ANALYZING THE LEGAL LANDSCAPE OF BIPA PREEMPTION

ERIN HELLER*

In a world where a face can unlock a phone and a handprint can open doors, the advent of biometric technology has been seen as a technological advancement that improves security and convenience for the population at large. While largely ignored after it was first passed, a near explosion of litigation of the Illinois Biometric Information Privacy Act ("BIPA") has had steep consequences for businesses in the last five years. Between the Illinois Supreme Court's decision in Rosenbach*, determining a plaintiff need not show actual harm to establish standing for a BIPA action, and* White Castle*, determining damages under BIPA accrue per statutory violation, businesses are facing a disastrous future. Threats of potentially multi-billion-dollar judgments for collecting and storing biometric information without an individual's written consent looms over large and small businesses alike. In response, defendants are using an array of preemption arguments to escape the potentially bankrupting judgments that can be awarded if a company is found liable for BIPA violations. This Note surveys the success and viability of various preemption arguments and recommends that states abdicate a private right of action for violations of biometric information privacy laws in favor of alternative enforcement mechanisms.*

TABLE OF CONTENTS

* J.D. Candidate, 2024, University of Illinois College of Law; B.S., 2018, University of Utah. My sincerest thanks to the members, editors, and staff of the *University of Illinois Law Review* for their meticulous and diligent work in publishing this Note.

I. INTRODUCTION

Imagine a cool autumn day in the late fall in the town of Champaign, Illinois. Jack and Jill walk down the street from their last class of the day to Jack's afternoon shift at the local pizza parlor. They are each carrying the Chromebook their school gave them for free to use during their high school years as the sun shines down on their faces. Technology in 2022 makes their lives even easier: the Chromebooks allow for voice recognition functionalities and the ability to unlock their computers with just their faces, instead of a password. Jack and Jill part ways as Jack enters the pizza parlor to clock in for his shift. It was an older, local joint, but the parlor recently upgraded their time clock. Instead of clocking in with his multi-digit employee number, Jack can now conveniently clock in and out with just his fingerprint. This not only makes it easier for Jack to clock in, but it helps the company monitor and minimize time clock errors by employees.[1] All these convenient features—the voiceprint, facial geometrics, and fingerprints are all considered part of Jack and Jill's "biometrics" or their "biometric identifiers."[2]

However, with the perks of new technology also come risks. Disaster strikes, and Champaign is plagued with cyber-attacks. Data compromises are seen across the city, and that includes Jack and Jill's high school and the pizza parlor. Data containing records of Jack and Jill's voiceprint and facial geometry scans are compromised from their use of the school laptops they were given. Jack's fingerprint scan is compromised from the timekeeping system at the pizza parlor. Jack and Jill have both had major components of their person

1. *See* discussion *infra* Section II.A.

2. *Biometrics*, DEP'T. OF HOMELAND SEC., https://www.dhs.gov/biometrics (last visited Nov. 21, 2023) [https://perma.cc/4FJ7-C6QY].

compromised in the data breach, and that creates a huge issue—unlike a password, they cannot change their voice, face, or fingerprints to remedy this breach. Had Jack and Jill continued to use numerical passwords to access the computers and time clock, they could easily reset those passwords and hope the password changes were made quickly enough to avoid an actual attempt at an unauthorized use of their information. However, their face, voice, and fingerprints are biologically unique to them as individuals. What was first part of the initial draw to the new technology—ease, convenience, and security—is now compromised with little to no remedy.

Luckily, Jack and Jill live in Illinois, where laws have been promulgated to govern and help remedy this situation.[3] Under the Illinois Biometric Information Privacy Act ("BIPA"), entities must abide by certain requirements in order to collect, store, and use biometric information like Jack and Jill's voiceprint, facial geometry scans, and fingerprints.[4] Let's imagine that in this instance, the companies using and storing their biometric information both failed to obtain a written release from Jack and Jill, putting both companies in violation of BIPA's requirements.[5] This is unfortunately where Jack and Jill's luck diverges, as will be discussed in detail in this Note.

Both Jack and Jill could try to sue the entity that collected, used, and stored their voiceprint and facial geometry scans under BIPA, and Jack could also sue the pizza parlor that collected, used, and stored his fingerprint under BIPA. However, under the current statutory scheme, the recovery BIPA provides is only available to Jack.[6] Here's why: Jack's injuries happened through his employment and were essentially his employer's fault.[7] One would naturally suspect that a remedy would be available to Jack under the Workers' Compensation Act.[8] However, courts have found that this type of injury is not compensable under the Workers' Compensation Act.[9] Thus, the private right of action found in BIPA is available for Jack to pursue.[10] However, Jill's situation is slightly different. She would not be successful in her suit against the company collecting, using, and storing her biometrics because courts have determined that the Children's Online Privacy Protection Act preempts her BIPA claims.[11] Thus, Jill loses her private right of action and potential recovery against the entity under BIPA.[12] So while Jack and Jill have both suffered from data breaches involving their biometric identifiers, with arguably the same inability to remedy their breach because they cannot change their biometrics, BIPA's private right of action is only available

3. *See* discussion *infra* Section II.B.
4. *See* 740 ILL. COMP. STAT. ANN. 14/15(b) (West 2008).
5. 740 ILL. COMP. STAT. ANN. 14/1–25 (West 2008).
6. *See id.*
7. *See id.*
8. *See* Illinois Workers' Compensation Act, 820 ILL. COMP. STAT. ANN. 305/1–30 (West 2022).
9. *See* McDonald v. Symphony Bronzeville Park, LLC, 174 N.E.3d 578, 586 (Ill. App. Ct. 2020).
10. *See id.*
11. *See* Farwell *ex rel.* H.K. v. Google LLC, 595 F. Supp. 3d 702, 711 (C.D. Ill. 2022).
12. *See id.*

to Jack.[13] This scenario illustrates how parties facing similar injuries might be denied the windfall of recovery that BIPA authorizes for individuals.[14]

BIPA's enactment in October 2008 went relatively unnoticed, but today is one of the "favorite bases" for class action litigation in Illinois.[15] Less than 170 BIPA class action lawsuits were filed in the first ten years after BIPA's enactment.[16] The floodgates opened in 2019 when the Illinois Supreme Court in *Rosenbach v. Six Flags* determined plaintiffs need not show they suffered any actual harm to establish standing—a technical violation of BIPA is sufficient to maintain a cause of action.[17] Subsequent to *Rosenbach*, over 300 BIPA class action lawsuits were filed just in 2019 alone.[18] Between fall 2017 and spring 2022, more than 1,400 BIPA lawsuits were filed in state and federal courts, and the number only continues to grow.[19]

BIPA's primary targets mostly include Illinois businesses of various sizes from an array of industries, including community hospitals, family-owned grocery stores, hotels, and airlines.[20] BIPA exists as a looming threat over Illinois businesses, large and small, with the potential for devastating impacts across a variety of business sectors and industries.[21]

On August 3, 2020, Senator Jeff Merkley [D-OR] introduced (on behalf of himself and Senator Bernie Sanders [I-VT]) a comprehensive federal biometric privacy act.[22] The federal act was modeled after BIPA, which means it unfortunately included the vague and ambiguous language that has been fiercely litigated in Illinois courts in the last few years.[23] Additionally, not only does the federal act not preempt BIPA,[24] it also includes the same problematic private

13. *See* 740 ILL. COMP. STAT. ANN. 14/20 (West 2008).

14. *See id.*

15. Molly S. DiRago, *The Litigation Landscape of Illinois' Biometric Information Privacy Act*, AM. BAR ASS'N (Aug. 20, 2021), https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/the-litigation-landscape/ [https://perma.cc/7LA2-52SV]; *see also* Aaron Charfoos, Adam M. Reich & John J. Michels, *Illinois Supreme Court Rejects Potentially Key BIPA Preemption Argument*, PAUL HASTINGS (Feb. 8, 2022), https://www.paulhastings.com/insights/client-alerts/illinois-supreme-court-rejects-potentially-key-bipa-preemption-argument [https://perma.cc/H3UD-6UUN].

16. Joseph Stafford, Michael Duffy & Ashley Conaghan, *Illinois Supreme Court Finds Insurer Has Duty to Defend BIPA Suit*, BLOOMBERG L. (June 18, 2021), https://news.bloomberglaw.com/privacy-and-data-security/illinois-supreme-court-finds-insurer-has-duty-to-defend-bipa-suit [https://perma.cc/WVE3-GKFT].

17. Megan L. Brown, Duane C. Pozza, Kathleen E. Scott & Tawanna D. Lee, *ILR Briefly: A Bad Match: Illinois and the Biometric Information Privacy Act*, U.S. CHAMBER OF COM. INST. FOR LEGAL REFORM (Oct. 12, 2021), https://instituteforlegalreform.com/research/ilr-briefly-a-bad-match-illinois-and-the-biometric-information-privacy-act [https://perma.cc/Z9GF-J54A]; Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1205 (Ill. 2019).

18. *See* DiRago, *supra* note 15.

19. Brief of Amicus Curiae Illinois Chamber of Commerce in Support of Defendant–Appellant Black Horse Carriers, Inc. at 2, Tims v. Black Horse Carriers, Inc., 216 N.E.3d 845 (Ill. 2023) (No. 127801) 2022 WL 3902864, at *2.

20. *Id.* at *1.

21. *See id.*

22. National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2019).

23. Joseph J. Lazzarotti, *National Biometric Information Privacy Act, Proposed by Sens. Jeff Merkley and Bernie Sanders*, X NAT'L L. REV. (Aug. 5, 2020), https://www.natlawreview.com/article/national-biometric-information-privacy-act-proposed-sens-jeff-merkley-and-bernie [https://perma.cc/V9SG-KYPE].

24. National Biometric Information Privacy Act of 2020.

right of action to those aggrieved by a statutory violation, which is the reason BIPA-related litigation has exploded in Illinois.[25] Unless the federal act is modified through the legislative process, it would likely yield similar problems to BIPA.[26]

Congress cannot turn a blind eye to the financially devastating impacts that BIPA's private right of action can have on businesses.[27] Accordingly, Congress should survey states with biometric privacy acts and review the language of the acts and their relative impacts. Then, Congress should modify the federal act to resolve commonly litigated issues, preempt all current state privacy acts that leave a carve-out for reintroduction of stricter bills if desired, and pass and implement a comprehensive federal privacy act. But given the unlikelihood of a federal act, individual states that have, or are contemplating passing a biometric information privacy act, should forego a private right of action and/or consider less catastrophic enforcement mechanisms.[28]

Part II of this Note will begin by outlining what biometrics are, why we use them, and the consequences of withdrawing from the use of biometric technologies. A brief history about BIPA and a review of its requirements, remedies, and key recent rulings from the Illinois Supreme Court will follow, as well as a comparison of some other states' biometric privacy laws. It will then review Article III standing under BIPA to contextualize the damages that defendants are seeking to avoid with preemption arguments. Next, Part II will review what preemption is, the legal history of preemption, and how it is rooted in the Supremacy Clause, which recognizes Congress's power to preempt or invalidate state laws through federal legislation. Part II will finally explain that preemption is one of the newest avenues defendants are using to defend against BIPA actions. Part III analyzes and describes the landscape of preemption arguments that have been made to fight against BIPA claims and will include the various acts that do and do not preempt BIPA. Part III further reviews the areas of success with this strategy and indicates one area of possible legislative consideration of preemption as it pertains to financial institutions. Finally, Part IV recommends the subsequent adoption of a comprehensive federal privacy act that learns from, is informed by the chaos caused by, and eradicates BIPA. Part IV alternatively suggests that states considering their own biometric information privacy laws should abandon the private right of action for an alternative enforcement mechanism.

II. BACKGROUND

A basic explanation of biometrics is useful in understanding why biometric privacy and security is such a unique area of privacy law. As explained in detail below, biometrics are largely permanent and pose significant risks in the instance

25. *See* DiRago, *supra* note 15.
26. *See id.*
27. *See* discussion *infra* Section II.A.
28. *See* discussion *infra* Part IV.

of data breaches and compromises.[29] This Note will review BIPA's requirements and remedies to contextualize and frame subsequent litigation.[30] Some states have passed biometric privacy legislation in an effort to mitigate and control potential data breaches and compromises, but those states have not included a private right of action for violations.[31] Further, this Note will briefly describe an initial line of defense against BIPA that, while now moot, aids in understanding the evolution of strategies used to defeat BIPA claims.[32] Finally, a basic review of preemption theories will contextualize BIPA preemption arguments.[33]

A. Biometrics: What Are They, Why We Use Them, and What Happens if We Stop?

Biometrics are physical characteristics unique to individuals that can be used for recognition or identification, like fingerprints, DNA, retinas, facial geometry, voice, and even odor.[34] Businesses use biometrics in a variety of ways—from building or area security to ease of access.[35] Use of biometrics in the workplace benefits both the company and an end-user employee.[36] Biometrics can also be used between businesses and consumers to enhance ease of access and security in a variety of ways.[37] Some examples include using biometrics to unlock cell phones, gain entry to theme parks, operate cash registers, clock in and out of work, and travel by air.[38] Companies using biometric technology may appeal to consumers as being technologically cutting-edge and prioritizing a seamless customer experience.[39] Additionally, the COVID-19 pandemic has spurred high demand for contactless technology on high-frequency touch surfaces that may require identification—such as time clocks, office doors, and elevator buttons—to help reduce the spread of the virus.[40] Overall, biometric authentication

29. *See* discussion *infra* Section II.A.

30. *See* discussion *infra* Section II.B.

31. *See* discussion *infra* Section II.C.

32. *See* discussion *infra* Section II.D.

33. *See* discussion *infra* Section II.E.

34. *See Biometrics*, *supra* note 2; *Types of Biometrics*, BIOMETRICS INST., https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ (last visited Nov. 21, 2023) [https://perma.cc/R6AX-45UK].

35. *See* Omar Arab, *What the Rapid Adoption of Biometrics Means for Your Business*, FORBES (Jan. 21, 2022, 7:15 AM), https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2022/01/21/what-the-rapid-adoption-of-biometrics-means-for-your-business/?sh=3049356c4486 [https://perma.cc/32FT-E7VW].

36. *Id.*

37. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1200 (Ill. 2019) (describing amusement park's use of biometrics for repeat-entry park passes that utilize a fingerprint scan).

38. Jason C. Gavejian, Joseph J. Lazzarotti & Jody Kahn Mason, *Jump in Facial and Voice Recognition Raises Privacy, Cybersecurity, Civil Liberty Concerns*, XII NAT'L L. REV. (Feb. 3, 2022), https://www.natlawreview.com/article/jump-facial-and-voice-recognition-raises-privacy-cybersecurity-civil-liberty [https://perma.cc/G5HL-4BPH].

39. *See* Andrew Zarkowsky, *Biometrics: An Evolving Industry with Unique Risks*, HARTFORD INSIGHTS (May 20, 2021), https://www.thehartford.com/insights/technology/biometrics [https://perma.cc/K4MA-7RF3].

40. *Id.*

can lead to higher security and an enhanced user experience, and is generally nontransferable and challenging to replicate.[41]

Some biometrics can change over time, such as facial geometry slowly modifying due to age or illness, but other biometrics, such as fingerprints or retinal blood vessel patterns, usually do not.[42] Changing biometrics may impact a security system's accuracy,[43] but on the flip side, when biometrics that can't be changed are compromised, such as fingerprints, affected individuals have little to no recourse.[44] After a person's biometrics are compromised, they are "at a heightened risk for identity theft" and are "likely to withdraw from biometric-facilitated transactions."[45] Additionally, a company faced with liability for using biometric technology, as prescribed by BIPA, may be tempted to refrain from or cease using biometric technology altogether to avoid future potential liability.[46]

Withdrawal from biometric-facilitated transactions can have risks and consequences for both consumers and companies.[47] For consumers, distrusting biometric technology to the point where consumers altogether avoid companies using biometric technology means less consumer choice and smaller pools of economic competition.[48] Consumers who are choice-deprived might experience behavioral impacts, such as "undermin[ed] happiness, motivation, satisfaction, and health," and less autonomy and control.[49] Companies forgoing use of biometric technology would not reap the described benefits of using such technology.[50] Additionally, they face the general risks associated with a failure to adapt to modern technology, such as unnecessary human error, loss of revenue, competitive disadvantage, decreased productivity, poor consumer experience, and security risks.[51]

41. *The Future of Security is Here—Biometric Authentication*, KOPPINGER & ASSOCS. (Nov. 4, 2022), https://koppingerins.com/blog/the-future-of-security-is-here-biometric-authentication [https://perma.cc/5MX9-KJGJ].

42. Alan S. Wernick, *Biometric Information—Permanent Personally Identifiable Information Risk*, BUS. L. TODAY (Jan. 28, 2019), https://businesslawtoday.org/2019/01/biometric-information-permanent-personally-identifiable-information-risk/ [https://perma.cc/54PH-SULD].

43. *Id.*

44. *Id.*

45. 740 ILL. COMP. STAT. ANN. 14/5(c) (West 2008).

46. *See, e.g.*, *The Future of Security is Here—Biometric Authentication*, *supra* note 41.

47. Some institutions have paused their use of biometric technology, specifically facial recognition, over concerns of invasive state surveillance, discrimination and bias, inaccuracy, and compelled or coerced access in violation of Fourth and Fifth Amendment rights. Maeve Allsup, *Compelled Biometric Access Legal Under 4th, 5th Amendments*, BLOOMBERG L. (July 2, 2020, 3:25 PM), https://news.bloomberglaw.com/us-law-week/compelled-biometric-access-legal-under-4th-5th-amendments [https://perma.cc/4QQG-68WA]; Jim Siegl, Anisha Reddy & Casey Waughn, *New York Hits Pause on Biometric Technology in Schools: What It Means for Education Stakeholders*, STUDENT PRIV. COMPASS, https://studentprivacycompass.org/new-york-hits-pause-on-biometric-technology-in-schools-what-it-means-for-education-stakeholders/ (Mar. 24, 2021) [https://perma.cc/U6LX-TCXR]. This Note does not address these concerns.

48. *See* Elena Reutskaja, Nathan N. Cheek, Sheena Iyengar & Barry Schwartz, *Choice Depravation, Choice Overload, and Satisfaction with Choices Across Six Nations*, 30 J. INT'L MKTG. 18, 18 (2022).

49. *Id.* at 18, 20.

50. *See supra* notes 34–41 and accompanying text.

51. Hannah Tomlinson, *5 Risks of Not Adapting to Modern Technology in Business*, E-BATE (July 2, 2021), https://blog.e-bate.io/risks-of-not-adapting-to-modern-technology [https://perma.cc/ESN6-XAQ9]; *Why You*

B. A Bit About BIPA: Requirements, Remedies, and Recent Rulings

In October 2008, Illinois made history by enacting the very first biometric data privacy law in the country.[52] The Illinois General Assembly passed BIPA in an effort to protect public welfare and safety through "regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[53] BIPA specifically defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[54] BIPA also specifically excludes other physical or related characteristics from the definition, such as writing samples, human biological samples used for scientific testing or screening, demographic data, tattoo descriptions, physical descriptions, and donated organs.[55]

BIPA sets forth multiple provisions with requirements for private entities using or possessing biometric data.[56] First, such entities must develop written, publicly available policies that establish a retention schedule and guidelines for permanent destruction of biometric identifiers and information after the initial purpose of collecting or obtaining the identifiers and information has been satisfied.[57] Otherwise, biometric information and identifiers should be permanently destroyed within three years of a person's last interaction with such entity, whichever is first.[58]

Next, private entities cannot "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" unless the entity notifies the person that their information is being collected or stored, the entity provides the specific purpose and length of time it will be stored, collected, and used, and the entity receives a written release by the person.[59] BIPA further prohibits a private entity possessing biometric information to sell, lease, trade, or profit from the information.[60] BIPA also regulates the disclosure, redisclosure, and dissemination of biometric information, contemplating consent, disclosure in compliance with state and federal law, and warrants and subpoenas.[61] Finally, private entities must store biometric information using a reasonable standard of care, similar to the manner in which it protects other confidential information.[62]

Must Avoid Outdated Technology in Business, NAT'L FUNDING: THE BOTTOM LINE (Nov. 1, 2019), https://www.nationalfunding.com/blog/outdated-business-technology/ [https://perma.cc/8XYH-Z7LL].

52. *The Evolution of Biometric Data Privacy Laws*, BLOOMBERG L. (Nov. 4, 2021), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/ [https://perma.cc/4JFT-8FSN].

53. 740 ILL. COMP. STAT. ANN. 14/5(g) (West 2008).

54. *Id.* 14/10.

55. *Id.*

56. *Id.* 14/15.

57. *Id.* 14/15(a).

58. *Id.*

59. *Id.* 14/5(b).

60. *Id.* 14/5(c).

61. *Id.* 14/5(d).

62. *Id.* 14/5(e).

Simply put, BIPA is a relatively short statute, and there does not seem to be much complexity or difficulty for BIPA compliance.[63] For some entities, it is as simple as having employees sign a written consent form with the required retention and destruction schedules, then treating the information as they would normally treat private company information.[64] However, failure to obtain written consent and provide retention and destruction schedules seems to be a ubiquitous pattern leading to litigation.[65] While surprising, there are some theories as to why more businesses didn't initially comply with BIPA. First, it's important to recognize that BIPA was passed in 2008—two years before Facebook started adding "tag" suggestions to uploaded photos by using facial-recognition software and twelve years before Apple added a thumbprint scanner for unlocking an iPhone.[66] So, BIPA was enacted long before an average person likely had frequent and conscious interaction with biometric technology.[67]

While biometric technology has existed since the 1960s, it's likely that many businesses were simply not focused on incorporating biometric-utilizing technology into their businesses at the time, especially while the technology was still relatively new to the United States marketplace.[68] Additionally, the United States was experiencing the massive financial crisis of the Great Recession, which deeply impacted the housing market and financial sector.[69] Regardless of the potential reasons, it seems that a wide variety of entities subject to BIPA's requirements simply did not sufficiently comply or attempt to comply at all, hence the metaphorical avalanche of BIPA cases disproportionately filed within the last eight years.[70]

Such case filings are made possible by the language and express authorization of BIPA itself.[71] BIPA diverges from most other existing biometric information privacy laws in a significant way—BIPA provides for a private right of action for individuals who have been aggrieved by a BIPA violation.[72] Not only that, but BIPA provides for liquidated damages for the greater of $1,000 or actual damages for negligent violations, and the greater of $5,000 or actual damages for intentional or reckless violations.[73] Last, but not least, BIPA authorizes recovery of reasonable attorneys' fees and costs, explicitly including expert witness fees

63. *See generally id.* 14/5.

64. *Id.* 14/15(d).

65. *See* discussion *infra* Part III.

66. Rachel Metz, *Here's Why Tech Companies Keep Paying Millions to Settle Lawsuits in Illinois*, CNN BUS. (Sept. 20, 2022, 8:33 AM), https://www.cnn.com/2022/09/20/tech/illinois-biometric-law-bipa-explainer/index.html [https://perma.cc/4SG5-NC9H].

67. *See id.*

68. Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE (Feb. 1, 2018, 11:43 AM), https://www.biometricupdate.com/201802/history-of-biometrics-2 [https://perma.cc/RQY8-VQ3J].

69. John Weinberg, *The Great Recession and Its Aftermath*, FED. RSRV. HIST., https://www.federalreservehistory.org/essays/great-recession-and-its-aftermath (Nov. 22, 2013) [https://perma.cc/2CX3-KUC7].

70. *Cook County, Illinois*, ATR FOUND.: JUD. HELLHOLES, https://www.judicialhellholes.org/hellhole/2022-2023/cook-county-illinois/ (last visited Nov. 21, 2023) [https://perma.cc/23E9-8N2M].

71. 740 ILL. COMP. STAT. ANN. 14/20 (West 2008).

72. *Id.*

73. *Id.*

and other nonmonetary relief as appropriate.[74] While damage awards under BIPA are permissive and discretionary, they are still authorized, and plaintiffs will likely claim the maximum amount of damages possible.[75]

Among BIPA's many problems, two key previously pending issues had stayed cases across the state for months, if not years, while under consideration of the Illinois Supreme Court.[76] First, the *Tims* court considered whether a one-year or a five-year statute of limitations governed BIPA claims.[77] In February 2023, the court ruled that the five-year "catchall" statute of limitations period controls BIPA claims because BIPA does not itself contain a limitations period.[78]

But perhaps even more catastrophic, until very recently, Illinois businesses, lawyers, and courts hung in limbo regarding how to interpret how multiple potential claims of BIPA violations accrue under the Act.[79] Claim accrual directly correlates to how damages are calculated under BIPA.[80] In May 2022, the Illinois Supreme Court heard oral arguments in *Cothron v. White Castle System, Inc.* regarding claim accrual.[81] *Cothron* involved a White Castle employee who used a fingerprint scanner to access the restaurant's computer system, and with each scan, her fingerprint was collected and sent to a third-party vendor for authentication.[82] The parties disputed whether the employee's claim accrued with each instance of fingerprint scanning and transmission, or if the claim accrued only after the first scan and transmission.[83] The Seventh Circuit certified the question of claim accrual to the Illinois Supreme Court.[84] Multiple *amici curiae* cautioned the Court that per-scan claim accrual could lead to exorbitant and bankrupting multi-billion dollar judgments.[85] But just fifteen days after the *Tims* decision, the Illinois Supreme Court answered the certified question—claims do accrue with each violation.[86] Despite acknowledging that the decision could subject White Castle to damages in excess of $17 billion, the court deferred the financial

74. *Id.*

75. *Id.*; Second Amended Class Action Complaint at 13 ¶ 58, Cothron v. White Castle Sys., Inc., No. 1:19-CV-00382 (N.D. Ill. Apr. 11, 2019).

76. *See* Tims v. Black Horse Carriers, Inc., 216 N.E.3d 845, 845 (Ill. 2023); Cothron v. White Castle Sys., Inc., 216 N.E.3d 918, 921 n.1 (Ill. 2023).

77. *Tims*, 216 N.E.3d at 853.

78. *Id.*

79. Kathryn Cahoy & Dominic Booth, *Federal Court Stays Suit Implicating Accrual of Claims Under the Illinois Biometric Information Privacy Act*, COVINGTON (July 15, 2022), https://www.insideprivacy.com/united-states/litigation/federal-court-stays-suit-implicating-accrual-of-claims-under-the-illinois-biometric-information-privacy-act/ [https://perma.cc/C3HG-WNRR].

80. *See* 740 ILL. COMP. STAT. ANN. 14/20 (West 2008).

81. *Supreme Court Oral Argument Audio and Video*, ILL. CTS., https://www.illinoiscourts.gov/courts/supreme-court/oral-argument-audio-and-video/ (last visited Nov. 21, 2023) [https://perma.cc/H6X9-6H3F] (search in search bar for "White Castle" and adjust date range to include May 2022; then click on graphic image under "Audio/Video" section to view oral argument audio and video).

82. Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1158 (7th Cir. 2021).

83. *Id.* at 1162–65.

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

85. Brief of Retail Litig. Ctr., Inc., Restaurant L. Ctr., and Nat'l Retail Fed'n as Amici Curiae in Support of Defendant-Appellant at 10, Cothron v. White Castle Sys., Inc., 216 N.E.3d 918 (Ill. 2023) 2021 WL 1418279, at *7.

86. *Cothron*, 216 N.E.3d at 920.

implications to consideration of the Illinois legislature, "even though the consequences [of the decision] may be harsh, unjust, absurd, or unwise."[87] However, Justice Overstreet acknowledged in his dissent that the consequence of crippling liability should be contemplated by the Court in determining legislative intent and that the decision may discourage the use of biometric technology altogether.[88]

Accordingly, as the first state to pass a biometric information privacy law,[89] Illinois has served as a harrowing example to the rest of the United States of how much confusion, uncertainty, and legal liability can stem from a biometric privacy law.[90] In fact, BIPA litigation in Cook County has led to the County's spot on the Judicial Hellholes® list for the last seven years in a row.[91] Now, after *Tims* and *White Castle*, Illinois businesses face crippling, catastrophic, and, as *White Castle* acknowledges, "annihilative liability."[92]

C. Additional Biometric Privacy Legislation

Illinois was not alone in determining the need for legislation governing biometric information privacy.[93] Texas and Washington were two of the next states to adopt similar provisions, adopting their statutes in 2009 and 2017, respectively.[94] Texas's privacy act requires notice and consent before capturing biometric identifiers for commercial purposes.[95] The statute does not provide for a private right of action, but the Attorney General may bring an action to recover the $25,000 civil penalty.[96] Washington's privacy act requires notice, consent, or a mechanism preventing subsequent use of biometric information for enrolling a biometric identifier in a database for a commercial purpose.[97] Like Texas, the statute does not provide for a private right of action.[98]

California initially took a different route and encompassed biometric information privacy in a larger consumer privacy act, the California Consumer Privacy Act.[99] The act includes a general (*i.e.*, non-biometric specific) private right of action, and while such right is "narrow," class actions have been filed alleging various biometric information violations.[100] In February 2022, Senator Bob

87. *Id.* at 928.

88. *Id.* at 934, 936 (Overstreet, J., dissenting).

89. *See supra* note 52 and accompanying text.

90. *See supra* note 70 and accompanying text.

91. *See Judicial Hellholes*, ATR FOUND.: JUD. HELLHOLES, https://www.judicialhellholes.org/reports/ (last visited Nov. 21, 2023) [https://perma.cc/AY8J-9BEG] (viewing reports from 2017 through 2023).

92. *See Cothron*, 216 N.E.3d at 934 (Overstreet, J., dissenting).

93. *See infra* notes 95–103.

94. TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2017); WASH. REV. CODE § 19.375.020(1) (2017).

95. TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017).

96. *Id.* § 503.001(d).

97. WASH. REV. CODE 19.375.020(1) (2017).

98. *Id.*

99. CAL. CIV. CODE § 1798.100 (West 2023).

100. Legaltech News, *Analyzing the CCPA's Impact on the Biometric Privacy Landscape*, BLANKROME (Oct. 14, 2020), https://www.blankrome.com/publications/analyzing-ccpas-impact-biometric-privacy-landscape [https://perma.cc/4ZLU-JL72].

Wieckowski introduced SB 1189 (entitled "Biometric Information") in California to expand the biometric information privacy requirement and echo many of BIPA's provisions, including a similar private right of action.[101] Other cities and states have imposed ordinances or other statutes that regulate biometric information to some extent, including New York City, Arkansas, Virginia, and Utah.[102]

D. Article III Standing

Article III standing under BIPA has been the subject of numerous articles and publications, and the issue is ultimately resolved.[103] While not directly related to preemption arguments, a brief overview helps frame the beginning of the evolution of methods defense attorneys have used to dismiss BIPA cases in their initial stages.[104]

A litigant's requirement that they have "standing" broadly means that the litigant has a right to seek a judicial ruling on a particular claim and is based on Article III, Section 2, Clause 1 of the United States Constitution.[105] Standing typically requires three elements: "(1) a concrete and particularized injury; (2) that is traceable to the allegedly unlawful actions of the opposing party; and (3) that is redressable by a favorable judicial decision."[106] A key issue concerning standing in privacy cases is the first requirement of having a concrete and particularized injury.[107] Just how concrete and particularized the injury is in a privacy case can vary— a plaintiff may have a risk of future injury after a data breach, spend resources to protect against a future risk, or feel distress over the mere fact that their data has been compromised.[108] However, many courts do not usually recognize any of those categories of harm as a concrete and particularized injury.[109] The few instances wherein courts have recognized risk of future harm as a cognizable injury have involved factually distinct allegations of hackers or actual or attempted misuse of data.[110] Otherwise, that type of risk typically fails

101. S.B. 1189, 2021–2022 Reg. Sess. (Cal. 2022); Alyona Eidinger, *California's Biometric Information Bill (SB 1189)—To Be, or Not To Be: That Is the Question*, CAL. LAWS. ASS'N (May 2022), https://calawyers.org/privacy-law/californias-biometric-information-bill-sb-1189-to-be-or-not-to-be-that-is-the-question [https://perma.cc/N4QP-K5KE]. SB 1189 is currently held in the suspense file without objection. *Id.*

102. *See* DiRago, *supra* note 15.

103. *See, e.g.*, Sojung Lee, Note, *Give up Your Face, and a Leg to Stand On Too: Biometric Privacy Violations and Article III Standing*, 90 GEO. WASH. L. REV. 795, 808–09 (2022).

104. *See infra* notes 106–20 and accompanying text.

105. *ArtIII.S2.C1.6.1 Overview of Standing*, CONGRESS.GOV: CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/artIII-S2-C1-6-1/ALDE_00012992/ (last visited Nov. 21, 2023) [https://perma.cc/T5CB-TQNC].

106. *Id.*

107. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 748 (2018).

108. *Id.* at 749–54.

109. *Id.* at 754.

110. *Id.* at 751–52.

as a cognizable harm to meet the injury requirement for standing.[111] The Illinois Supreme Court, however, disagrees.[112]

In *Rosenbach v. Six Flags Entertainment Corp.*, the Illinois Supreme Court held that a technical violation of BIPA alone constituted an injury sufficient to establish Article III standing.[113] A company that breaches any of the duties imposed in Section 15 of BIPA[114] invades, impairs, or denies a person their statutory rights, making them an aggrieved person under BIPA.[115] The court reasoned that violations of Section 15 mean that the "right of the individual to maintain [their] biometric privacy vanishes into thin air," which is the precise harm the Illinois legislature identified as worth preventing.[116] Accordingly, "some actual injury or adverse effect" need not be alleged because a violation of BIPA, even without more, is a "real and significant" injury to qualify someone as an aggrieved person entitled to seek damages under BIPA.[117] Since *Rosenbach* obviated the strategy previously used to dismiss BIPA lawsuits,[118] defendants have moved to new arguments, namely, preemption arguments.[119]

E. Doctrine of Preemption

Preemption can be a complicated legal doctrine, but at its most basic level, preemption is the idea that a law with higher authority displaces a law with lower authority when those two laws are in conflict with each other.[120] More specifically, preemption is a principle derived from the Supremacy Clause in the United States. Constitution that a federal law can "supersede or supplant any inconsistent state law or regulation."[121] Preemption is not an unusual situation either.[122] Federal preemption of state law is likely the most commonly used constitutional law doctrine in practice and frequently occurs in regulated industries, such as drugs, banking, securities, and tobacco.[123]

The "ultimate touchstone" of whether a federal law preempts a state law is Congress's intent, which courts derive primarily from the plain text of a statute.[124] But in evaluating whether there is preemption, there is a presumption against preemption unless it was the "clear and manifest purpose of

111. *See id.* at 752.

112. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019).

113. *Id.*

114. Section 15 of BIPA lists the requirements and obligations of the act, including the disclosure of a data retention schedule, the informed consent and written policy requirements, and guidelines for destroying biometric information after it has been collected. 740 ILL. COMP. STAT. ANN. 14/15 (West 2008).

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

116. *Id.* (quoting Patel v. Facebook Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).

117. *Id.* at 1206–07.

118. *See id.*

119. *See* discussion *infra* Part III.

120. *Preemption*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/preemption (last visited Nov. 21, 2023) [https://perma.cc/3CS3-ZQPL].

121. *Preemption*, BLACK'S LAW DICTIONARY (11th ed. 2019); *accord* U.S. CONST. art. VI, § 2.

122. JAY B. SYKES & NICOLE VANATKO, FEDERAL PREEMPTION: A LEGAL PRIMER 1 (2019).

123. *Id.*

124. *Id.* at 3.

Congress."[125] In a somewhat recent development, that presumption no longer exists in instances of express preemption.[126] In those instances, preemption clauses are simply given their ordinary meaning.[127]

There are two main types of conflicts that exist regarding issues of preemption: express and implied preemption.[128] This Note will briefly describe both types.

1. Express Preemption

Federal law expressly preempts state law when there is explicit language stating its preemptive effect.[129] Express preemption functions at the state level by restricting lower levels of the government from regulating particular areas.[130] Expressly preemptory legislation does not have to be built from the ground up.[131] Language that has worked before is often invoked when drafting new legislation.[132] Certain key phrases have specific meaning across various statutory contexts and appear repeatedly.[133] For example, preemption clauses can supersede all state laws "related to" a particular regulated subject.[134] This is demonstrated in the Employee Retirement Income Security Act ("ERISA"), which encompasses the key phrase in a clause that states its requirements preempt state laws that "relate to" regulated employee benefit plans.[135] While ERISA's "relate to" clause is broad and potentially very far-reaching, the Supreme Court "relie[s] on legislative history and purpose to cabin [its] scope."[136] How exactly the scope is defined and circumscribed is typically a matter of judicial interpretation.[137]

2. Implied Preemption

Implied preemption occurs when federal law preempts state law not expressly, but through structure and purpose that reflects a congressional intent to preempt.[138] There are two sub-categories within implied preemption: field and conflict preemption.[139] Field preemption "occurs when a pervasive scheme of

125. *Id.* (quoting Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947)).

126. Puerto Rico v. Franklin Cal. Tax-Free Trust, 579 U.S. 115, 125 (2016) (determining there is no presumption against preemption when a statute has an express preemption clause, and the plain wording of the clause is the best evidence of Congress's preemptive intent).

127. *Id.*

128. SYKES & VANATKO, *supra* note 122, at 2.

129. *Id.*

130. *What You Need to Know About Preemption*, NAT'L LEAGUE OF CITIES, https://www.nlc.org/wp-content/uploads/2020/11/Preemption_101.pdf (last visited Nov. 21, 2023) [https://perma.cc/T3PK-JVAK].

131. *See* SYKES & VANATKO, *supra* note 122, at 6.

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.* at 7; Employee Retirement Income Security Act of 1974, 29 U.S.C. § 1144(a).

136. SYKES & VANATKO, *supra* note 122, at 7.

137. *See, e.g.*, Egelhoff v. Egelhoff, 532 U.S. 141, 151 (2001) (interpreting whether a Washington state statute is related to ERISA plans).

138. SYKES & VANATKO, *supra* note 122, at 2.

139. *Id.* Two sub-categories also exist within conflict preemption: possibility and obstacle preemption. *Id.*

federal regulation implicitly precludes supplementary state regulation, or when states attempt to regulate a field where there is clearly a dominant federal interest."[140] Essentially, field preemption occurs when Congress has manifested an intention that the states should not regulate a particular area, and that the federal government should exclusively govern.[141] Some examples of those fields include nuclear safety, aircraft noise, and wholesale of natural gas in interstate commerce.[142] Instances of implied preemption are frequently determined and clarified through litigation.[143]

Conflict preemption "occurs when a state law interferes with federal goals."[144] It can either be the case that it is impossible for regulated parties to comply with both laws or that state laws hinder the purpose and objective of Congress perpetuated through the federal law.[145] To illustrate, in *Brod v. Sioux Honey Ass'n Cooperative*, honey that was filtered to remove pollen was required to be labeled its common name of "honey" under federal regulations, but a California law forbid such a product to be labeled as "honey."[146] The court called the situation a "classic case of conflict preemption."[147] In that instance, it would be impossible for the producer to comply with the federal regulations requiring that the product be labeled honey and abide by the California law forbidding that labeling.[148] Thus, the California law was preempted.[149]

F. Current Landscape of Preemption Challenges

Various preemption arguments have been used in hopes of dismissing BIPA litigation.[150] Acts successfully preempting BIPA claims currently include the Railway Labor Act,[151] the Labor Management Relations Act,[152] and the Children's Online Privacy Act.[153] Acts or other regulations that do not preempt BIPA claims include the Illinois Workers' Compensation Act,[154] the Medical Device Amendments of 1976,[155] the Federal Railroad Safety Act,[156] the Interstate Commerce Commission Termination Act,[157] and Food and Drug Administration

140. *Id.* at 17.
141. *See id.*
142. *Id.* at 18.
143. NAT'L LEAGUE OF CITIES, *supra* note 130.
144. SYKES & VANATKO, *supra* note 122, at 17, 23–24.
145. *Id.* at 23–24.
146. 895 F. Supp. 2d 972, 974–75 (N.D. Cal. 2012).
147. *Id.* at 981.
148. *Id.*
149. *Id.*
150. *See* discussion *infra* Section III.A.
151. Miller v. Sw. Airlines Co., No. 18-C-86, 2018 WL 4030590, at *6 (N.D. Ill. Aug. 23, 2018).
152. Fernandez v. Kerry, Inc., No. 17-CV-08971, 2020 WL 7027587, at *6 (N.D. Ill. Nov. 30, 2020); Peatry v. Bimbo Bakeries USA, Inc., No. 19-C-2942, 2020 WL 919202, at *1 (N.D. Ill. Feb. 26, 2020); Hicks v. Evergreen Living & Rehab Ctr., LLC, No. 20-CV-04032, 2021 WL 4440315, at *4 (N.D. Ill. Mar. 8, 2021).
153. H.K. v. Google LLC, 595 F. Supp. 3d 702, 711 (N.D. Ill. 2022).
154. McDonald v. Symphony Bronzeville Park LLC, 174 N.E.3d 578, 586 (Ill. App. Ct. 2020).
155. Crumpton v. Octapharma Plasma, Inc., 513 F. Supp. 3d 1006, 1012–15 (N.D. Ill. 2021).
156. Fleury v. Union Pac. R.R. Co., 528 F. Supp. 3d. 885, 892, 894 (N.D. Ill. 2021).
157. *Id.* at 894.

regulations.[158] This list is not comprehensive and does not represent an exhaustive list of potential preemptory acts, but it does help illustrate the breadth of preemption theory arguments.

III. ANALYSIS

A. Preemption Arguments Across Industries

There have been varying levels of success in preempting BIPA claims.[159] These preemption arguments are usually won and lost before trial, frequently as Rule 12(b)(6) motions to dismiss or motions to strike.[160] While many BIPA claims are in the employment context, they are not so limited.[161] Regardless of the scenarios prompting litigation, preemption arguments are being used as another way to dismiss, or at least interrupt and push to settlement, an array of claims.[162] Especially in the wake of the *Tims* and *White Castle* decisions, it would be unsurprising if more preemption arguments are metaphorically "tried on" in an attempt to avoid looming liability.[163]

1. Acts, Legislation, or Regulations Preempting BIPA

Some attempts to preempt BIPA claims have been successful on the basis of both express and implied preemption.[164] The following subsection discusses the cases and statutes wherein BIPA claims were preempted, namely, by the Railway Labor Act, the Labor Management Relations Act, and the Children's Online Privacy Protection Act.[165]

a. Railway Labor Act

One of the first cases alleging a preemption issue with BIPA claims was *Miller v. Southwest Airlines Co.*[166] In *Miller*, three putative class representative plaintiffs worked as ramp agents and operations agents at Chicago Midway International Airport ("Midway").[167] All such employees were union members for the purpose of collective bargaining, and the union had indeed entered into a collective bargaining agreement ("CBA") with Defendant Southwest Airlines

158. Marsh v. CSL Plasma Inc., 503 F. Supp. 3d. 677, 684–85 (N.D. Ill. 2020).

159. *See* discussion *infra* Subsections III.A.1–2.

160. *See, e.g.*, *Crumpton*, 513 F. Supp. 3d at 1011.

161. *See, e.g.*, H.K. *ex rel*. Fairwell v. Google LLC, 595 F. Supp. 3d 702, 704–05 (C.D. Ill. 2022).

162. *See* Miller v. Sw. Airlines Co., 18-CV-86, 2018 WL 4030590, at *5 (N.D. Ill. Aug. 23, 2018), *aff'd*, 926 F.3d 898 (7th Cir. 2019); Fernandez v. Kerry, Inc., No. 17-CV-08971, 2020 WL 7027587, at *6 (N.D. Ill. Nov. 30, 2020), *aff'd*, 14 F.4th 644 (7th Cir. 2021).

163. *See generally* Tims v. Black Horse Carriers, Inc., 216 N.E.3d 845 (Ill. 2023); Cothron v. White Castle Sys., Inc., 216 N.E.3d 918 (Ill. 2023).

164. *See* discussion *infra* Subsection III.A.1.

165. *See* Railway Labor Act, 45 U.S.C. §§ 181–88; Labor Management Relations Act, 29 U.S.C. §§ 141–91; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06.

166. *See Miller*, 2018 WL 4030590, at *2.

167. *Id.* at *1.

Co. ("Southwest").[168] Southwest implemented a time clock system at Midway requiring fingerprint scans to clock in and out of work.[169] The plaintiffs sued Southwest, alleging in their complaint that Southwest violated BIPA by not providing notice or obtaining written consent to use biometric data and by failing to publish a data retention and deletion schedule among other things.[170] The Railway Labor Act ("RLA") governs CBAs in the airline industry and was designed in part to provide legal dispute resolution tactics as a substitute for strikes.[171] The RLA requires arbitration to settle major and minor disputes.[172]

The court held that the plaintiffs' claims were minor disputes preempted by the RLA because the claims required interpretation of the CBA negotiated between the union and Southwest.[173] Because the CBA governed terms and conditions of employment, the BIPA claim required interpretation to determine whether Southwest had authority to use any particular timekeeping system.[174] Further, the CBA established a grievance procedure requiring arbitration for dispute resolution as required by the RLA.[175] As such, the plaintiffs' claims required interpretation of the CBA and, thus, were preempted by the RLA and were required to be submitted to arbitration, making the district court an improper venue.[176]

b. Labor Management Relations Act

In *Fernandez v. Kerry Inc.*, former production employees ("Plaintiffs") working at Kerry, Inc. used their fingerprints to clock in and out of work beginning in approximately 2011.[177] Plaintiffs filed suit against Kerry, Inc. alleging that the company violated BIPA by failing to inform them of the purpose and length of time their fingerprints would be stored, collected, and used, provide a publicly available retention schedule and guidelines for destroying the fingerprints, and receive a written release to capture and collect their fingerprints.[178] From the initial point when Kerry, Inc. was collecting and using Plaintiffs' fingerprints until the time that Plaintiffs quit, Plaintiffs were union members with a CBA in effect.[179] The CBA detailed a grievance procedure for dispute resolution regarding the interpretation and application of the CBA which required arbitration.[180]

168. *Id.*
169. *Id.*
170. *Id.*
171. *See id.* at *4.
172. *Id.*
173. *Id.* at *5.
174. *Id.*
175. *Id.*
176. *Id.* at *6.
177. Fernandez v. Kerry, Inc., No. 17-CV-08971, 2020 WL 7027587, at *1 (N.D. Ill. Nov. 30, 2020), *aff'd*, 14 F.4th 644 (7th Cir. 2021).
178. *Id.*
179. *Id.* at *2.
180. *Id.*

The court determined that the Labor Management Relations Act ("LMRA") preempted Plaintiffs' BIPA claim.[181] The LMRA preempts a state law claim if the resolution of the claim requires interpretation of a CBA.[182] That is true whether a claim is founded directly on rights of a CBA or if a claim substantially depends on a CBA's analysis.[183] The court reasoned that the facts were nearly identical to *Miller*,[184] and the way an employee clocks in is undoubtedly the subject of negotiation between employers and unions and thus a mandatory subject of bargaining.[185] Using *Miller*'s precedent, the Plaintiffs' BIPA claim was preempted by the LMRA.[186] Further, the Plaintiffs' specific contentions toward their Section 15(a) claims also failed.[187] Regardless of when the Plaintiffs' claims actually accrued, their BIPA claims relate back to their employment and union membership and are subject to the CBA, so the claims were preempted.[188] Ultimately, the complaint was dismissed without prejudice with leave to file an amended complaint.[189]

In *Peatry v. Bimbo Bakeries USA, Inc.*, Plaintiff Lisa Peatry's fingerprint was collected upon hiring at Bimbo Bakeries USA, Inc. ("Bimbo"), and she subsequently used her fingerprint to clock in and out of work.[190] Peatry filed suit against Bimbo alleging, in part, BIPA violations, including failure to keep and maintain a publicly available retention schedule, failure to obtain informed, written consent from Peatry, and Bimbo's disclosure of biometric information before obtaining consent.[191] During her employment as a machine operator at a Bimbo facility, Bimbo entered into a CBA with the union at the facility to, in part, make and enforce plant rules, introduce new, improved, or changed methods, materials, or facilities, and negotiate wage tables.[192] The CBA also detailed grievance procedures, requiring employees' adherence to such procedures.[193] Under *Miller*'s precedent, Peatry's BIPA claims required interpretation of the CBA.[194] Thus, similarly to *Fernandez*,[195] her claims were preempted.[196]

181. *Id.* at *6.
182. *Id.* at *3 (quoting Lingle v. Norge Div. of Magic Chef, Inc., 486 U.S. 399, 413 (1988)).
183. Caterpillar Inc. v. Williams, 482 U.S. 386, 394 (1987).
184. Miller v. Sw. Airlines Co., 926 F.3d 898, 901 (7th Cir. 2019).
185. *Id.* at 903.
186. *Fernandez*, 2020 WL 7027587, at *4.
187. *Id.* at *6.
188. *Id.*
189. *Id.* at *8.
190. Peatry v. Bimbo Bakeries USA, Inc., No. 19-CV-2942, 2020 WL 919202, at *1 (N.D. Ill. Feb. 26, 2020).
191. *Id.*
192. *Id.* at *2.
193. *Id.*
194. *Id.* at *3.
195. *See* Fernandez v. Kerry, Inc., No. 17-CV-08971, 2020 WL 7027587, at *3 (N.D. Ill. Nov. 30, 2020), *aff'd*, 14 F.4th 644 (7th Cir. 2021).
196. *Peatry*, 2020 WL 919202, at *4.

Finally, there is a similar story in *Hicks v. Evergreen Living & Rehab Center*—Plaintiff Jarita Hicks used her fingerprint to clock in and out of work.[197] Hicks was a union member with a CBA while working at Evergreen Living & Rehab Center, LLC ("Evergreen") as a Certified Nursing Assistant, and the union was the sole collective bargaining agent for such employees.[198] The CBA gave authority to Evergreen to promulgate rules regarding work attendance not otherwise addressed in the CBA and established a grievance procedure for dispute resolution.[199] Hicks filed suit against Evergreen, alleging that Evergreen failed to comply with BIPA's requirements by not creating or making publicly available a retention schedule and destruction guidelines, failing to inform employees of biometric information collection or purpose and length of storage, and failing to obtain prior written authorization before collecting the data.[200] The court recognized that *Miller* controlled, that Hicks' claims required interpretation of the CBA, and, thus, her claims were preempted and subsequently dismissed.[201]

c. Children's Online Privacy Protection Act

Preemption arguments against BIPA claims are not at all limited to the employer-employee relationship context.[202] In *H.K v. Google LLC*, minor plaintiffs and other elementary school students were supplied laptops by Defendant Google LLC ("Google") that were pre-installed with the product "G Suite for Education."[203] As a part of the product's use, children's voiceprints and facial geometry scans were collected and stored.[204] Minor plaintiffs sued Google alleging a systemic violation of BIPA by collecting, storing, and using children's biometric data without written consent from any parents and failing to provide a publicly available retention and destruction schedule.[205] Google argued that the claims were preempted by the Children's Online Privacy Protection Act ("COPPA"), a federal act that regulates the "online collection of personal information from children who . . . are under the age of 13."[206] Google luckily escaped potentially massive liability—because COPPA broadly regulates the collection of children's data, the plaintiff's allegations fell "squarely in COPPA's

197. Hicks v. Evergreen Living & Rehab Ctr., LLC, No. 20-CV-04032, 2021 WL 4440315, at *1 (N.D. Ill. Mar. 8, 2021).

198. *Id.*

199. *Id.* at *2.

200. *Id.*

201. *Id.* at *4.

202. *See, e.g.*, H.K. *ex rel*. Fairwell v. Google LLC, 595 F. Supp. 3d 702, 704–05 (C.D. Ill. 2022).

203. *Id.*

204. *Id.* at 705.

205. *Id.* at 704.

206. *Id.* at 706. Google also argued that the claims were preempted by the Illinois Student Online Personal Protection Act ("SOPPA"), which "exclusively governs the collection, use, and protection of personal data, including biometric data, in Illinois K–12 schools." *Id.* The court, however, did not reach an answer on SOPPA preemption due to the unanswered threshold question regarding who a legally authorized representative under BIPA is. *Id.* at 712.

orbit[.]"[207] Thus, COPPA preempted the BIPA claims because of an express preemption provision disallowing any State or local government from imposing liability in connection with an activity described in COPPA that is inconsistent with COPPA.[208]

2. Acts, Legislation, or Regulations Not Preempting BIPA

Other attempts to preempt BIPA claims have not been as successful.[209] The following section discusses the cases and statutes wherein BIPA claims were not preempted—namely, the Illinois Workers' Compensation Act, the Medical Device Amendments of 1976, the Federal Railroad Safety Act, and Food and Drug Administration regulations.[210]

a. Illinois Workers' Compensation Act

On an interlocutory appeal in *McDonald v. Symphony Bronzeville Park, LLC*, the court considered the certified question of whether the exclusivity provisions of the Workers' Compensation Act ("WCA") barred BIPA claims for statutory damages.[211] Plaintiff Marquita McDonald was an employee of Symphony Bronzeville Park, LLC ("Bronzeville") and Symphony Healthcare LLC and used her fingerprint to clock in and out of work.[212] McDonald sued her employers alleging that they continuously violated BIPA by failing to give proper notice of the purpose and length of time her fingerprints were collected, stored, and used for, failing to provide a publicly available retention and destruction schedule, and failing to obtain a written release.[213] The WCA has two "exclusivity provisions," and the Illinois Supreme Court has indicated those provisions mean that the WCA generally provides the exclusive way in which an employee can recover against their employer for a work-related injury.[214]

However, the court held that statutory violations of BIPA escaped the exclusivity provisions by not being compensable under the WCA.[215] Relying on *Folta*,[216] determining whether an injury is compensable under the WCA is related to whether it is the type of injury that categorically fits within the purview of the WCA.[217] Significantly, that requires consideration of the character of the

207. *Id.* at 711.

208. *Id.* at 709.

209. *See infra* Subsection III.A.2.

210. *See* Illinois Workers' Compensation Act, 820 ILL. COMP. STAT. ANN 305/1–29.2 (West 2022); Medical Device Amendments of 1976, Pub. L. No. 94-295, 90 Stat. 539 (amending 21 U.S.C. §§ 301–399); 49 U.S.C. §§ 20101–20171.

211. McDonald v. Symphony Bronzeville Park LLC, 174 N.E.3d 578, 579 (Ill. App. Ct. 2020), *aff'd*, 193 N.E.3d 1253. The court only considered statutory damages from the alleged violation of statutory privacy rights and did not address actual damages. *Id.* at 582.

212. *Id.* at 579.

213. *Id.*

214. *Id.* at 583.

215. *Id.*

216. Folta v. Ferro Eng'g, 43 N.E.3d 108, 113 (Ill. 2015).

217. *McDonald*, 174 N.E.3d at 585.

injury.[218] Looking at the character of injuries under BIPA, part of the substantial force behind BIPA is its assessment of liability to private entities who fail to comply with BIPA's requirements, available without actual damages, which is designed to have a preventative and deterrent effect.[219] The court reasoned that a claim with those qualities does not "represent[] the type of injury that categorically fits within the purview of the [WCA], which is a remedial statute designed to provide financial protection for workers that have sustained an actual injury."[220] Accordingly, the WCA did not preempt McDonald's BIPA claims.[221]

b. FDA Regulations and Medical Device Amendments of 1976 to the Food, Drug, and Cosmetics Act

A motion to dismiss based in part on the theory of field and conflict preemption was denied in *Marsh v. CSL Plasma Inc*.[222] CSL Plasma is a plasma-donation business that used a donor-identification system that relied on biometric information—namely, fingerprints—to authenticate donor identities and track donations.[223] Plaintiffs Jada Marsh and Charles Hilson alleged that CSL Plasma violated BIPA by collecting their biometric information without obtaining the necessary written consent, making the required disclosures, and developing the required data retention and destruction policies.[224]

CSL Plasma argued field preemption was applicable because Food and Drug Administration ("FDA") regulations regarding plasma donation cover "donor informed consent, screening, eligibility, suitability, confidentiality, record-keeping, and storage" to the extent that the regulation could not be supplemented by state law.[225] Despite CSL Plasma's contention, the United States Supreme Court has recognized that the FDA's plasma-donation regulations are not intended to be exclusive.[226] Additionally, a statement by the FDA explained that its regulations are not intended to be exclusive to the plasma-donation industry, whose statement is dispositive unless "the agency's position is inconsistent with clearly expressed congressional intent . . . or subsequent developments reveal a change in that position."[227] Because there was no clear congressional intent to undermine the FDA's statement, there was "no textual anchor . . . suggest[ing] Congress has occupied the entire field of the plasma-donation industry."[228] Further, conflict preemption was inapplicable because CSL Plasma did not present any statute or regulation that BIPA made it impossible to comply with.[229]

218. *Id.*
219. *Id.* at 585–86.
220. *Id.* at 586.
221. *Id.* at 587.
222. Marsh v. CSL Plasma Inc., 503 F. Supp. 3d. 677, 684–85 (N.D. Ill. 2020).
223. *Id.* at 679.
224. *Id.*
225. *Id.* at 684 (internal quotation mark omitted).
226. *Id.* (quoting Hillsborough Cnty. v. Automated Med. Lab'ys, Inc., 471 U.S. 707, 714 (1985)).
227. *Id.* at 684–85 (quoting *Hillsborough Cnty.*, 471 U.S. at 714–15) (internal quotation mark omitted).
228. *Id.* at 685.
229. *Id.*

A year later, another case regarding another plasma donation company's practices was similarly decided.[230] The company's affirmative defense alleging express, conflict, and field preemption was stricken down in *Crumpton v. Octapharma Plasma, Inc.*[231] Octapharma Plasma, Inc. ("Octapharma") is a plasma-donation company that uses donated blood plasma to create treatments and therapies for various ailments.[232] Similarly to CSL Plasma,[233] Octapharma used a fingerprint scan system to create a biometric template that identified individual donors and maintained their related medical history records.[234] The fingerprint scan system was used each time an individual donated plasma.[235] Plaintiff Mary Crumpton alleged that Octapharma violated BIPA by collecting her fingerprint scan without obtaining the proper written consent and without making the required disclosures under BIPA.[236]

Using a slightly different approach than CSL Plasma, Octapharma first claimed that the Medical Device Amendments of 1976 ("MDA") to the Food, Drug, and Cosmetics Act ("FDCA") expressly preempted BIPA because it provides that no state may legislate contrary to the MDA with respect to a medical device.[237] However, the MDA regulates the use of medical devices, whereas BIPA regulates private entities in possession of biometric identifiers or information.[238] Because BIPA did not impose any requirements on the donor management software system used by Octapharma or the actual device used to remove the donor's blood and separate its component parts, express conflict preemption was inapplicable.[239]

Octapharma also failed to show that compliance with BIPA would do "major damage to clear and substantial federal interests" such to establish conflict preemption.[240] Octapharma identified no federal statutes or regulations that are incompatible with BIPA—the FDCA requires identity screening procedures but does not mandate or indicate a preference for any specific kind of method.[241] Because Octapharma was not required to utilize a biometric identity screening method, conflict preemption was inapplicable.[242] Octapharma's cursory references to the FDA's health and safety goals were insufficient to establish that Congress intended to occupy the entire field of plasma donation or biometric privacy; thus, field preemption was inapplicable.[243]

230. Crumpton v. Octapharma Plasma, Inc., 513 F. Supp. 3d 1006, 1014 (N.D. Ill. 2021).
231. *Id.* at 1014–15, 1017.
232. *Id.* at 1011.
233. *Marsh*, 503 F. Supp. 3d. at 679.
234. *Crumpton*, 513 F. Supp. 3d at 1011.
235. *Id.* at 1011.
236. *Id.* at 1010–11.
237. *Id.* at 1013.
238. *Id.*
239. *Id.*
240. *Id.* (quoting Patriotic Veterans, Inc. v. Indiana, 736 F.3d 1041, 1049 (7th Cir. 2013)).
241. *Id.* at 1013.
242. *Id.* at 1014.
243. *Id.*

c. Federal Railroad Safety Act and Interstate Commerce Commission Termination Act

In *Fleury v. Union Pacific*, Union Pacific argued on a motion to dismiss that the Federal Railroad Safety Act ("FRSA") and Interstate Commerce Commission Termination Act ("ICCTA"), coupled with certain Department of Homeland Security regulations, preempted BIPA because the combination covered the subject of biometric information as a security precaution to access railroad facilities.[244] Union Pacific required railyard visitors to scan their biometric information into identity verification kiosks, through which they collected and stored the biometric information.[245] Fleury, a truck driver who was required to use the identity verification kiosks, alleged that Union Pacific violated BIPA by failing to obtain written consent, provide the other required disclosures, and by transmitting Fleury's data to unknown third parties without consent until June 2020 when Fleury signed a disclosure and consent form.[246]

In order to make all laws regarding railroad safety as uniform as possible nationwide, the FRSA has an express preemption clause.[247] However, the clause provides that states may adopt laws related to railroad safety and security matters until specific federal regulations or orders cover the same subject matter.[248] While there are regulations that govern physical railway security access and require a transportation security plan for hazardous materials, the Court found no FRSA preemption.[249] In order to fall within the express preemption clause, BIPA would have to cover the same subject matter.[250] The Court reasoned that BIPA's subject matter is the security concern of how biometric information is collected and used, and the regulations did not address the subject.[251]

Regarding the ICCTA, Congress gave the Surface Transportation Board ("STB") exclusive jurisdiction over all rail transportation regulation.[252] The ICCTA has a broad express preemption clause, but "it does not encompass everything touching on railroads[,]" and state and local entities generally retain the right to promulgate public health and safety regulations on interstate railroads.[253] The Court determined Fleury's claim was not categorically preempted or preempted as applied because BIPA does not impose restrictions on moving property by rail or receiving property at railroad facilities.[254] Although unsuccessful at the stage it was offered, the court indicated a willingness to entertain preemption as applied at a later time when Union Pacific could provide less

244. 528 F. Supp. 3d. 885, 890 (N.D. Ill. 2021).
245. *Id.* at 888.
246. *Id.*
247. *Id.* at 890.
248. *Id.*
249. *Id.* at 890–92.
250. *Id.* at 892.
251. *Id.* at 892–93.
252. *Id.* at 893.
253. *Id.* at 894.
254. The Seventh Circuit reviews preemption issues under 49 U.S.C. § 10501 by using a two–tiered analysis offered by the STB that includes "categorical" or "*per se*" preemption and "as-applied preemption." *Id.*

speculative determinations as to the impact of creating piecemeal regulations of railway security measures.[255]

B. Potentially Contemplated Preemption Issue

Perhaps the slew of preemption arguments stemming from BIPA are themselves the best evidence to suggest that the Illinois legislature did not anticipate them.[256] However, Section 25(c) contains an exception for financial institutions and affiliates subject to Title V of the Gramm-Leach-Bliley Act of 1999 (the "Act") and its associated rules.[257] Two parallel cases illustrate both how this exception suggests the Illinois legislature did consider at least one preemption argument and defense counsels' creativity in attempting to relieve their clients of liability under BIPA.[258]

Fee v. Illinois Institute of Technology and *Patterson v. Respondus, Inc.* both involve universities as named defendants—Illinois Institute of Technology ("IIT") and Lewis University ("Lewis"), respectively.[259] Both universities claimed in motions that they qualified as "financial institutions" subject to the Act because they are significantly engaged in lending funds to consumers by way of making and administering student loans.[260] The *Fee* court determined that under the plain language of BIPA and the Act, "Section 25(c) applies to institutions of higher education that are significantly engaged in financial activities, such as making or administering student loans."[261] The *Patterson* court agreed.[262] While neither case was resolved on these motions,[263] the *Fee* court's language indicates an escape route is available if a university defendant can factually prove that it regularly makes and engages in administering student loans.[264] The fact that BIPA includes Section 25(c)'s exception suggests that the Illinois legislature did contemplate the possibility of preemption but did not possibly know or expect how comprehensively defendants would argue preemption.[265]

255. *Id.* at 895.

256. *See* discussion *supra* Section III.A.

257. 740 ILL. COMP. STAT. ANN. 14/25(c) (West 2008).

258. *See generally* Fee v. Ill. Inst. of Tech., No. 21-CV-02512, 2022 WL 2791818 (N.D. Ill. July 15, 2022); Patterson v Respondus, Inc., No. 20-C-7692, 2022 WL 7100547 (N.D. Ill. Oct. 11, 2022).

259. *Fee*, 2022 WL 2791818, at *1; *Patterson*, 2022 WL 7100547, at *1.

260. *Fee*, 2022 WL 2791818, at *2; *Patterson*, 2022 WL 7100547, at *2.

261. *Fee*, 2022 WL 2791818, at *6.

262. *Patterson*, 2022 WL 7100547, at *3–4.

263. *Fee*, 2022 WL 2791818, at *6; *Patterson*, 2022 WL 7100547, at *10.

264. *See Fee*, 2022 WL 2791818, at *6.

265. *See* Stauffer v. Innovative Heights Fairview Heights, LLC, 480 F. Supp. 3d 888, 902 (S.D. Ill. 2020) (acknowledging plaintiff's "compelling argument" that including the exception for financial institutions under the Gramm-Leach-Bliley Act was to avoid federal preemption).

IV. RECOMMENDATION

Illinois has been essentially beta testing one of the toughest biometric data privacy laws in the country for the last fifteen years.[266] While other legislation has been introduced,[267] as of April 2022, BIPA is the only biometric privacy law that provides for a private right of action.[268] Allowing a private right of action has given rise to litigation turning on statutory interpretation and construction or other ambiguity from the statute.[269] Given the slew of issues arising from BIPA and yet to come, defensive preemption is an appropriate solution.[270] Congress should review BIPA's impact in Illinois and pass legislation preempting BIPA—and all its problems, like the statute of limitations[271] and claim accrual through per-scan damages[272]—to ensure clarity and fairness for all parties. Unlike the current proposed federal legislation,[273] there should not be a carveout for states that have passed individual, specific biometric privacy statutes. This is to promote consistency across state and federal standards, which trickles down to litigation.

Hindsight is always 20/20. Like what other states have been doing by way of the legislative process,[274] Congress can review the problems BIPA created and pass federal legislation that clarifies those problems. While it is far from realistic to assume that Congress can anticipate every problem a federal biometric privacy statute could yield, it could at least work to resolve questions that have been litigated in Illinois courts.

Unfortunately, the obvious cannot be ignored—passing federal legislation is historically quite difficult.[275] In the last twenty years, Congress has only passed between 4 and 8% of bills and resolutions introduced.[276] And, approximately

266. *See Illinois Biometric Information Privacy Act FAQs*, JACKSON LEWIS, https://www.jacksonlewis.com/sites/default/files/docs/IllinoisBIPAFAQs.pdf (last visited Nov. 21, 2023) [https://perma.cc/Y8HF-5HRU].

267. Molly S. DiRago, Kim Phan, Ronald I. Raether Jr. & Robyn W. Lin, *A Fresh "Face" of Privacy: 2022 Biometric Laws*, TROUTMAN PEPPER HAMILTON SANDERS LLP (Apr. 5, 2022), https://www.troutman.com/insights/a-fresh-face-of-privacy-2022-biometric-laws.html [https://perma.cc/2GGG-W698].

268. *Id.*

269. *See, e.g.*, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1200 (Ill. 2019).

270. "Defensive preemption," a term coined by J.R. DeShazo and Jody Freeman, is a regulatory dynamic where businesses "react to statutory innovations at the state level by seeking legislation at the federal level." Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 905–06, 939 (2009).

271. *See* Tims v. Black Horse Carriers, Inc., 216 N.E.3d 845, 854 (Ill. 2023) (ruling a five-year limitations period applies to all BIPA claims); W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc., 154 N.E.3d 804, 830 (Ill. App. Ct. 2020); Bradenberg v. Meridian Senior Living, LLC, 564 F. Supp. 3d 627, 632–33 (C.D. Ill 2021).

272. Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1166–67 (7th Cir. 2021) (certifying novel state law question to the Illinois Supreme Court of whether BIPA claims accrue after each violation or only after the first violation, demonstrating desirability of specific legislative contemplation of claim accrual); Cothron v. White Castle Sys., Inc., 216 N.E.3d 918, 933 (Ill. 2023) (Overstreet, J., dissenting) (court rules that claims accrue per each BIPA violation despite potentially "harsh, unjust, absurd, or unwise" consequences).

273. *See* discussion *supra* Part I.

274. *See* discussion *supra* Section II.C.

275. *See Statistics and Historical Comparison*, GOVTRACK, https://www.govtrack.us/congress/bills/statistics (last visited Nov. 21, 2023) [https://perma.cc/8LFJ-3W3S].

276. *Id.* It is noted, however, that Congress is moving towards passing "fewer but larger bills." *Id.*

one-third of the laws being passed in the same time period consisted of ceremonial laws rather than substantive laws.[277] So while comprehensive federal legislation could solve the problem, considering alternative solutions is more pragmatic.

Another possible solution is for states implementing their own biometric information privacy statutes to simply forgo a private right of action; if there is a different method to enforce biometric privacy statutes, the need for creative preemption arguments would dissipate.[278] BIPA's impact on Illinois courts cannot be understated, and other states considering parallel legislation should assess the impact and repercussions a similarly expansive private right of action could have on its citizens. For example, California's proposed Biometric Information bill (SB 1189) was analyzed by the state's Senate Committee on Appropriations, who determined the fiscal impact would cause:

> Unknown cost pressures to the judicial branch, **potentially in the millions or tens of millions**, to adjudicate court filings generated by the provisions of this bill . . . The fiscal impact of this bill cannot be known with certainty, as the impact will be dependent on numerous factors, including, but not limited to, how many businesses currently operate in a manner that would violate the provisions of this bill, whether and when they are willing and/or able to amend their business models to comply with the bill's provisions, and how many lawsuits are generated in response to its passage. **Reports indicate that BIPA, a similar law passed in Illinois, has generated thousands of court filings, including hundreds of class-action lawsuits**. While it is not known how many lawsuits would be brought as a result of this bill, . . . an increase in workload could result in delayed court services and would put pressure on the General Fund to increase the amount appropriated to backfill for trial court operations.[279]

States should carefully consider alternative enforcement mechanisms, which might include authorization of the state's attorney general to pursue legal action to recover a civil penalty,[280] a separately established office or division of an existing government entity to monitor and enforce biometric information privacy compliance, or administrative penalties for noncompliance.

BIPA's purpose is to protect individuals from having their biometrics compromised through "regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers[.]"[281] However, plaintiffs

277. Drew Desilver, *A Productivity Scorecard for the 115th Congress: More Laws than Before, But Not More Substance*, PEW RSCH. CTR. (Jan. 25, 2019), https://www.pewresearch.org/fact-tank/2019/01/25/a-productivity-scorecard-for-115th-congress/ [https://perma.cc/P4RM-4EAA].

278. Fredric D. Bellamy, *Looking to the Future of Biometric Data Privacy Laws*, REUTERS (Apr. 6, 2022, 9:13 AM), https://www.reuters.com/legal/legalindustry/looking-future-biometric-data-privacy-laws-2022-04-06/ [https://perma.cc/E8ZF-XZ9Q].

279. SENATE COMMITTEE ON APPROPRIATIONS, 2021–2022 Regular Session, *Bill Analysis, SB 1189 (Wieckowski)—Biometric Information* (Apr. 7, 2022), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202120220SB1189# (emphasis added) (click on "Bill Analysis" ribbon; select document entitled "04/22/22- Senate Appropriations" to download) [https://perma.cc/K9Q9-GZQT].

280. TEX. BUS. & COM. § 503.001(d) (West 2017).

281. 740 ILL. COMP. STAT. ANN. 14/5(g) (West 2008).

are using the statute to claim damages for tens of thousands of dollars, even hundreds of thousands of dollars, and since claims can stand after purely technical violations of BIPA, no actual injury need occur.[282] Plaintiffs are claiming exorbitant damages without actual injury, and defense attorneys are fighting off claims with preemption arguments.[283] These fights do not truly go to the heart of the purpose of the statute: to protect the Illinois public's welfare.[284] Resolving these questions through comprehensive federal legislation, or some other enforcement and compliance mechanism, can refocus any potential litigation to true biometric privacy violations that warrant appropriate and proportionate legal redress.

V. CONCLUSION

BIPA was originally introduced to serve "the public welfare, security, and safety."[285] However, BIPA's purpose has been distorted through statutory interpretation that has served largely to hook employers with massive damages without actual injury apart from a pure statutory violation.[286] Various preemption arguments are working, but many are not.[287] This has led to analogous situations with vastly different outcomes for the same or similar injuries just because a business may be in one industry versus another.[288]

Certain strains of preemption arguments have proved successful—that includes the RLA, the LMRA, and the COPPA.[289] Others have not, such as the WCA, the MDA of 1976, the FRSA, the ICCTA, and FDA regulations.[290] The BIPA violations at issue in any given array of cases can be very similar, but being fortunate enough to be operating within a certain context can absolve a company of liability.[291]

Congress has an opportunity to correct BIPA's complications. Passing comprehensive federal biometric privacy legislation, whether by reviving and amending S. 4400 or introducing a new bill, can provide greater clarity for pending statutory questions and better protect businesses and individuals. Alternatively, states can adopt or amend their own biometric privacy laws to include enforcement mechanisms besides a private right of action. This way BIPA's original purpose can be restored, and actually protecting biometric privacy can once again be the heart and focus of related litigation.

282. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).
283. *See* discussion *supra* Part III.
284. 740 ILL. COMP. STAT. ANN. 14/5(g) (West 2008).
285. *Id.*
286. *See generally Rosenbach*, 129 N.E.3d at 1207.
287. *See* discussion *supra* Section III.A.
288. *See* discussion *supra* Section III.A.
289. *See* discussion *supra* Subsection III.A.1.
290. *See* discussion *supra* Subsection III.A.2.
291. *See* discussion *supra* Part I.