brought by union employees.[99]

2. *Biometric Privacy Receives Heightened Attention from Lawmakers*

While Illinois courts continue to grapple with various challenges to BIPA's scope, policymakers are also considering the enactment of biometric privacy legislation on a nationwide scale.[100] On the federal level, U.S. Senators Jeff Merkley and Cory Booker introduced legislation in February 2020 that would temporarily restrict—and eventually govern—the specifics of the government's use of facial recognition technology.[101] Then, approximately six months later, U.S. Senators Jeff Merkley and Bernie Sanders proposed separate legislation attempting to govern private use of biometric data.[102] According to these Senators' offices, their proposed legislation is intended to raise

97. Johnson v. United Airlines, Inc., No. 17 C 08858, 2018 WL 3636556, at *1 (N.D. Ill. July 31, 2018).

98. Miller v. Sw. Airlines Co., 926 F.3d 898, 903 (7th Cir. 2019).

99. Walton v. Roosevelt Univ., No. 1-21-0011, 2022 WL 522760, at *6 (Ill App. Ct. Feb. 22, 2022).

100. *See* Press Release, Jeff Merkley, U.S. Sen. for Or., Merkley, Sanders Introduce Legislation to Put Strict Limits on Corporate Use of Facial Recognition (Aug. 4, 2020), https://www.merkley.senate.gov/news/press-releases/merkley-sanders-introduce-legislation-to-put-strict-limits-on-corporate-use-of-facial-recognition-2020.

101. *See* Press Release, Jeff Merkley, U.S. Sen. For Or., Merkley, Booker Introduce Legislation to Prohibit Irresponsible Government Use of Facial Recognition Technology (Feb. 12, 2020), https://www.merkley.senate.gov/news/press-releases/merkley-booker-introduce-legislation-to-prohibit-irresponsible-government-use-of-facial-recognition-technology-2020.

102. Rebecca Heilweil, *Jeff Merkley and Bernie Sanders Have a Plan to Protect You from Facial Recognition*, VOX (Aug. 4, 2020, 2:00 PM), https://www.vox.com/recode/2020/8/4/21354053/bernie-sanders-jeff-merkley-national-biometric-information-privacy-act.

awareness of the widespread nature of facial recognition technology and would be modeled after BIPA.[103]

There have also been notable state law developments in the biometric privacy space, starting with Illinois and recently expanding to other states. In Illinois, state senators have proposed three amendments to BIPA; however, each amendment has failed to progress past the bill reading stage in the Illinois State Senate.[104] These amendments contain a variety of proposed alterations to BIPA, such as eliminating the private right of action, limiting damage awards for plaintiffs who have not suffered an actual injury, clarifying ambiguous terms in the statute, and ensuring that CBAs are honored.[105] While helpful to illuminate the litany of issues with BIPA, Illinois legislators made it clear that these amendments were proposed as a starting point rather than a final product.[106]

In the Illinois House of Representatives, however, another recently proposed amendment to BIPA made some legislative progress and received strong feedback from both supporters and opponents of the amendment.[107] Namely, in February 2021, House Minority Leader Jim Durkin introduced House Bill (H.B.) 559, which aims to ease the burden placed on small and mid-sized businesses by BIPA.[108] Among other measures, H.B. 559 would amend BIPA by implementing a one-year statute of limitations, providing employers with a 30-day window to "cure" a violation, limiting recoverable damages to the amount of a claimant's actual harm suffered, and allowing businesses to obtain

103. *Id.*

104. *Bill Status of SB3593*, ILL. GEN. ASSEMBLY, https://ilga.gov/legislation/BillStatus.asp?GA=101&SessionID=108&DocTypeID=SB&DocNum=3593 (last visited May 6, 2022); *Bill Status of SB3591*, ILL. GEN. ASSEMBLY, https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3591&GAID=15&DocTypeID=SB&LegId=125459&SessionID=108 (last visited May 6, 2022); *Bill Status of SB3776*, ILL. GEN. ASSEMBLY, https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3776&GAID=15&DocTypeID=SB&LegId=125841&SessionID=108&GA=101 (last visited May 6, 2022).

105. Ahlering et al., Seyfarth Shaw LLP, The Biometric Information Privacy Act in the Era of COVID-19, at 50–52 (June 10, 2022), https://www.seyfarth.com/dir_docs/publications/BIPA_Presentation_June_10_2020-FINAL.pdf.

106. *Id.* at 52.

107. Lauraann Wood, *Illinois Bill Seeks to File Down Biometric Law's Sharp Teeth*, Law360 (Mar. 22, 2021, 7:49 PM), https://www.law360.com/articles/1367329/illinois-bill-seeks-to-file-down-biometric-law-s-sharp-teeth; Grace Barbic, *Judiciary Committee Advances Bill that Edits BIPA Law*, CHI. DAILY L. BULLETIN (Mar. 11, 2021, 11:32 AM), https://www.chicagolawbulletin.com/state-house-advances-bill-revisiting-bipa-20210311.

108. *Illinois House Bill 559*, LEGISCAN, https://legiscan.com/IL/bill/HB0559/2021 (last visited May 6, 2022).

consent through electronic means rather than a written release.[109] Supporters of H.B. 559, pointing to the fact that most BIPA lawsuits are filed against small businesses, label the amendment as one that fairly balances individual privacy rights with the protection of Illinois businesses.[110] Conversely, opponents of the amendment label H.B. 559 as a "'get out of jail free' card" that "gut[s] a gold standard privacy law . . . ."[111] Despite strong support from many business groups, the Illinois House of Representatives declined to read H.B. 559 prior to its third reading deadline, which effectively halted the proposal for the time being.[112]

Outside of Illinois, state lawmakers in New York have proposed three biometric privacy bills since 2018, with the most recent bill being proposed in January 2021.[113] The newest bill, Assembly Bill 27, mirrors BIPA in a myriad of ways by including a written policy requirement, a written notification component, and a provision governing the collection, retention, and dissemination of biometric data.[114] Assembly Bill 27 also contains an identical damages model to that of BIPA, i.e., $1,000 per negligent violation and $5,000 per each reckless or intentional violation.[115] Assembly Bill 27 is currently being assessed by New York's Consumer Affairs and Protection Committee.[116]

While New York legislators are still considering a biometric privacy law on the state level, municipal lawmakers in New York City succeeded in passing their own ordinance focused on biometric identifiers.[117] This law, which took effect in July 2021, mirrors BIPA in that it generally regulates the "'collection, use, and retention' of biometric identifier information."[118] Though the New York City ordinance is

109. Barbic, *supra* note 107; *see also Bill Status of HB0559,* ILL. GEN. ASSEMBLY, https://www.ilga.gov/legislation/BillStatus.asp?DocNum=559&GAID=16&DocTypeID=HB&SessionID=110&GA=102 (last visited May 6, 2022).

110. Barbic, *supra* note 107.

111. Wood, *supra* note 107.

112. Stefan Dandelles & Jean Liu, *The Illinois Biometric Information Privacy Act Remains Firm as Attempt at Reform Was Halted*, KAUFMAN DOLOWICH VOLUCK NEWS & RES. (Apr. 27, 2021), https://www.kdvlaw.com/news-resources/the-illinois-biometric-information-privacy-act-remains-firm-as-attempt-at-reform-was-halted/.

113. Grande, *supra* note 74.

114. *See generally* Assembly B. 27, 2021-2022 Leg., Reg. Sess. (N.Y. 2021).

115. *Id.*

116. *Assembly Bill A27,* THE N.Y. ST. SENATE, https://www.nysenate.gov/legislation/bills/2021/A27 (last visited May 21, 2022).

117. Marian A. Waldmann Agarwal & Linnea Dale Pittman, *Open for Business: Are You Prepared for New York City's Biometric Identifier Information Law?*, MORRISON FOERSTER (June 23, 2021), https://www.mofo.com/resources/insights/210623-biometric-identifier-information-law.html.

118. *Id.*

more limited since it only covers "commercial establishments," the ordinance still maintains a private right of action allowing for damages of $500 per negligent violation and $5,000 per intentional or reckless violation.[119] Interestingly, however, this ordinance allows defendants a chance to "cure" the violation within 30 days after the filing of the action.[120]

III. Analysis

BIPA is a well-intentioned law and at the time of its passage, it was positioned to effectively regulate the biometric practices of large data collectors like Pay By Touch, the company whose bankruptcy fueled passage of the law.[121] However, in the last decade, biometric technology has become substantially more advanced and popular among businesses, both small and large.[122] In light of these technological advancements, as well as recent case law developments, it is becoming evident that BIPA has been stretched beyond its original intended scope. The broad and oftentimes ambiguous language of BIPA—combined with its unique private right of action, nonexistent cap on damages, and unclear statute of limitations[123]—made the law a springboard for a slew of "cookie-cutter" class actions.[124]

BIPA class actions are one the hottest filing trends in the country, and the "[l]itigation [r]ollercoaster [d]riven by [BIPA]" is not expected to slow down anytime soon, especially given the Illinois Supreme Court's holding in *Rosenbach*.[125] To that end, it is also

119. N.Y.C. Admin. Code §§ 22-1202–03 (2021).

120. N.Y.C. Admin. Code § 22-1203.

121. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 819.

122. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. Irvine L. Rev. 107, 109 (2019). Since the passage of BIPA, employers have increasingly used biometrics—namely, biometric timekeeping software—to curb the "buddy punching" practice wherein employees clock in for their co-workers before they arrive at work. *Id.*; *see also* Peter Tsai, *Data Snapshot: Biometrics in the Workplace Commonplace, but Are They Secure?*, Spiceworks (Mar. 12, 2018), https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure. According to one survey, sixty-two percent of companies used biometric technology in 2018, and by 2020, that number would rise to eighty-six percent. *Id.* Fingerprint scanning is also the most popular biometric technology in the workplace, with fifty-seven percent of businesses reporting their use of such technology as of 2018. *Id.*

123. In September 2021, an Illinois appellate court held that BIPA claims under Sections 15(c) and (d) are subject to a one-year statute of limitations, while claims under Sections 15(a), (b), and (e) are subject to Illinois's catch-all five-year limitations period. Tims v. Black Horse Carriers, Inc., 184 N.E.3d 466, 473 (Ill. App. 2021). However, the Illinois Supreme Court granted the defendant's leave to appeal, so the state's supreme court may clarify BIPA's applicable statute of limitations in 2022. *Id.* at 468.

124. Maatman, Jr. et al., *Copy-Cat Class Actions*, *supra* note 15.

125. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 819, 825.

important to note that, while some BIPA class actions have been filed against large data collectors,[126] the majority of companies facing new BIPA suits are small-to-mid-size employers that use biometric time-keeping software.[127] Though the statute does offer certain compliance measures that businesses should take,[128] these proactive measures can be costly and confusing for large and small businesses alike. Unless BIPA is amended or otherwise preempted by federal legislation, businesses of all sizes will be forced to continue expending significant financial resources to defend this *Rosenbach*-driven flood of complex class actions.[129]

A. Legal Questions Stemming from Rosenbach

Though the Illinois Supreme Court did issue a unanimous decision in *Rosenbach*, this ruling and its progeny have nevertheless been clouded in debate over a number of legal issues.[130] In terms of the decision itself, one could begin by questioning the Illinois Supreme Court's approach in interpreting the phrase "aggrieved person." Namely, the Supreme Court used *Merriam-Webster*'s definition citing "denial of legal rights" to support its conclusion that an "aggrieved person" need not suffer actual harm to bring suit under BIPA.[131] Conversely, the Illinois appellate court that considered this question under the same statutory framework used a *Black's Law Dictionary* definition citing the phrase "adversely affected" to come to the opposite conclusion of the Illinois Supreme Court.[132] These conflicting interpretations of the law are just one example of how knowledgeable legal minds can differ as to the key components of BIPA.

With respect to the *Rosenbach* court's primary holding regarding what constitutes an "aggrieved individual," several federal courts have

126. *See, e.g.*, *Facebook Biometric Information Privacy Litigation*, GILARDI & CO. LLC, http://www.facebookbipaclassaction.com/; *see also* Molly Stubbs, *Clearview AI Faces Fourth Lawsuit Alleging Biometric Privacy Violations*, EXPERT INST. (June 25, 2020), https://www.expertinstitute.com/resources/insights/clearview-ai-faces-fourth-lawsuit-alleging-biometric-privacy-violations/.

127. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 821–22; *see also* Celeste Bott, *Breaking Down Illinois' Biometric Privacy Litigation Boom*, Law360 (Apr. 27, 2020, 8:15 PM), https://www.law360.com/articles/1252596/breaking-down-illinois-biometric-privacy-litigation-boom.

128. 740 ILL. COMP. STAT. 14/5(a)–(e).

129. Ahlering et al., Seyfarth Shaw LLP, *supra* note 105, at 25–27, 46.

130. *See generally* Michael C. Andolina et al., *Emerging Issues and Ambiguities under Illinois' Biometric Information Privacy Act*, WESTLAW THOMSON REUTERS (May 21, 2020), https://www.sidley.com/-/media/publications/westlaw-journal_emerging-issues-and-ambiguities-under-illinois-biometric-information-privacy-act.pdf?la=EN.

131. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1205 (Ill. 2019).

132. *Id.* at 129.

also considered the same question and rendered contrary decisions. For instance, prior to the issuance of the *Rosenbach* decision, federal courts in Illinois[133] and New York[134] dismissed BIPA class actions on the basis that bare procedural violations could not warrant Article III standing in light of the U.S. Supreme Court's holding in *Spokeo v. Robins*.[135] Despite the fact that these interpretations of BIPA have since been overruled by *Rosenbach*, they nevertheless underscore the perspective that varying judicial interpretations may not be the central issue in clarifying the contours of BIPA; rather, the bigger problem may be the language of BIPA itself.

B. Reconciling BIPA with Federal and State Standing Principles

In connection with the aforementioned questions concerning what it means to be aggrieved under BIPA, the *Rosenbach* holding also initiated a series of ongoing debates concerning the applicability of federal and state standing principles to BIPA claims.[136] On the state level, *Rosenbach* eliminated the need to analyze BIPA claims for "actual harm," thereby treating the law as a strict liability statute.[137] The Illinois Supreme Court's decision also spurred hotly-contested questions concerning the interplay between state and federal jurisdiction over BIPA claims.[138] These subsequent effects of *Rosenbach* have led different jurisdictions to issue contradictory decisions on which types of BIPA claims warrant state or federal standing[139] and thus, help to further illuminate the ambiguities of the statute itself.

1. Rosenbach Effectively Made BIPA a Strict Liability Statute

As a threshold matter, it is fair to assume that *Rosenbach* aligned with the liberal standing requirements set forth by the Illinois Su-

133. McCollough v. Smarte Carte, Inc., No. 16-C-03777, 2016 WL 4077108, at *4 (N.D. Ill. Aug. 1, 2016).

134. Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 502, 513 (S.D.N.Y. 2017).

135. Spokeo v. Robins, 578 U.S. 330, 342 (2016) (holding that the plaintiff did not satisfy Article III's injury-in-fact requirement because he alleged mere procedural violations of the Fair Credit Reporting Act).

136. *See generally* Andolina et al., *supra* note 130.

137. MATT FLEISCHER-BLACK, BIG QUESTIONS FOR BIPA CASE LAW IN 2021 2 (2021), https://lewisbrisbois.com/assets/uploads/files/CSLR_Big_Questions_for_BIPA_Case_Law_in_2021.pdf.

138. Teresa Milano, *The BIPA Litigation Landscape and What Lies Ahead*, WOODRUFF SAWYER INSIGHTS (Apr. 1, 2021), https://woodruffsawyer.com/cyber-liability/bipa-litigation-landscape/; *see generally* Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).

139. Meal et al., *supra* note 88.

preme Court.[140] The state merely requires that a plaintiff's injury be distinct, fairly traceable to the defendant's conduct, and likely to be addressed by the relief sought.[141] In this sense, specific claims that an entity, for example, failed to follow BIPA's retention or written policy requirements can easily meet this low standard in light of *Rosenbach*'s elimination of any "actual harm" requirement.

However, the Illinois Supreme Court in *Rosenbach* went further by effectively allowing BIPA to be a strict liability statute. Strict liability is typically applied by Illinois courts in one of two scenarios: (1) when a defendant introduces an unreasonably dangerous product to the market; or (2) "when a defendant engages in ultrahazardous or abnormally dangerous activity . . . ."[142] Illinois courts are usually reluctant to label an activity as "ultrahazardous."[143] "The essential question [here] is whether the risk created is so unusual . . . as to justify the imposition of strict liability even though the activity is carried on with all reasonable care."[144] Many courts—as well as the *Restatement of Torts*[145]—also weigh public policy considerations[146] and assess legislative intent[147] when determining whether to impose strict liability under a certain statute.

---

140. In Illinois, standing can be shown by demonstrating some injury to a legally cognizable interest. Greer v. Ill. Hous. Dev. Auth., 524 N.E.2d 561, 574–75 (Ill. 1988). The claimed injury, whether actual or threatened, must be distinct and palpable, fairly traceable to the defendant's actions, and substantially likely to be prevented or redressed by the grant of the relief requested. *Id.*

141. *Id.*

142. Miller v. Civil Constructors, Inc., 615 N.E.2d 239, 242 (Ill. App. Ct. 1995).

143. *See id.* at 244–45 (holding that the use of firearms on a quarry's shooting range was not ultrahazardous activity); *see also In* re Chi. Flood Litig., 680 N.E.2d 265, 279–80 (Ill. 1997) (reasoning that pile driving under a bridge that caused a breach in the tunnel was not ultrahazardous activity).

144. *Miller*, 615 N.E.2d at 244.

145. According to the Restatement of Torts:

> In determining whether an activity is abnormally dangerous, the following factors are to be considered: (a) existence of a high degree of risk of some harm to the person, land or chattels of others; (b) likelihood that the harm that results from it will be great; (c) inability to eliminate the risk by the exercise of reasonable care; (d) extent to which the activity is not a matter of common usage; (e) inappropriateness of the activity to the place where it is carried on; and (f) *extent to which its value to the community is outweighed by its dangerous attributes*.

RESTATEMENT (SECOND) OF TORTS § 520 (AM. LAW INST. 1965) (emphasis added).

146. *See Miller*, 615 N.E.2d at 244; *see also* Cassidy v. China Vitamins, LLC, 120 N.E.3d 959, 965–67 (Ill. 2018).

147. When assessing whether the General Assembly intended to impose strict liability upon defendants who violate a certain law, Illinois courts look to the plain language of the law and whether that statute, read as a whole, evinces such intent. Abbasi v. Paraskevoulakos, 718 N.E.2d 181, 186 (Ill. 1999).

As applied to BIPA, reasonable consideration of these standards demonstrates that BIPA is not an appropriate strict liability statute under Illinois law. Specifically, since BIPA claims do not involve the sale of certain products, it can only be deemed a strict liability law if violators of BIPA are engaged in "ultrahazardous or abnormally dangerous activity."[148] This leads to an important distinction in BIPA cases; that is, the distinction between cases against large data collectors and those against employers using biometric timekeeping software. As mentioned in Part II,[149] biometric timeclocks immediately discard an employee's fingerprint scan and store only anonymous templates of an employee's unique fingerprint characteristics.[150] Therefore, even in the event of a breach, no usable personal information is revealed.[151]

In acknowledgement of this fact, an employer using biometric timekeeping software cannot reasonably be judged as engaging in "ultrahazardous or abnormally dangerous activity" because no one's personal privacy is truly at risk. Allowing plaintiffs to hold employers strictly liable for mere failures to comply with BIPA contradicts BIPA's legislative intent[152] and harms the judicial system by wasting judicial resources on cases in which no plaintiff was at risk of suffering an actual injury. Moreover, the language in BIPA cannot be plainly read as suggesting that the Illinois General Assembly intended for the law to hold defendants strictly liable, especially in light of other recognized strict liability statutes in Illinois.[153] The Illinois Supreme Court's interpretation of BIPA as a strict liability law also harms businesses by forcing them to defend high-stakes, expensive class action litigation for simply failing to comply with procedural requirements rather than for actually putting an individual's privacy in harm's way.

Importantly, this is not to say that all BIPA actions fail under this strict liability framework. To the contrary, the high-profile class actions against Facebook[154] and Clearview AI[155] are both aimed at pro-

148. Miller, 615 N.E.2d at 242.

149. *See infra* Part II.

150. *How Do Fingerprint Biometric Time Clocks Work?*, *supra* note 25.

151. *Id.*

152. *See generally* 740 ILL. COMP. STAT. 14/5. Specifically, BIPA's section dedicated to legislative findings and intent notes that "[a]n overwhelming majority of members of the public are weary of the use of biometrics *when such information is tied to finances and other personal information*." *Id.* § 5(d) (emphasis added).

153. *See, e.g.*, The Illinois Consignment of Art Act, 815 ILL. COMP. STAT. 320/2(5) (1985). The Act explicitly provides that "an art dealer shall be strictly liable for the loss of or damage to the work of fine art . . . ." *Id.*

154. *Facebook Biometric Information Privacy Litigation*, *supra* note 126.

155. Stubbs, *supra* note 126.

tecting individuals' data, i.e., scans of facial geometry that carry actual value in terms of personal privacy. However, when considering that the bulk of recent BIPA class actions were filed against companies for using biometric timekeeping software,[156] it becomes clear that the Illinois Supreme Court's decision in *Rosenbach* has extended BIPA beyond its intended scope by imposing on employers what essentially amounts to strict liability for mere procedural violations which carry little risk of actual harm to personal privacy.

2. Bryant and the Troublesome Issue of BIPA "Claim-Splitting"

With respect to federal court standing, another ongoing judicial split of interpretation further illuminates the broad nature of BIPA and *Rosenbach*'s problematic ramifications. Namely, the Seventh Circuit in *Bryant* found that claims under § 15(b) of BIPA warranted Article III standing, while claims regarding BIPA's public disclosure requirements under § 15(a) were not sufficiently concrete and particularized to warrant Article III standing.[157] As a result of the Seventh Circuit's somewhat surprising distinction offered in *Bryant*, Illinois courts handling BIPA class actions are now sorting through a number of petitions for removal to federal court under a framework that is not entirely clear.[158]

The questionable distinction set forth in *Bryant* has led to even more contentious BIPA standing debates in both the Seventh Circuit as well as other jurisdictions. To complicate matters even further, both the Second[159] and Ninth[160] Circuits have also weighed in on whether claims under § 15(a) of BIPA warrant standing in federal court. These

156. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 821–22.

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

158. *See, e.g.*, Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1247–49 (7th Cir. 2021) (affirming the district court's grant of the plaintiffs' motion to remand, thereby reasoning that the plaintiffs' claims were not sufficient to warrant standing in federal court); Roberson v. Maestro Consulting Servs., LLC, No. 20-CV-00895-NJR, 2021 WL 1017127, at *2 (S.D. Ill. Mar. 17, 2021) (staying an action in which the defendant initially removed the case to federal court, followed by the plaintiffs' failed attempt to remand the action to state court); *see also* Meal et al., *supra* note 88.

159. Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 16 (2d Cir. 2017) (holding that the plaintiffs' § 15(a) BIPA claim was not sufficient to warrant Article III standing because the plaintiffs did not allege that the defendant failed to implement an adequate retention schedule nor that it did not destroy the plaintiffs' biometric data within a satisfactory period, thus rendering the plaintiffs' claim "a bare procedural violation").

160. Patel v. Facebook, Inc., 932 F.3d 1264, 1274 (9th Cir. 2019) (holding that, "[b]ecause the privacy right protected by BIPA is the right not to be subject to the collection and use of . . . biometric data," the plaintiffs' allegations of procedural violations under §§ 15(a) and 15(b) of BIPA were sufficient to warrant Article III standing pursuant to the Illinois Supreme Court's ruling in *Rosenbach*).

cases were all initiated under different circumstances, and in light of BIPA's ambiguous nature with respect to "actual damage" and what it means to be "aggrieved," the Second and Ninth Circuits' interpretations differed from the Seventh Circuit's perspective in *Bryant*. Consequently, "as matters now stand the circuit courts have enunciated three different, and mutually inconsistent, standards by which § 15(a) claims are to be evaluated for Article III purposes."[161]

C. A Plethora of New Defense Theories Further Highlights BIPA's Ambiguities

A brief analysis of the flurry of new defense theories being offered by defendants facing BIPA class actions also helps highlight the many ambiguities of the statute. First, BIPA defendants have raised several different preemption arguments with varying success.[162] In one sense, these arguments are simply a reflection of companies testing the contours of BIPA in light of Southwest Airlines' successful preemption defense in *Miller*.[163] However, from a statutory perspective, they also reflect the unclear language of BIPA. For example, RLA preemption is generally accepted as appropriate where a union plaintiff's claims fall within their CBA[164] (as was the case in *Miller*[165] and *Croom*[166]). BIPA, however, makes no mention of the law's relationship to CBAs, thereby forcing courts and parties to waste unnecessary time and resources litigating these issues.

In addition to preemption, defendants have also begun trying to evade BIPA liability by challenging what types of entities are covered under BIPA. These arguments have been offered by a wide range of

161. Meal et al., *supra* note 88.

162. While the Illinois appellate court did reject the defendant's argument in McDonald that BIPA is preempted by the Illinois Workers' Compensation Act, the Illinois Supreme Court agreed to hear the defendant's appeal. Bott, *Ill. Justices To Weigh Workers' Comp Effect On BIPA*, *supra* note 95. The Northern District of Illinois also struck down an affirmative defense contending that various federal public health statutes preempted BIPA. Crumpton v. Octapharma Plasma, Inc., 513 F. Supp. 3d 1006, 1013–14 (N.D. Ill. 2021). However, two airlines have now been successful in arguing for federal preemption under the RLA. *See* Miller v. Sw. Airlines Co., 926 F.3d 898, 903 (7th Cir. 2019); *see also* Crooms v. Sw. Airlines Co., 459 F. Supp. 3d 1041, 1050–51 (N.D. Ill. 2020) (granting the defendant's motion to dismiss on the basis that the union plaintiffs' BIPA claims are preempted by the RLA and thus should be determined by the adjustment board).

163. *See generally Miller*, 926 F.3d at 898.

164. *See* Hawaiian Airlines, Inc. v. Norris, 512 U.S. 246, 246–47 (1994); *see also* 115 ILL. COMP. STAT. 5/10(b) (1985).

165. *Miller*, 926 F.3d at 904.

166. *Crooms*, 459 F.3d at 1048.

companies, from third-party service providers[167] to parent corporations[168] and health care providers.[169] Regardless of the type of business involved, such defenses generally follow a similar line of reasoning, i.e., that the entity is not covered by BIPA due to the statute's lack of clarifying text. For instance, in a ruling concerning a health care entity's defense that it was exempt from BIPA, an Illinois federal court noted that, while BIPA explicitly "does not apply to 'information captured from a patient in a health care setting,'" the statute failed to define both "health care" and "patient."[170] The court accordingly had to uphold the defendant's affirmative defense even though it was not a traditional healthcare provider but rather a plasma donation center.[171] Once again, BIPA's ambiguities forced the court to interpret broad terms and issue caselaw precedent that is sure to be challenged and relitigated in future disputes.

These examples are by no means exhaustive, as Illinois courts are also currently assessing proposed defenses concerning BIPA's unclear statute of limitations,[172] cap (or lack thereof) on damages,[173] and definition of what constitutes "possession" of a "faceprint" or "voiceprint,"[174] to name just a few. This sense of uncertainty surrounding nearly every important aspect of the statute shows that, while the Illinois General Assembly likely sought to implement a relevant, practical statute in 2008, the advances in biometric technology and the types of employers using biometrics have rendered certain

167. *See, e.g.*, Complaint, Ragsdale v. Amazon Web Servs., Inc., No. 2019-ch-13251 (Ill. Cir. Ct. Nov. 15, 2019); *see also* Heard v. Becton, Dickinson & Co., 440 F. Supp. 3d 960 (N.D. Ill. 2020).

168. *See, e.g.*, Wordlaw v. Enterprise Leasing Co., No. 20-CV-3200, 2020 WL 7490414 (N.D. Ill. Dec. 21, 2020).

169. *See, e.g.*, Crumpton v. Octapharma Plasma, Inc., 513 F. Supp. 3d 1006 (N.D. Ill. 2021).

170. *Id.* at 1015–16.

171. *Id.* at 1016–17.

172. *See, e.g.*, Tims v. Black Horse Carriers, No. 2019-CH-03522, 2020 WL 11885555 (Ill. Cir. Ct. Feb. 26, 2020). An Illinois appellate court issued a ruling on BIPA's applicable limitations period in September 2021. *See* Tims v. Black Horse Carriers, Inc., 184 N.E.3d 466, 473 (Ill. App. Ct. 2021). But in January 2022, the Illinois Supreme Court granted the defendant's petition for leave to appeal. *See* Tims v. Black Horse Carriers, Inc., 184 N.E.3d 1029 (Ill. 2022).

173. *See, e.g.*, Cothron v. White Castle Sys., Inc., 477 F. Supp. 3d 723 (N.D. Ill. 2020). The Seventh Circuit ruled on this case in December 2021 but refused to decide on the issue of when a BIPA claim accrues, instead certifying this question for review by the Illinois Supreme Court. *See* Cothron v. White Castle System, Inc., 20 F.4th 1156 (7th Cir. 2021).

174. *See, e.g.*, Hazlitt v. Apple Inc., 543 F. Supp. 3d 643, 646 (S.D. Ill. 2021); *see also* Hannah Schaller et al., *BIPA Litigation in 2021: Where We've Been & Where We're Headed*, ZwillGen Blog (Aug. 18, 2021), https://www.zwillgen.com/litigation/bipa-litigation-2021/; *see also* Frances Floriano Goins & Michael Hoenig, *Illinois Federal Court Rules Apple May Be "In Possession" of Biometric Data Stored on User Devices*, JD Supra (June 23, 2021), https://www.jdsupra.com/legalnews/illinois-federal-court-rules-apple-may-1793870/.

components of the statute practically inapplicable. Unless some action is taken to curb or otherwise alter these troublesome aspects of BIPA, businesses will be forced to keep litigating complicated class actions under an umbrella of uncertain and constantly evolving caselaw.

D. Legislative Measures to Cure BIPA's Gray Areas

In light of the current state of BIPA caselaw, it seems very unlikely that all federal and state courts will come to similar conclusions with respect to ongoing litigation over the myriad of aforementioned gray areas of BIPA. While the current BIPA class action landscape is at least partially due to the Illinois Supreme Court's ruling in *Rosenbach*,[175] successfully overturning this case would likely be a futile effort, as the Supreme Court's holding was unanimous[176] and has since been followed by a litany of courts both in and outside of Illinois.[177] Thus, some type of legislative measure would be the most appropriate and effective way to fix BIPA's practical issues. Namely, rather than pursuing a preemptive federal biometric privacy statute (which, based on proposed federal legislation, would largely be based on BIPA anyway[178]), an amendment by the Illinois General Assembly could properly address BIPA's most pressing statutory issues while also upholding its respectable goal of protecting individual privacy.

For a legislative amendment to effectively protect businesses—like those only facing suit for using biometric timekeeping software—from meritless BIPA litigation, it must clearly address a number of the statute's current ambiguities. To determine the correct approach for such an important endeavor, a good starting point is the amendments that have already been proposed by members of the Illinois General Assembly. Though only H.B. 559 has successfully passed the committee stage of the legislative process,[179] the four proposed amendments have collectively identified several vital aspects of the statute that must be adjusted. For instance, these proposed amendments highlighted

175. Maatman, Jr. et al., *supra* note 47; *see also* Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 825.

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

177. *See, e.g.*, Rottner v. Palm Beach Tan, Inc., No. 1-18-0691, 2019 WL 1049107, at *2–3 (Ill. App. Ct. Mar. 4, 2019) (reversing the circuit court's grant of the defendant's motion to dismiss in light of the *Rosenbach* decision); *see also* Patel v. Facebook, Inc., 932 F.3d 1264, 1273–74 (9th Cir. 2019) (concluding that, pursuant to the *Rosenbach* ruling, the plaintiff's claims of procedural violations of BIPA were sufficient to warrant Article III standing).

178. Heilweil, *supra* note 102.

179. Barbic, *supra* note 107; *see also Bill Status of HB0559*, *supra* note 109; Charles N. Insler, *Will the Proposed Amendments to the Biometric Information Privacy Act (BIPA) Be Retroactive?*, ABA (Apr. 30, 2021), https://www.americanbar.org/groups/business_law/publications/blt/2021/05/bipa/.

BIPA's unclear (and oftentimes excessive) damages structure, opportunity for plaintiffs to file suit without suffering actual harm, relationship to CBAs, and vague definitions of key terms.[180]

Using these amendments as a springboard for BIPA reconstruction, an amendment should be proposed that clearly and specifically introduces the following elements into BIPA: (1) a three-year statute of limitations; (2) clarification that, when union member plaintiffs bound by a CBA bring suit under the law, their claims are to be decided by an adjustment board; (3) clarification that the statute does not cover parent corporations or third-party service providers who have no direct role in the collection, storage, or regulation of biometric data; (4) further explanation of the types of data and technology covered by the law in light of technological developments, which should include clearly defining the terms "voiceprint," "face geometry," and "violation," among others;[181] (5) a revised damages structure still allowing for $1,000 for negligent violations and $5,000 for intentional or reckless violations, with the caveat that repeated procedural violations do not count as separate violations; and, most importantly, (6) a revised private right of action that allows only plaintiffs who suffer actual harm to recover liquidated damages in a civil lawsuit, leaving regulatory enforcement for procedural violations up to the Illinois Department of Labor.

Collectively, these elements seek to balance an individual's right to privacy with the fact that BIPA, as currently constructed, is being utilized by many plaintiffs to punish businesses for procedural violations that do not place anyone's privacy at risk. This plaintiff-friendly advantage of BIPA could be remedied by the aforementioned revisions to the statute's private right of action, which would still allow plaintiffs such as those in the record-setting Facebook case to secure substantial settlements, while simultaneously limiting the exposure of companies who are presently being sued for procedural violations that do not place individual privacy at risk. Notably, this Comment's proposed amendment does not go as far as H.B. 559, which allows for a longer statute of limitations and denies employers the right to cure violations that result in actual harm, thereby striking a middle ground that aims to secure bipartisan support for the amendment. The BIPA playing field must be evened out, and an amendment of the nature proposed in this Comment is the most direct and efficient means of statutory reform that still keeps BIPA's original purpose intact.

180. Ahlering et al., *supra* note 105, at 50–52.
181. Andolina et al., *supra* note 130.

IV. Impact

In light of BIPA's numerous ambiguities and the slew of class action litigation being filed against businesses for mere procedural violations, the statute must be amended to curb this punitive trend. Without amendment or preemption by federal statute, this dangerous class action filing trend will continue harming businesses without disruption. Moreover, the COVID-19 pandemic[182] further complicates the future of the statute by forcing employers to use more technology than ever,[183] which in turn involves more biometric data collection.[184] In sum, a commonsense amendment to the statute that adjusts only the most damaging aspects of the statute would allow continued protection of individual privacy while simultaneously easing the burden on Illinois employers who use biometric technology for legitimate business reasons.

A. Without Amendment, BIPA Remains a Broad, Punitive Statute

If the Illinois General Assembly were to allow BIPA to remain in place as currently constructed, businesses of all sizes and industries will be forced to comply with—and oftentimes defend against—complex class actions brought under BIPA. In terms of litigation, class actions of any nature are typically very expensive to defend against, as corporations spent $2.64 billion on defending class actions in 2019 alone.[185] BIPA class actions can be especially costly to defend against, given that defendants usually must engage in extensive discovery to

182. Coronavirus disease 2019 ("COVID-19") is a new strain of communicable virus that was not previously seen in human beings until December 2019. *About COVID-19*, CDC (Nov. 4, 2021), https://www.cdc.gov/coronavirus/2019-ncov/cdcresponse/about-COVID-19.html. COVID-19 quickly spread throughout the world, and as of April 2022, the United States alone accounted for nearly eighty-three million cases and over one million deaths. *United States Coronavirus Cases*, Worldometer (May 9, 2022), https://www.worldometers.info/coronavirus/country/us/. The COVID-19 pandemic has, among other more devastating effects, substantially altered the economy by forcing millions to lose their jobs and pushing many employees to work from home. *Coronavirus: How the World of Work May Change Forever*, BBC Worklife, https://www.bbc.com/worklife/article/20201023-coronavirus-how-will-the-pandemic-change-the-way-we-work (last visited May 8, 2022).

183. *How COVID-19 Has Pushed Companies over the Technology Tipping Point—and Transformed Business Forever*, McKinsey & Co. (Oct. 5, 2020), https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#.

184. Nicole Lewis, *Biometric Technology Use During the Pandemic Can Pose Ethical Problems*, Soc'y for Hum. Res. Mgmt (Nov. 9, 2020), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/biometric-technology-use-during-pandemic-can-pose-ethical-problems.aspx.

185. Carlton Fields, 2020 Carlton Fields Class Action Survey 4 (2020), https://classactionsurvey.com/pdf/2020-class-action-survey.pdf.

effectively oppose class certifications and obtain expert witnesses to testify as to the biometric technology involved.[186] To heighten a BIPA defendant's potential financial exposure even further, an Illinois appellate court recently held that claims under Sections 15(a) and (b) accrue upon "*each and every* capture and use" of a plaintiff's biometric information.[187]

In response to these high costs, the Illinois Supreme Court suggested that businesses should simply comply with the law, which the court labeled an easy endeavor with minimal costs compared to potential financial exposure under BIPA.[188] However, compliance with the law is frankly not as simple as the court implies. In fact, both large and small companies face unique challenges in complying with BIPA's various requirements. For example, large employers who have consistently used biometric technology over a long period of time may struggle to obtain written consent from every individual who utilized the company's biometric technology over an unclear period of time (due to the statute's unclear statute of limitations). Conversely, small businesses that lack the requisite legal resources and technical expertise to comply with BIPA may struggle to understand the various contours of the law and to implement adequate data security measures. Suffice to say, BIPA compliance is a technical, time-consuming process that cannot be easily completed without significant resources and expertise.

Furthermore, the increasing use of technology due to the COVID-19 pandemic[189] makes concerns over the scope of BIPA even more prominent. To heighten the stakes even further, many expect the pandemic to change the nature of work forever, leading to more remote work opportunities and an increased reliance on technology.[190] This suggests that employers of the future will have to be even more careful with how they collect and store biometric data, leading to new

186. Ahlering, et al., *supra* note 105, at 25.

187. Watson v. Legacy Healthcare Fin. Servs., LLC, No. 1-21-0279, 2021 WL 5917935, at *5 (Ill App. Ct. Dec. 15, 2021) (emphasis added). Should the principle announced in *Watson* be adopted by the Illinois Supreme Court, BIPA defendants, and particularly employers requiring their employees to clock in and out using their biometric identifiers, would potentially be liable for enormous damage amounts.

188. Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1207 (Ill. 2019). According to the Illinois Supreme Court:

> Compliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced.

Id.

189. *How COVID-19 Has Pushed Companies over the Technology Tipping Point—and Transformed Business Forever*, *supra* note 183.

190. *Coronavirus: How the World of Work May Change Forever*, *supra* note 182.

compliance challenges. A prime example of this is a recent BIPA class action filed against Amazon claiming that the e-commerce giant improperly collected workers' facial geometry, retinas, and irises via its daily COVID-19 temperature checks.[191] Amazon filed a motion to dismiss arguing that it did not "collect" or "possess" the plaintiff's biometric data, but the court denied the motion pursuant to its broad reading of these statutory terms.[192] While the Amazon case is far from resolved, it is safe to assume that this is just the first of many BIPA-related issues to stem from the COVID-19 pandemic.

B. A Preview into a Post-Amendment BIPA Landscape

While the future BIPA landscape remains dark for virtually all Illinois businesses, a comprehensive amendment addressing BIPA's most pressing issues could reverse this trend and even the playing field for businesses. The amendment proposed by this Comment would lift the burden of defending complex class action litigation off most employers using biometric timekeeping software in good faith. Importantly, it would also allow most of BIPA's existing compliance measures to remain in place – including heightened penalties for egregious violators of the law. In contrast to the current BIPA landscape, this situation would fairly balance the interests of all involved parties and reduce the punitive nature of the statute.

Furthermore, this type of legislative measure would further public policies that are valued by businesses, the court system, and society as a whole. Namely, the judicial system has long been concerned with conserving judicial resources,[193] promoting efficient litigation,[194] and protecting businesses.[195] The current version of BIPA, however, leaves many key issues unclarified, thereby forcing courts to continually reassess complex questions of statutory interpretation and attempt to remedy circuit splits that may have no clear answer. Businesses will clearly benefit from a restructured BIPA statute in the form of reduced liabil-

191. Order, Naughton v. Amazon.com, Inc., No. 20-cv-06485, at *1–2 (N.D. Ill. Jan. 3, 2022); *see also* Jenny Colgate, *Amazon Sued for Another BIPA Violation, This Time Related to COVID-19 Employee Scans*, JD SUPRA (Oct. 19, 2020), https://www.jdsupra.com/legalnews/amazon-sued-for-another-bipa-violation-88723/.

192. *Naughton*, 2022 WL 19324, at *3–4.

193. Rivers v. Walt Disney Co., 980 F. Supp. 1358, 1362 (C.D. Cal. 1997) (noting that most courts agree to stay preliminary proceedings "because of the judicial resources that are conserved").

194. Farshad Ghodoosi, *The Concept of Public Policy in Law: Revisiting the Role of the Public Policy Doctrine in the Enforcement of Private Legal Arrangements*, 94 NEB. L. REV. 685, 708 (2016).

195. South Dakota v. Wayfair, Inc., 138 S.Ct. 2080, 2104 (2018) (voicing concerns that a tax law penalizing internet sellers would disproportionately impact small businesses).

ity and litigation costs, as will society as a whole. To that end, society must balance the protection of privacy rights with protecting businesses from these cookie-cutter cases with excessive damage models. This Comment's proposed amendment adequately balances these issues, thereby finding a middle ground that protects privacy, promotes judicial efficiency, and clarifies what is expected of employers with respect to the collection of biometric data.

V. Conclusion

BIPA is a well-intentioned law, but in the decade-plus since its enactment, plaintiffs' class action attorneys have primarily used BIPA as a mechanism to punish businesses for procedural violations. The biggest driving force in this trend was the Illinois Supreme Court's ruling in *Rosenbach*, which held that plaintiffs need not suffer actual harm to file suit under BIPA.[196] While this decision opened the door to a flood of new lawsuits based on procedural violations, BIPA's class action filing explosion is also grounded in an even more basic source: the language of BIPA itself. BIPA's numerous textual ambiguities have led to a litany of unanswered legal questions, further increasing the costs of defending a BIPA class action.[197]

This slew of BIPA class action filings by unharmed plaintiffs is troubling for several reasons. Specifically, BIPA contains an uncapped damages model allowing plaintiffs to request between $1,000 and $5,000 per each violation of the law.[198] Given that most BIPA cases are filed against employers using biometric timekeeping systems,[199] the simple fact is that these businesses are being penalized for technical violations involving biometric templates that cannot even be used by unauthorized third parties.[200] Once hit with this type of lawsuit, defendants must not only bear the high costs of class action litigation, but they must also litigate the myriad of open legal questions concerning BIPA's textual ambiguities. While a select few of these questions have been concretely answered, courts continue to grapple with how to properly interpret BIPA, with courts still split on important issues such as standing and preemption defenses.[201]

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

197. *See generally* Andolina et al., *supra* note 130.

198. 740 Ill. Comp. Stat. 14/20 .

199. Insler, *How to Ride the Litigation Rollercoaster*, *supra* note 2, at 821–22.

200. *How Do Fingerprint Biometric Time Clocks Work?*, *supra* note 25.

201. Meal et al., *supra* note 88; *see also* Amy Harwath, *Is BIPA Preempted? – Illinois Appellate Court Considers Workers' Compensation Exclusivity Question*, Sheppard Mullin Lab. & Emp't L. Blog (Jan. 30, 2020), https://www.laboremploymentlawblog.com/2020/01/articles/class-actions/bipa-preempted-illinois-appellate/.

In light of these considerations, the Illinois General Assembly must take action and amend BIPA accordingly. The amendment proposed in this Comment would remedy the aforementioned concerns by relieving the expensive burden currently placed on Illinois businesses defending BIPA class actions brought by unharmed plaintiffs. Importantly, though, this Comment's proposed amendment would also preserve the original intent of BIPA by continuing to allow a private right of action against companies that release personal data and cause an actual risk of harm. Illinois should be commended for prioritizing personal privacy, but to do so in the most fair and reasonable manner, BIPA must not be allowed to continue to punish businesses for failing to comply with a complex—and oftentimes unclear—statutory framework. A commonsense amendment to BIPA would allow the state to keep protecting personal data while also holding violators of the law accountable, but only to a degree commensurate with the actual violation.

James Nasiri