COMMENTS

Identifiable to Whom? Clarifying Biometric Privacy Rights in Illinois and Beyond

Hana Ferrero†

Illinois's Biometric Information Privacy Act (BIPA) is the country's most powerful law governing biometric data—data generated from an individual's biological characteristics, like fingerprints and voiceprints. Over the past decade, BIPA garnered a reputation as an exceptionally plaintiff-friendly statute. But from 2023 to 2024, the Illinois legislature, Illinois Supreme Court, and Ninth Circuit Court of Appeals all sided with BIPA defendants, largely for the first time. Most significantly, in Zellmer v. Meta Platforms, Inc.*, the Ninth Circuit dismissed the plaintiff's BIPA claim because the face scan collected by the defendant could not be used to identify him.*

It is unclear whether these developments represent a trend or an exception to BIPA's plaintiff friendliness. Which path is charted will largely turn on how courts interpret Zellmer. *While* Zellmer *established that a biometric identifier must be able to identify an individual, lower courts have construed its holding narrowly to require that the entity collecting biometric data must itself be able to identify using that data, rather than it being sufficient for any entity to do so. Reading BIPA this narrowly would significantly weaken the statute's protections.*

After detailing how employer and consumer cases catalyzed this recent defendant-friendly shift, this Comment proposes a two-step framework to determine whether a biometric identifier is able to identify, thereby falling under BIPA's reach. Given BIPA's broad influence, where courts ultimately land on this question will be crucial to the protection of biometric data nationwide.

† B.A. 2021, University of Notre Dame; J.D. Candidate 2026, The University of Chicago Law School. I would like to thank Jack Brake, Anne Marie Hawley, and Jonah Klausner for their thoughtful edits and Jake Holland for his indispensable advice all throughout the drafting process.

INTRODUCTION

For nearly a decade following the Illinois legislature's unanimous adoption of the Biometric Information Privacy Act[1] (BIPA) in 2008—the subject of no legislative debate and little media attention—the statute did not give rise to a single lawsuit. In 2015, a federal district court judge in Illinois remarked that he was "unaware of any judicial interpretation of the statute."[2] Fast forward to 2025, however, and BIPA is considered the most stringent biometric privacy law in the country[3]—a model state law in an area notable for the absence of uniform federal legislation. A nationwide regulatory regime has developed around the statute, with judges throughout the country ruling on many of the several thousand BIPA lawsuits filed since 2018.[4] Plaintiffs have extracted multimillion-dollar settlements under the statute from some of the most powerful national companies.[5] And businesses have changed their practices solely to avoid BIPA liability.[6] BIPA has altered the actions of courts, plaintiffs, and companies across the country. Given the continued lack of federal data privacy legislation, this influence is unlikely to change anytime soon.

The Illinois legislature passed BIPA in response to concerns about the increasing use of biometrics in the business sector.[7] The statute regulates how entities collect, use, disclose, and store biometric information—data generated by measurements of an individual's biological characteristics that is used to identify an individual—like voiceprints and fingerprints. Members of the public are hesitant about sharing this data because, as detailed in the statute, "[t]he full ramifications of biometric technology are

---

1 740 ILL. COMP. STAT. 14/1 et seq. (2024).

2 Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

3 *See, e.g.*, Rachel Metz, *Here's Why Tech Companies Keep Paying Millions to Settle Lawsuits in Illinois*, CNN (Sept. 20, 2022), https://perma.cc/XED3-NTDT ("[Illinois's] rule, passed in 2008, is seen as the toughest in the nation."); Ian A. Wright & Kaitlin H. Owen, *Labor & Employment Advisory: New Law Limits Damages Plaintiffs Can Seek Under Illinois Biometric Information Privacy Act*, ALSTON & BIRD LLP (Aug. 14, 2024), https://perma.cc/TE66-FND9 ("BIPA has gained national attention in recent years as one of the strictest biometric laws in the country.").

4 *See* Bianca Gonzalez, *BIPA One Step Closer to Seeing Its First Major Change Since 2008 Inception*, BIOMETRIC UPDATE (Apr. 12, 2024), https://perma.cc/W3VM-TRK2.

5 *See* Metz, *supra* note 3.

6 *See* Jake Holland, *Meta Disables Some Filters in Texas, Illinois Following Lawsuits*, BLOOMBERG L. (May 12, 2022) [hereinafter Holland, *Meta Disables Some Filters*], https://news.bloomberglaw.com/privacy-and-data-security/meta-disables-some-filters-in-texas-illinois-following-lawsuits.

7 *See* 740 ILL. COMP. STAT. 14/5(a).

not fully known."[8] After all, biometrics differ from other sensitive identifiers like Social Security numbers that can be changed if compromised. Once biometrics are compromised, the individual has no recourse.[9]

These concerns have long been present, accompanying the rise of modern technologies that can store and use biometric information. Law enforcement made frequent use of fingerprinting and facial recognition by the late 1960s—spurring the development of more sophisticated biometric technologies, which by the 2000s were mainstream not just in law enforcement but also in corporate, commercial, and social settings.[10] What, then, accounts for BIPA's rise to prominence over the past decade? Its statutory scheme, which includes a private right of action and significant liquidated damages, has made it an attractive tool for plaintiffs. And the courts further encouraged BIPA litigation. Since the first lawsuits were brought under the statute in 2015, almost every judicial decision interpreting BIPA has favored plaintiffs. Seminal cases drew on BIPA's private right of action, conferred broad standing to bring claims, and allowed for potentially astronomical recovery. Thus, BIPA garnered a reputation as a plaintiff-friendly statute.[11] Until 2024, there was little reason to dispute this characterization.

But multiple recent developments suggest that this plaintiff-friendly landscape may be shifting toward one that favors defendants. First, in direct response to two emblematically plaintiff-friendly cases, the Illinois legislature amended BIPA for the first time since its enactment. The amendment (1) clarifies that only one BIPA violation occurs when an entity collects or disseminates the same biometric identifier from the same individual and (2) allows collecting entities to obtain consent via

---

8 *Id.* 14/5(f).

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

10 Amanda Moen, *A Brief History of Biometrics*, BIOCONNECT (Dec. 8, 2021), https://perma.cc/FVH7-8HC8.

11 *See, e.g.*, KWABENA APPENTENG, CYLE CATLETT, DAVID HAASE, ORLY HENRY, JENNIFER JONES, MICHAEL LOTITO, SHANNON MEADE & YARA MROUEH, LITTLER WORKPLACE POL'Y INST., BIPA'S DEVASTATING EFFECTS ON ILLINOIS BUSINESSES 9 (2023) ("BIPA has long been described as a 'plaintiff-friendly' statute based on its statutory language and Illinois court decisions interpreting the Act."); David J. Oberly, *Analyzing the Impact of the BIPA Claim Accrual Decision*, BIOMETRIC UPDATE (Mar. 2, 2023), https://perma.cc/M53L-JRU6 ("[C]ourts routinely tend to favor plaintiff-friendly, expansive interpretations of BIPA.").

electronic signature.[12] Second, in *Mosby v. Ingalls Memorial Hospital*,[13] the Illinois Supreme Court held that biometrics collected from both patients and healthcare employees fall outside of BIPA's scope and are therefore unprotected by the statute. Third, and most significantly, the Ninth Circuit in *Zellmer v. Meta Platforms, Inc.*[14] ruled against a plaintiff's BIPA challenge to Meta's collection of his "face signature" on the ground that the face signature was merely a string of numbers that was not able to identify him. Rather, the face signature could at most be used to identify the plaintiff's gender and age. Since the Ninth Circuit decided *Zellmer*, lower courts have latched onto its holding but have gone even further to argue that the entity collecting the biometric identifiers must *itself* be able to uniquely identify individuals for that data to fall with the scope of BIPA, dismissing claims where the collecting entity lacks the ability to do so. While these decisions invoked different aspects of the statute, all were deemed clear wins for BIPA defendants.[15]

It is too soon to ascertain the full consequences of these developments. But the shift in defendants' favor is notable, and courts now have the chance to dictate whether these recent decisions represent a trend or an exception to BIPA's general plaintiff friendliness. In particular, the most important issue left unresolved is what it means for a biometric identifier to be able to identify an individual, because the *Zellmer* court did not have the final say on the issue—the Illinois Supreme Court and Illinois legislature could both override the Ninth Circuit's holding by adopting a different test. Therefore, which path courts take will largely be driven by the question at the heart of this Comment: Is a biometric identifier able to identify, bringing it within BIPA's

---

12 Act of Aug. 2, 2024, § 5, 2024 Ill. Legis. Serv. P.A. 103-769 (West) (amending 740 ILL. COMP. STAT. 14/10, 14/20).

13 234 N.E.3d 110 (Ill. 2023).

14 104 F.4th 1117 (9th Cir. 2024).

15 *See, e.g.*, Lori Tripoli, *Aftermath of the Ninth Circuit BIPA Liability Shake-Up in* Zellmer v. Meta, CYBERSECURITY L. REP. (Oct. 23, 2024), https://perma.cc/PH9X-R5EV ("Prospective defendants in Illinois [BIPA] cases might rest a little easier following a recent Ninth Circuit Court of Appeals decision."); *Illinois Supreme Court Issues Rare Win for BIPA Defendants*, GORDON REES SCULLY MANSUKHANI, LLP (Nov. 2023), https://perma.cc/62KA-WDWB ("[*Mosby*] comes as a positive note in the midst of an untenable landscape for BIPA defendants."); Matthew Sachaj, Mary Smigielski & Josh Kantrow, *Illinois Gov. J.B. Pritzker Signs BIPA Amendment Into Law*, LEWIS BRISBOIS BISGAARD & SMITH LLP (Aug. 5, 2024), https://perma.cc/9ZMN-RN9M ("[C]ompanies today are in a significantly better position than they were before the BIPA Amendment.").

scope, only if the collecting entity can *itself* use it to uniquely identify an individual?

Reading BIPA, as lower courts have done post-*Zellmer*, to apply only if a company could itself identify the individuals whose biometric data it collects would significantly reduce potential liability for defendants. This interpretation even threatens to hollow out the law entirely, given that BIPA cases increasingly involve situations where the collecting entity lacks the additional information (e.g., names, phone numbers, or email addresses) required to link biometric identifiers to specific individuals. That is, BIPA cases increasingly involve (1) nonusers, who are not providing any additional information to the companies that collect their biometric data, and (2) third parties that are not themselves collecting the biometric data they use but rather obtaining the data from another collecting entity.[16] If BIPA is construed to require the collecting entity to itself identify, nonusers will have no recourse when the collecting entity does not have the additional information needed to personally identify them, or passes the biometric identifier onto a third party that instead has the ability to do so. Given the rise of data aggregators and brokers, which allow for large quantities of personal information to be amassed in one place,[17] there is a high chance that a biometric identifier could be linked to an individual, even if the collecting entity itself cannot do so. This would lead to the exact harm against which the Illinois legislature intended BIPA to protect—potential compromise of immutable data—while allowing the companies that collect the biometric data to escape liability under the statute. On the other hand, reading BIPA to require only the possibility that *any* entity could use the biometric identifier to uniquely identify an individual—as this Comment argues is consistent with the statute's text and purpose—would soften *Zellmer*'s holding, limiting it to technologies like the face signatures at issue in the case.

Where courts ultimately land on this question will not just impact those residing in Illinois. With no comprehensive federal

---

16 *See infra* Part II.B.2, C.2.

17 *See* Arjun Bhatnagar, *Data Brokers: The Hidden Threat to Privacy*, FORBES (Dec. 18, 2024), https://perma.cc/VB7A-AGY9:

> Companies that aggregate and buy data are growing at a rapid pace, working without transparency or consent in how they use, share and sell personal information. . . . The fallout is visible in the rise of data breaches, with nearly 1,600 reported just in the first half of 2024—a 14% increase from the same period in 2023—and over 1 billion sensitive data points leaked.

law governing biometric or data privacy, BIPA is an indispensable model for jurisdictions considering similar legislation. In 2023, there were twenty-two biometric privacy or facial information bills proposed in states across the country.[18] Approximately half of these closely mirrored BIPA.[19] In 2024, thirteen states considered biometric privacy bills,[20] with that number likely to grow in 2025. Beyond biometrics, commentators have likened statutes including the Washington My Health My Data Act[21] (MHMDA) and the New York City Biometric Identifier Information Act[22] to BIPA. Given far-reaching reliance on BIPA, a solidified trend toward a defendant-favorable interpretation would weaken protection for this data across the country. Courts and legislatures have reason to pay close attention to the way BIPA litigation unfolds.

This Comment analyzes the recent developments that have transformed BIPA from a plaintiff-friendly statute to a more defendant-friendly one, explores the broader trends underlying these developments, and offers a path forward regarding a primary question they have left unresolved: What exactly does it mean for a biometric identifier to be able to identify an individual, bringing it under BIPA's scope? Part I introduces BIPA and other statutes that govern biometric information and data privacy. Next, Part II recounts the story behind recent interventions by the Illinois legislature, Illinois Supreme Court, and Ninth Circuit, each of which sided with BIPA defendants—largely for the first time. It outlines how unprecedented threats to companies collecting biometric identifiers, posed by both employee and consumer plaintiffs, catalyzed this defendant-friendly shift. Finally, Part III directs attention to the primary question now left open—unresolved by the Illinois Supreme Court and legislature—proposing a two-step approach for determining whether a biometric identifier falls under BIPA's reach: First, consistent with *Zellmer*'s holding, a biometric identifier is limited to those enumerated terms in BIPA's statutory definition that are able to *uniquely* identify an individual. Second, if the identifier can

---

18 *See* Joe Duball, *The Rise of US State-Level BIPA: Illinois Leads, Others Catching Up*, INT'L ASS'N PRIV. PROS. (Mar. 28, 2023), https://perma.cc/YA78-7K8D.

19 *See id*.

20 *See 2024 State Biometric Privacy Law Tracker: Tracking U.S. State Biometric Privacy Legislation*, HUSCH BLACKWELL LLP (last updated Jan. 16, 2025), https://www.huschblackwell.com/2024-state-biometric-privacy-law-tracker.

21 WASH. REV. CODE § 19.373.005 et seq. (2025).

22 N.Y.C., N.Y., ADMIN. CODE §§ 22-1201 to -1205 (2025).

indeed uniquely identify, it is covered by BIPA if *any* entity could use it to do so. Part III also offers timely guidance to federal courts while demonstrating how they will soon further weaken BIPA's protections by construing the term biometric identifier narrowly or revert toward a broader conception that restores BIPA as a pro-plaintiff statute.

I. LEGAL LANDSCAPE: OVERVIEW OF BIPA AND STATE PRIVACY LAWS

In the absence of a federal privacy law, the states have adopted a variety of regulatory approaches. Illinois's BIPA is a chief example. Part I.A sets out BIPA's key features, which other states have drawn upon in crafting their own legislation. Then, Part I.B situates BIPA within the broader privacy law landscape.

A. The Illinois Biometric Information Privacy Act

As the pioneering biometric privacy law, BIPA's statutory language and judicial interpretations have together shaped its influence. This Section first summarizes BIPA's statutory provisions. Then, it discusses three qualities in particular—a private right of action, broad standing, and generous liquidated damages—that have made BIPA uniquely impactful for plaintiffs.

1. Statutory framework.

The Illinois legislature passed BIPA in October 2008 following the bankruptcy announcement of Pay By Touch, a company that created fingerprint-based payment technology used by vendors throughout the state.[23] The announcement drew public scrutiny to the security concerns posed by this then-new technology, which stored thousands of shoppers' fingerprints and financial information.[24] In enacting BIPA, the legislature noted specific apprehension over biometrics as opposed to other identifiers, given that an individual has no recourse once their biometrics are compromised.[25] Because the risks imposed by biometric technology were not fully known,[26] the legislature found that "[t]he public welfare, security, and safety will be served by regulating the

---

[23] *See* APPENTENG ET AL., *supra* note 11, at 3–4.

[24] *See id.*

[25] 740 ILL. COMP. STAT. 14/5(c).

[26] *Id.* 14/5(e)–(f).

collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[27]

Entities covered by BIPA must comply with its five main provisions: (1) written policy, (2) informed consent, (3) sale, (4) dissemination, and (5) storage. First, an entity that possesses biometric identifiers or information must publicly disclose and comply with a written policy establishing a timeline and guidelines for destruction of this data.[28] Second, an entity that collects or obtains an individual's biometric identifiers or information must receive their consent to collect, store, or use the data.[29] Third, an entity cannot sell or otherwise profit from an individual's biometric identifiers or information.[30] Fourth, an entity cannot disseminate biometric identifiers or information without an individual's consent.[31] Finally, an entity must store biometric identifiers or information using the reasonable standard of care in the industry.[32] Note that BIPA creates an informed consent regime—the statute permits collecting and disseminating biometric data if individuals agree.

BIPA defines both "biometric identifier" and "biometric information." A biometric identifier is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[33] Biometric information is "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[34] Biometric information expressly does not encompass information derived in ways "excluded under the definition of biometric identifiers," such as writing samples or demographic data.[35] Additionally, under BIPA's recently litigated healthcare exemption, "[b]iometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996."[36] Biometric data is commonly collected for medical testing and

---

27 *Id.* 14/5(g).
28 *Id.* 14/15(a).
29 *Id.* 14/15(b).
30 740 ILL. COMP. STAT. 14/15(c).
31 *Id.* 14/15(d).
32 *Id.* 14/15(e).
33 *Id.* 14/10.
34 *Id.*
35 740 ILL. COMP. STAT. 14/10.
36 *Id.*

treatment purposes, such as to match patients to their electronic health records. Recognizing the frequency and importance of this healthcare-specific use, the legislature excluded biometric data used in the medical context from BIPA's requirements.

2. Reasons for BIPA's influence.

Three features have made BIPA particularly powerful for plaintiffs. First, BIPA's private right of action[37] provides anyone aggrieved by a violation of the statute with the right to bring a claim. This stands in contrast to other state biometric privacy laws, which specify that only the state's attorney general may bring claims on behalf of those aggrieved.[38] Under that exclusive public enforcement model, the government determines the defendants against whom it will enforce privacy laws, whereas a private right of action largely allows Illinois residents to sue any company for violations. Since state attorneys general have limited resources, they target only a few of the most egregious violators. Conversely, private plaintiffs often have the ability and incentive to target minor violations by defendants of different sizes.[39] These BIPA defendants comprise two categories: (1) employers that collected biometric data from their employees and (2) technology companies that collected biometric data from consumers.[40] Most BIPA lawsuits are class actions involving large groups of these plaintiffs who had their biometric data collected or disseminated by the same entity.[41] This allows for sizeable damage awards calculated on a per-plaintiff basis. But individual plaintiffs can and have successfully brought lawsuits under the statute as well.[42]

Second, courts have articulated a broad conception of standing under BIPA, making it easy for plaintiffs to bring claims in either state or federal court. In *Rosenbach v. Six Flags Entertainment Corp.*,[43] the Illinois Supreme Court for the first time established that a mere violation of BIPA, without any

---

37 *Id.* 14/20(a).

38 *See, e.g.*, TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2023); WASH. REV. CODE § 19.375.030(2).

39 *See* APPENTENG ET AL., *supra* note 11, at 7–8.

40 *See infra* Part II.B.2, C.2.

41 *See* Orly Henry, Jeffrey Iles, Kwabena Appenteng & Trish Martin, *Damage Control: Illinois Enacts Amendment to the State's High Risk Biometric Information Privacy Act*, LITTLER MENDELSON P.C. (Aug. 6, 2024), https://perma.cc/GY9H-XKXG.

42 *Id.*

43 129 N.E.3d 1197 (Ill. 2019).

additional injury, was sufficient for standing to bring a claim in state court.[44] Thus, an individual is "aggrieved" under § 20(a) any time an entity technically violates the statute.[45] The plaintiff-friendly conception of standing articulated in *Rosenbach* was momentous. The 2019 decision, which was the first authoritative interpretation on BIPA's standing requirement,[46] was largely responsible for opening the floodgates to a wave of BIPA cases that has not receded since. After *Rosenbach*, the number of BIPA lawsuits filed increased by 1400%.[47] Federal courts have also broadened standing for BIPA plaintiffs.[48] In *Bryant v. Compass Group USA, Inc.*,[49] the Seventh Circuit held that a plaintiff meets Article III standing requirements by pleading a violation of § 15(b)—that an entity collected or obtained their biometric data without consent—without any further injury.[50] The court reasoned that denying the plaintiff the ability to consent was "no bare procedural violation; it was an invasion of her private domain, much like an act of trespass would be."[51] In *Patel v. Facebook, Inc.*,[52] the Ninth Circuit agreed with the Seventh Circuit that a violation of BIPA's procedural requirements itself harms plaintiffs' privacy interests and thus confers standing.[53]

Third, BIPA provides for liquidated damages, meaning plaintiffs need not prove actual damages to recover substantial awards. A defendant must pay the greater of $1,000 or actual damages for each negligent violation of the statute, and the greater of $5,000 or actual damages for each intentional or reckless violation.[54] The threat of these liquidated damages,

---

44 *Id.* at 1206.

45 *Id.* (quoting 740 ILL. COMP. STAT. 14/20(a)).

46 *See* Brett M. Doran & Tiffany S. Fordyce, *Seventh Circuit Finds Article III Standing for (Some) Section 15(a) Violations of the Illinois Biometric Privacy Act*, GREENBERG TRAURIG (Nov. 30, 2020), https://perma.cc/69KN-R976.

47 KAITLYN HARGER, CHAMBER OF PROGRESS, WHO BENEFITS FROM BIPA? AN ANALYSIS OF CASES BROUGHT UNDER ILLINOIS' STATE BIOMETRICS LAW 8 (2023). There were 9 BIPA cases filed in 2018 and 134 filed in 2019. *Id.*

48 Unlike in state court, to bring a lawsuit in federal court, plaintiffs must meet the "case or controversy" requirement of the U.S. Constitution. *See* U.S. CONST. art. III, § 2, cl. 1.

49 958 F.3d 617 (7th Cir. 2020).

50 *Id.* at 626–27.

51 *Id.* at 624; *cf.* Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1155 (7th Cir. 2020) (holding that under *Bryant*'s reasoning, an unlawful retention of biometric data under § 15(a) is as concrete an injury as an unlawful collection of biometric data under § 15(b)).

52 932 F.3d 1264 (9th Cir. 2019).

53 *Id.* at 1275.

54 740 ILL. COMP. STAT. 14/20(a). A defendant that acts negligently fails to exercise reasonable care, whereas a defendant that acts recklessly acts with conscious disregard for the danger or harm to others. *See* 720 ILL. COMP. STAT. 5/4-6 to -7.

especially in the class action context, looms over potential defendants. This leads to BIPA settlements in which companies do not admit liability, yet decide against the risk of proceeding to trial. In fact, only one BIPA case has made it to the trial stage.[55] And even there, the parties ultimately settled after trial but before final judgment.[56]

Taken together, these features—a private right of action, broad standing, and liquidated damages—give any individual aggrieved by a technical violation of BIPA the potential to recover substantial damages without having to prove further harm.

B. State Privacy Laws

With BIPA's statutory scheme established, this Section zooms out to examine laws protecting sensitive information throughout the country. Since 2008, two states have enacted laws that, like BIPA, specifically address biometric information. Others have recognized the need to protect this information but have opted to do so through broader consumer and data privacy statutes. And BIPA's applicability extends even beyond states enacting or considering biometric laws. In the past couple of years, commentators have compared BIPA to statutes protecting other biometric data.

1. Laws protecting biometric data.

Several state and municipal laws specifically protect biometric data. Shortly following the passage of BIPA in 2008, Texas enacted the Capture or Use of Biometric Identifier Act[57] (CUBI). There has not been as much litigation under CUBI as under BIPA, as the Texas law lacks a private right of action. But CUBI has not been toothless. In July 2024, Texas Attorney General Ken Paxton secured a $1.4 billion settlement with Meta, which had captured the face geometry of millions of individuals without their consent.[58] This is the largest state data privacy settlement

---

[55] *See* Mike Scarcella, *BNSF Railway to Pay $75 Mln to Resolve Biometric Privacy Class-Action*, REUTERS (Feb. 27, 2024), https://www.reuters.com/legal/litigation/bnsf-railway-pay-75-mln-resolve-biometric-privacy-class-action-2024-02-27/.

[56] *See generally* Settlement and Release Agreement, Rogers v. BNSF Ry., 680 F. Supp. 3d 1027 (N.D. Ill. 2023) (No. 1:19-CV-03083).

[57] 2009 Tex. Gen. Laws 2018 (codified as amended at TEX. BUS. & COM. CODE ANN. § 503.001).

[58] *See Attorney General Ken Paxton Secures $1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data in Largest Settlement Ever Obtained*

to date.[59] In 2017, Washington State passed its Biometric Privacy Protection Act[60] (BPPA). The statute allows for recovery of up to $500,000.[61] New York City also has its own Biometric Identifier Information Act, complete with a private right of action and liquidated damages.[62] Unlike BIPA, the New York City statute includes a safe harbor under which businesses have thirty days to cure alleged violations.[63] It also requires companies to post "clear and conspicuous" signage notifying customers that their biometric information is being collected, shared, or stored.[64]

More generally, twenty states have enacted comprehensive consumer data privacy laws that regulate the handling of and clarify rights over sensitive information such as financial data, names and addresses, and other personally identifiable information.[65] The number of states with such laws in effect is on track to more than double from 2024 to 2026.[66] Many of these laws may also encompass biometric data[67] and biometric information.[68] For example, the California Consumer Privacy Act[69] (CCPA) covers biometric information,[70] meaning consumers have a right to access, delete, and opt out of the sale of this information.[71] Virginia's

---

from an Action Brought by a Single State, KEN PAXTON ATT'Y GEN. OF TEX. (July 30, 2024) [hereinafter *Paxton Secures $1.4 Billion Settlement*], https://perma.cc/TF6W-MSRH. This settlement shortly followed Paxton's creation of a team established to aggressively enforce the state's data privacy laws (including CUBI), suggesting more of these actions are likely to follow. *See Attorney General Ken Paxton Launches Data Privacy and Security Initiative to Protect Texans' Sensitive Data from Illegal Exploitation by Tech, AI, and Other Companies*, KEN PAXTON ATT'Y GEN. OF TEX. (June 4, 2024), https://perma.cc/876P-XGB8.

59 *Paxton Secures $1.4 Billion Settlement*, *supra* note 58.

60 2017 Wash. Sess. Laws 1141 (codified as amended at WASH. REV. CODE § 19.375.010 et seq).

61 *Is Biometric Information Protected by Privacy Laws*, BLOOMBERG L. (June 20, 2024), https://perma.cc/QH73-AZAT.

62 N.Y.C., N.Y., ADMIN. CODE § 22-1203.

63 *Id.*

64 *Id.* § 22-1202(a).

65 *See Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L. (Sept. 10, 2024), https://perma.cc/T3YH-773F.

66 *See* Benjamin W. Perry, Lauren N. Watson & Zachary V. Zagger, *U.S. Continues Patchwork of Comprehensive Data Privacy Requirements: New Laws Set to Take Effect over Next 2 Years*, OGLETREE DEAKINS (Aug. 6, 2024), https://perma.cc/4PH4-Y9AX.

67 *See id.*

68 *See* CAL. CIV. CODE §§ 1798.100–.199.100 (West 2025); VA. CODE ANN. §§ 59.1-575 to -585 (2024); COLO. REV. STAT. §§ 6-1-1301 to -1314 (2025); CONN. GEN. STAT. §§ 42-515 to -526 (2025); UTAH CODE ANN. §§ 13-61-101 to -404 (West 2025).

69 CAL. CIV. CODE §§ 1798.100–.199.100 (West 2025).

70 *Id.* § 1798.140(c).

71 *See id.* §§ 1798.100–.135.

Consumer Data Protection Act[72] offers similar protections for biometric data.[73] And the Colorado Privacy Act,[74] which governs collection, retention, and deletion, was amended in May 2024 to add heightened protections for biometric data.[75] While the CCPA has a limited private right of action for certain data breaches,[76] none of these state statutes contains an unfettered private right of action akin to BIPA's.

2. Laws protecting other personal data.

States have also enacted other narrowly focused privacy laws targeting health data, genetic information, and neural data. In 2023, Washington State passed the MHMDA to protect sensitive health data, including biometrics.[77] The Washington legislature recognized that "[i]nformation related to an individual's health conditions or attempts to obtain health care services is among the most personal and sensitive categories of data collected."[78] Among other protections, the statute gives consumers the right to have their health data deleted, prohibits the sale of health data without authorization, and prevents the use of geofences[79] around healthcare facilities.[80] Notably, it is the first state biometric privacy law after BIPA containing a private right of action. This has caused commentators to dub the MHMDA "BIPA 2.0."[81]

---

72 VA. CODE ANN. §§ 59.1-575 to -585 (2024).

73 *Id.*

74 COLO. REV. STAT. §§ 6-1-1301 to -1314 (2025).

75 An Act Concerning Protecting the Privacy of an Individual's Biometric Data, 2024 Colo. Sess. Laws 2101 (amending COLO. REV. STAT. §§ 6-1-1303 to -1304, -1314).

76 CAL. CIV. CODE § 1798.150(a)(1).

77 2023 Wash. Sess. Laws. 867, 867–68 (codified at WASH. REV. CODE § 19.373.010(4)). Nevada and Connecticut adopted similar healthcare privacy laws in 2023, suggesting a possible trend in this direction. However, neither contain a private right of action. *See generally* Act of June 15, 2023, 2023 Nev. Stat. 3450 (codified at NEV. REV. STAT. §§ 598.0977, 603A.400–.550); An Act Concerning Online Privacy, Data and Safety Protections, 2023 Conn. Legis. Serv. P.A. 23-56 (West) (amending CONN. GEN. STAT. §§ 42-515 to -526).

78 WASH. REV. CODE § 19.373.005(2).

79 As defined in the MHMDA, a geofence is "technology that uses . . . spatial or location detection to establish a virtual boundary around a specific physical location, or to locate a consumer within a virtual boundary." *Id.* § 19.373.010(14). Prohibiting the use of geofences helps ensure patients' privacy regarding visits to healthcare facilities (e.g., abortion clinics, substance abuse treatment, and mental health clinics) and their underlying medical conditions.

80 *Id.* §§ 19.373.40, .70, .80.

81 *See, e.g.*, Jennifer Quinn-Barabanov, Eric Berman & Shannon Reid, *BIPA 2.0? Washington's New Privacy Law Creates Private Litigation and AG Enforcement Risk for Businesses*, STEPTOE LLP (Mar. 29, 2024), https://perma.cc/9EMJ-FZVE; Andrew

Since 2023, there has also been a surge of litigation under the Illinois Genetic Information Privacy Act[82] (GIPA).[83] GIPA bans employers from soliciting, requesting, or requiring genetic testing and information as a condition of employment.[84] GIPA went into effect in 1998,[85] meaning it lay dormant, rarely used by plaintiffs, for a far longer period than BIPA. And yet, inspired by the flurry of successful litigation under BIPA, plaintiffs filed over fifty GIPA lawsuits in 2023 alone.[86] Given the lack of GIPA case law and textual similarities between GIPA and BIPA, courts have relied extensively on BIPA precedent to decide GIPA cases.[87] Similarly, plaintiff-friendly GIPA decisions spurred new lawsuits through 2024.[88]

Lastly, in 2024, Colorado and California passed bills to protect neural data.[89] While each defines "neural data" slightly differently, these laws govern information that measures an individual's central or peripheral nervous system activity.[90] The Colorado and California legislatures intended these laws as prophylactic measures—to stave off public concern over new and emerging technologies such as augmented reality headsets.[91] Like BIPA, these other tailored privacy laws are responsive to unease about similarly immutable information.

Kingman, *Washington's My Health My Data Act: Welcome to BIPA 2.0*, INT'L ASS'N PRIV. PROS. (May 8, 2023), https://perma.cc/5RYF-EWZZ.

82 410 ILL. COMP. STAT. 513/1 et seq.

83 *See* Kristin Bryan, Kyle Fath & James Brennan, *Employers and Insurance Companies Continue to Be Targeted with Deluge of Claims Under the Illinois Genetic Information Privacy Act*, SQUIRE PATTON BOGGS (May 7, 2024), https://perma.cc/3P4V-Y2BH.

84 *See* 410 ILL. COMP. STAT. 513/25.

85 Genetic Information Privacy Act, 1997 Ill. Laws 1419, 1425 (codified as amended 410 ILL. COMP. STAT. 513/1 et seq.).

86 *See* Bryan et al., *supra* note 83.

87 *See, e.g.*, Ginski v. Ethos Seafood Grp., LLC, 2024 WL 4265249, at *9 (N.D. Ill. Sept. 23, 2024); McKnight v. United Airlines, Inc., 2024 WL 3426807, at *7 (N.D. Ill. July 16, 2024).

88 *See* Bryan et al., *supra* note 83.

89 *See* Act of Apr. 17, 2024, 2024 Colo. Sess. Laws 222 (codified at COLO. REV. STAT. 6-1-1303(16.7)); An Act to Amend Section 1798.140 of the Civil Code, Relating to Privacy, 2024 Cal. Stat. 7482 (amending CAL. CIV. CODE § 1798.140).

90 COLO. REV. STAT. 6-1-1303(16.7) (defining "neural data" as "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device"); CAL. CIV. CODE § 1798.140(ae)(1)(G)(ii) (defining "neural data" as "information that is generated by measuring the activity of a consumer's central or peripheral nervous system").

91 *See* Michelle R. Bowling, Dan Jasnow & D. Reed Freeman, Jr., *California and Colorado Establish Protections for Neural Data*, ARENTFOX SCHIFF LLP (Oct. 11, 2024), https://perma.cc/M8PW-LGJB.

In sum, states have recognized the need to protect personal data, whether through biometric laws, comprehensive consumer privacy laws, or other tailored laws. These states will continue to look to BIPA as a guide, given its robust protections and the body of litigation that has developed surrounding the statute. BIPA's private right of action, broad standing, and liquidated damages have made it a particularly formidable tool for plaintiffs. But as states enact other laws safeguarding biometrics and personal information, BIPA developments have and will continue to influence their interpretations.

II. THE PERFECT STORM: EXPLAINING THE SHIFT AWAY FROM A PLAINTIFF-FRIENDLY APPROACH

Three recent developments have rapidly weakened BIPA, namely, the 2024 amendment limiting damage accrual, the *Mosby* court's expansive interpretation of BIPA's healthcare exemption, and the *Zellmer* court's articulation of what constitutes a biometric identifier. This Part describes these developments and the trends driving them. That these developments all occurred within less than a year is striking. Although there have been thousands of BIPA cases, fewer than fifty have made their way to the federal courts of appeals or the Illinois Supreme Court,[92] and there were dozens of failed attempts to amend BIPA prior to 2024.[93] Then, several blows against the previously robust BIPA regime landed at once.

Corresponding shifts in defendants' relative power underlie these changes. BIPA cases have typically fallen into two categories: claims brought by employees against employers and claims brought by consumers against technology companies. Historically, most BIPA cases had fallen into the former category. But recently, there has been an increase in the number and influence of lawsuits filed by consumers against new types of defendants, adding to the already strong interests of traditional employer defendants in combatting BIPA claims. These consumer cases have made it so that technology and social media platforms have a far larger stake in the statute. Their interests have supplemented the interests of employers, who remain the majority of BIPA

---

[92] As of April 12, 2025, Westlaw revealed nine Illinois Supreme Court and twenty-nine federal court of appeals cases that mention BIPA.

[93] *See* Daniel R. Saeedi, Rachel L. Schaller & Gabrielle N. Ganze, *Illinois Governor Signs the First Amendment to BIPA Since Its Passage 16 Years Ago*, BLANK ROME LLP (Aug. 13, 2024), https://perma.cc/B62H-SQVS.

defendants. This mix of litigation is central to the story of how BIPA began to appear so formidable that a variety of institutional actors saw fit to pare it back. Alone, neither type of case—consumer or employer—might have been threatening enough to provoke such a sudden and significant backlash. But employee and consumer cases each have aspects that *together* threatened to make BIPA a more powerful tool for plaintiffs than ever before. Employee cases raise concerns over continuous damage accrual and harm to local businesses. Consumer cases implicate considerations about larger classes and wider geographic scope.[94] Each of the recent defendant-favorable developments exemplify the impacts of these cases: the Illinois legislature was influenced by employer cases, the Illinois Supreme Court took note of both types of cases, and the Ninth Circuit was most impacted by consumer cases.

BIPA's contraction, ironically enough, began in February 2023 with the Illinois Supreme Court ruling in favor of employee plaintiffs in two emblematically plaintiff-friendly BIPA cases, *Tims v. Black Horse Carriers, Inc.*[95] and *Cothron v. White Castle Systems, Inc.*[96] However, the legislature and courts, coming to terms later that year with the unprecedented danger these cases together posed for BIPA defendants, acted swiftly. The end result of these expansive decisions for employees was an amendment that unraveled the plaintiff-favoring effects of these holdings, most influenced by the potentially disastrous impacts on Illinois employers. That November, the Illinois Supreme Court also *itself* served a blow to plaintiffs in *Mosby*. Whereas the legislature was primarily focused on employers, the court here was spurred by both employer and consumer cases. Then, in June 2024, the Ninth Circuit sided with the defendant technology company in *Zellmer*, the most important consumer case that has reached the federal courts of appeals, showing the full impact of the response to these consumer cases. Within months, these developments upended the

---

[94] While this Part focuses on the impacts of employee and consumer plaintiffs, one level removed are the plaintiffs' lawyers with their own incentives to pursue cases that result in the highest returns. Typically, these attorneys receive 20% to 40% of any BIPA settlement. HARGER, *supra* note 47, at 17. For further quantitative analysis regarding BIPA attorney fees and settlement shares, see *id.* at 16–21; and INST. FOR LEGAL REFORM, U.S. CHAMBER OF COM., A BAD MATCH: ILLINOIS AND THE BIOMETRIC INFORMATION PRIVACY ACT 6–7 (2021).

[95] 216 N.E.3d 845 (Ill. 2023).

[96] 216 N.E.3d 918 (Ill. 2023).

plaintiff-friendly landscape that had been the hallmark of BIPA litigation.

A. Illinois Legislature

The pro-defendant shift was set into motion when the Illinois Supreme Court decided two consecutive employment-related BIPA cases: *Tims* and *Cothron*. These cases together "exponentially increase[d] the already-significant risk for companies that are subject to BIPA."[97] While these decisions, at first blush, appear to only highlight courts' plaintiff-friendly inclinations, the aftermath was quite different. In August 2024, the Illinois legislature amended BIPA for the first time since its enactment more than a decade prior,[98] reversing the impact of these cases in response to the pressing concerns of employer defendants.

1. *Tims*, *Cothron*, and the 2024 BIPA amendment.

The Illinois Supreme Court's BIPA expansion began by generously construing the time limit for bringing BIPA claims. In *Tims*, the court held that Illinois's five-year catchall statute of limitations applies to BIPA.[99] An employee who worked for Black Horse Carriers from June 2017 to January 2018 alleged that the company collected and distributed his fingerprints throughout his employment without obtaining his consent, violating the statute.[100] The defendant employer argued that Illinois's one-year statute of limitations governing privacy rights applied to this claim.[101] The Illinois Code states that "[a]ctions for slander, libel[,] or for publication of matter violating the right of privacy, shall be commenced within one year next after the cause of action accrued."[102] The plaintiff instead argued for the application of Illinois's five-year catchall limitations period, which is used for statutes that lack a specified limitations period.[103] Under this provision, "all civil

---

97 Daniel K. Alvarez, Michael G. Babbitt, Laura E. Jehl, LaRue L. Robinson & Kari Prochaska, *Significant Illinois Biometric Information Privacy Act Rulings Create Additional Liability Risk for Companies*, WILLKIE FARR & GALLAGHER LLP (Feb. 21, 2023), https://perma.cc/6NTB-NC9F.

98 *See* Saeedi et al., *supra* note 93.

99 *Tims*, 216 N.E.3d at 850.

100 Tims v. Black Horse Carriers, Inc., 184 N.E.3d 466, 468 (Ill. App. Ct. 2021), *rev'd in part*, 216 N.E.3d 845 (Ill. 2023).

101 *Tims*, 216 N.E.3d at 848.

102 735 ILL. COMP. STAT. 5/13-201.

103 *Tims*, 216 N.E.3d at 850, 853.

actions not otherwise provided for, shall be commenced within 5 years next after the cause of action accrued."[104]

The court sided with the plaintiff, adopting the longer limitations period. It first focused on the text, particularly on the word "publication" in the privacy statute of limitations.[105] Section 15 of BIPA applies to the "collection, retention, disclosure, and destruction of biometric identifiers and biometric information."[106] Of these actions, only those governed by § 15(c)—sale of biometric data—and § 15(d)—dissemination of biometric data—could conceivably be seen as "publication."[107] Because the one-year statute of limitations for "*publication* of matter violating the right of privacy"[108] did not extend to all of BIPA's provisions, the court turned to practical concerns. Applying two different limitations periods to different subsections of BIPA "would create an unclear, inconvenient, inconsistent, and potentially unworkable regime."[109]

The court further concluded that BIPA's purpose supported the application of a longer statute of limitations period, citing two reasons. First, "it would thwart legislative intent to (1) shorten the amount of time an aggrieved party would have to seek redress for a private entity's noncompliance with the Act and (2) shorten the amount of time a private entity would be held liable for noncompliance with the Act."[110] Second, whereas a one-year statute of limitations makes sense for privacy torts like defamation and slander, it does not make sense for BIPA violations. When someone defames an individual, they quickly notice the harm.[111] In contrast, it is unclear when an individual will uncover evidence of a BIPA violation.[112] Although a five-year limitations period creates a broad window of potential liability for companies, this is warranted to give parties enough time to seek redress.

Just two weeks after this decision, the Illinois Supreme Court confronted a different issue in *Cothron* but similarly sided with the employee plaintiff. There, the plaintiff argued that White Castle collected and disclosed her fingerprints to a third-party

---

104 735 ILL. COMP. STAT. 5/13-205.
105 *Tims*, 216 N.E.3d at 852.
106 *Id.*
107 *Id.*
108 735 ILL. COMP. STAT. 5/13-201 (emphasis added).
109 *Tims*, 216 N.E.3d at 849.
110 *Id.* at 854.
111 *Id.*
112 *Id.*

vendor throughout her several years of employment.[113] The court held that the defendant had violated § 15(b) and (d) of BIPA with "every scan or transmission."[114] That is, every time the same employee scanned her fingerprint and White Castle collected it, a new cause of action accrued that allowed her to recover damages. The defendant had argued that a BIPA claim accrues only once, when an entity *first* collects or discloses an individual's biometric data. The plaintiff responded that BIPA's text suggests claims accrue *each* time the entity collects or discloses such data.[115]

The court admitted that this understanding of accrual upon each collection or dissemination could lead to absurd, astronomical, and even possibly unconstitutional damages.[116] Nevertheless, BIPA's text and purpose compelled this interpretation. The court reasoned that, under the plain text of § 15(b), an entity can "collect" or "capture" something more than once.[117] A system captures an employee's fingerprint each and every time they scan it. Similarly, under § 15(d), "disclosure" can happen more than once.[118] The threat of large potential damages also comports with BIPA's purpose of incentivizing entities to prevent problems before they occur.[119] To alleviate concerns over astronomical damages, the court stated that BIPA damages appeared to be discretionary rather than mandatory. The statute provides damages that a "prevailing party *may* recover."[120] A trial court would therefore have the flexibility to fashion a damage award that is enough to deter without destroying a defendant's business entirely.[121] Finally, the court expressly suggested that the legislature "review these policy concerns and make clear its intent regarding the assessment of damages under the Act."[122]

Again, while these decisions might seem to showcase BIPA's pro-plaintiff orientation, they quickly prompted a countervailing

---

113 *Cothron*, 216 N.E.3d at 920–21.

114 *Id.* at 926.

115 *Id.* at 923.

116 *Id.* at 928. Statutory damages that are so severe as to be wholly disproportionate to the offense may violate the Due Process Clause. *Id.* at 938 (Overstreet, J., dissenting from denial of rehearing); *cf.* State Farm Mut. Auto. Ins. v. Campbell, 538 U.S. 408, 425 (2003) ("[I]n practice, few awards exceeding a single-digit ratio between punitive and compensatory damages, to a significant degree, will satisfy due process.").

117 *Cothron*, 216 N.E.3d at 924–25.

118 *Id.* at 925–26.

119 *Id.* at 928–29.

120 *Id.* at 929 (emphasis in original).

121 *Id.*

122 *Cothron*, 216 N.E.3d at 929.

change. The Illinois legislature took the *Cothron* court's suggestion and passed an amendment to BIPA that Governor J.B. Pritzker signed into law.[123] The amendment clarifies that only *one* violation of § 15(b) occurs when the same entity collects the same biometric identifier from the same individual:

> [A] private entity that, in more than one instance, collects, captures, purchases, receives through trade, or otherwise obtains the same biometric identifier or biometric information from the same person using the same method of collection in violation of subsection (b) of Section 15 has committed a single violation of subsection (b) of Section 15 for which the aggrieved person is entitled to, at most, one recovery.[124]

This also goes for "a private entity that, in more than one instance, discloses, rediscloses, or otherwise disseminates the same biometric identifier or biometric information from the same person to the same recipient using the same method of collection" in violation of § 15(d).[125] For context, prior to the amendment, *Cothron* defendant White Castle could have faced up to $17 billion in damages for collecting employees' fingerprints throughout their employment—roughly twenty-five times their annual revenue.[126] After the amendment, they faced a maximum of $10 to $50 million.[127]

The amendment also clarifies that entities can obtain informed consent via electronic signature, defined as "an electronic

---

[123] Act of Aug. 2, 2024, 2024 Ill. Legis. Serv. P.A. 103-769. Unlike BIPA's initial passage, the amendment was not unanimous, passing 46–13 in the Senate and 81–30 in the House. Chris Burt, *Limit to Accrual of Biometric Data Privacy Violation Penalties a Step Away in Illinois*, BIOMETRIC UPDATE (May 20, 2024), https://perma.cc/HE2Y-DMF7. In fact, many businesses opposed the amendment for not going far enough. Hannah Meisel, *Illinois Senate Advances Changes to State's Biometric Privacy Law After Business Groups Split*, CAP. NEWS ILL. (Apr. 11, 2024), https://perma.cc/34A7-8TSQ.

[124] Act of Aug. 2, 2024, sec. 5, § 20(b), 2024 Ill. Legis. Serv. P.A. 103-769.

[125] *Id.* sec. 5, § 20(c), 2024 Ill. Legis. Serv. P.A. 103-769.

[126] *See* Alicia Kelso, *Why White Castle Beefed Up Its Late-Night Daypart Investments*, NATION'S REST. NEWS (July 12, 2024), https://www.nrn.com/quick-service/why-white-castle-beefed-up-its-late-night-daypart-investments.

[127] Tatum Andres, Nicole D. Allen, John M. Brigagliano & Amanda M. Witt, *Illinois Legislature Passes Bill Amending BIPA Violation Accrual Standards*, KILPATRICK TOWNSEND & STOCKTON LLP (May 20, 2024), https://perma.cc/B9Q4-5ZL6. This $10 to $50 million range was calculated by multiplying the number of individuals employed by White Castle within the statute of limitations period by BIPA's statutory damage awards ($1,000 for each negligent violation or $5,000 for each intentional or reckless violation). The $17 billion number was calculated by multiplying this $10 to $50 million range by an estimate of how many times these employees scanned their fingerprints over the entire duration of their employment within the statute of limitations period.

sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[128] This part of the amendment received less attention than the clarification on damages accrual, but it now allows entities to procure consent more easily, in the form of an electronic confirmation or checkbox.[129] Both parts were seen as substantial wins for defendants.[130]

2. Employee cases and the Illinois legislature's reaction.

The Illinois legislature's amendments were responsive to the strong impact of employee cases. Like *Tims* and *Cothron*, 88% of BIPA cases involve employer-employee disputes over technologies requiring employees to scan their fingerprints to clock into and out of work.[131] While employee cases have been numerous since BIPA litigation began, *Tims* and *Cothron* marked a potential sea change: these cases threatened to expose individual employers to immediate catastrophic liability and create lasting, long-term negative economic consequences for the Illinois economy. The legislature, even more so than courts, had reason to be concerned about the economic health of the state and the employers in it.

Tims and *Cothron* made it possible for employees to recover significant damages awards for BIPA violations long after the fact. This put employers at risk of possibly ruinous lawsuits bringing claims that they had previously assumed were extinguished—for example, claims brought by former employees that had not filed a BIPA claim within a year of leaving the company. To illustrate the combined effect of *Tims*'s five-year statute of limitations and *Cothron*'s articulation of claim accrual, consider an employee who scanned into work every day for three years, from 2018 through 2020. Before *Tims* and *Cothron*, the employee could not bring a single BIPA claim as of January 1, 2022. After these two cases, however, the employee had all of 2022 to sue for each and every time she scanned into work[132] (as opposed to just the

---

[128] Act of Aug. 2, 2024, sec. 5, § 10, 2024 Ill. Legis. Serv. P.A. 103-769.

[129] *See* Brett M. Doran, Tiffany S. Fordyce, Jena M. Valdetero & Zachary Pestine, *BIPA Update: Illinois Limits Liability and Clarifies Electronic Consent for Biometric Data Collection*, GREENBERG TRAURIG LLP (Aug. 14, 2024), https://perma.cc/9PLV-NMHL.

[130] *See* Sachaj et al., *supra* note 15.

[131] HARGER, *supra* note 47, at 9.

[132] Beyond just scanning into work, many workplace scenarios even involve *dozens* of scans per day, such as when a restaurant employee scans their fingerprint before placing each order. *See* Jake Holland, *White Castle Biometric Privacy Case to Shape Litigation*

first time) for all three years of her employment (not just one). Because BIPA has grown in influence since 2018, this would mean many potential plaintiffs previously unaware of any violation would be able to sue. And plaintiffs might even be incentivized to sit on their claims, allowing continued violations to stack up before suing to maximize damages.[133]

Because of this potential for astronomical damages, these decisions threatened to disrupt the state's economy. Employers have complained about BIPA's impact for years, but these complaints were far more urgent in light of *Tims* and *Cothron*. In amicus briefs filed in both cases, employers raised major concerns: businesses would feel compelled to settle meritless cases, companies would face bankruptcy,[134] thousands of Illinois residents would end up unemployed,[135] and in-state employers would avoid the use of beneficial technology or simply choose to do business elsewhere.[136]

That economic concerns loomed so large for the legislature reflected, in large part, the traditional dominance of employer cases in BIPA litigation. It is in this context that these concerns about the ability of businesses to operate in the state are most acute.[137] With employers, there is a risk of driving the company

---

Landscape, BLOOMBERG L. (Sept. 7, 2021), https://news.bloomberglaw.com/privacy-and-data-security/white-castle-biometric-privacy-case-to-shape-litigation-landscape.

[133] Data comparing employee cases before and after *Tims* and *Cothron* corroborate these concerns. 2023 saw the highest number of workplace BIPA settlements since the statute's enactment. *See* Michael Kheyfets, *Analyzing Biometric Data Privacy Class Action Settlements*, BLOOMBERG L. (Apr. 2024), https://perma.cc/V5SZ-YAVQ. And these settlements themselves resulted in higher payouts for plaintiffs. Before February 2023, 34% of workplace settlements had per-class member awards of under $1,000, averaging $838 per member. *Id.* After *Tims* and *Cothron*, 46% of workplace settlements had per-class member awards over $1,000, averaging $1,049 per member. *Id.*

[134] Brief of Amicus Curiae Illinois Manufacturers' Association et al. in Support of Defendant-Appellant White Castle Systems, Inc. at 13, *Cothron*, 216 N.E.3d 918 (No. 128004) ("An interpretation of BIPA which allows for a 'per-scan' theory of accrual or liability . . . could bankrupt Illinois businesses and cause thousands of Illinois employees to be unemployed.").

[135] *Id.*

[136] Motion of Restaurant Law Center et al. for Leave to File a Brief as Amici Curiae in Support of Defendant-Appellant at 11, *Cothron*, 216 N.E.3d 918 (No. 128004) ("Companies . . . may choose to carve out their Illinois operations when rolling out important new technology systems, or more concerningly, choose to do business elsewhere.").

[137] Technology companies also changed their business practices in response to BIPA, disabling or refusing to offer certain technological features to consumers in Illinois. *See* Holland, *Meta Disables Some Filters*, *supra* note 6 ("Meta Platforms Inc. has pulled certain augmented reality features for users in Texas and Illinois following privacy litigation in those states."); Metz, *supra* note 3 ("To avoid even the potential for violating the law, some companies have gone as far as deciding not to sell a product in the state."). But these

out of state or out of business entirely. This risk was enough to trigger a prompt response from the legislature.

B. Illinois Supreme Court

Despite its plaintiff-friendly holdings in *Tims* and *Cothron*, the Illinois Supreme Court itself, perhaps having more fully realized the expansiveness of *Tims* and *Cothron* and the increase in BIPA litigation they caused,[138] turned in a defendant-favorable direction nine months later. This shift was also due in part to the added influence of consumer cases on the Illinois Supreme Court. In *Mosby*, the court confronted the scope of BIPA's healthcare exemption. A straightforward application of BIPA's statutory language and precedent suggested that a decision for the plaintiffs was likely. Yet the court read the healthcare exemption to exclude thousands of healthcare employees' biometric data from BIPA's protection.[139] It is unclear what influenced the Illinois Supreme Court to go in this defendant-favorable direction, or whether this was due to special concerns involving the use of biometrics for common activities in healthcare settings. But although *Mosby* involved an employer-employee dispute, the decision is partially explained by the entrance of consumer cases into the BIPA arena.

1. *Mosby* and the healthcare exemption.

In *Mosby*, the court interpreted BIPA's healthcare exemption in a defendant-favorable way. A group of nurses argued that their employer required them to scan their fingerprints before providing patient care or accessing medications and did so without the nurses' consent.[140] The Illinois Supreme Court held that the healthcare exemption does not only apply to patients' biometric identifiers. Rather, the court read the exemption to extend to biometrics used for healthcare purposes generally, including the fingerprints of these nurses.[141]

The court did so despite the fact that the text of the statute and past decisions indicated that the plaintiffs had a strong BIPA

companies are less involved in the local economy by way of employing state residents and are less threatened by bankruptcy resulting from steep damages.

[138] *See supra* note 133 and accompanying text.

[139] By one estimate, 10% of Illinois's workforce lost BIPA protection as a result of *Mosby*. Hannah Meisel, *State High Court Finds Medical Personnel Exemption to Biometric Information Privacy Law*, CAP. NEWS ILL. (Dec. 1, 2023), https://perma.cc/6V28-L47Q.

[140] *Mosby*, 234 N.E.3d at 113–14.

[141] *Id.* at 123.

claim: BIPA's text references biometric information governed by the Health Insurance Portability and Accountability Act[142] (HIPAA), which naturally refers to patient, not employee, information. Prior factually similar BIPA cases concerning healthcare workers had not stretched the exemption to include those employees.[143] Yet here the court broke with both language and precedent.

In siding with the defendants, the *Mosby* court focused on the disjunctive "or" in BIPA's healthcare exemption: "Biometric identifiers do not include information captured from a patient in a health care setting *or* information collected, used, or stored for health care treatment, payment, or operations under [HIPAA]."[144] The court therefore reasoned that satisfying either condition, before or after the "or," means the biometric information is exempt from BIPA.[145] It noted that the first clause contains the word "patient"; the second does not. The first clause excludes coverage of information taken from a particular *source* ("patient in a health care setting"); the second excludes coverage of information used for a particular *purpose* ("health care treatment"), regardless of the source.

The plaintiffs had argued that "under" means "below or beneath so as to be covered or protected by."[146] Again, the information covered under HIPAA is that of patients, not employees. However, the court agreed with the defendant's definition of "under" as "subject to the authority, control, guidance, or instruction of," reasoning that HIPAA provides the guidance needed to determine the meaning of "health care treatment."[147] The court found that BIPA borrowed from HIPAA by using phrases ("health care treatment, payment, or operations") that are defined in HIPAA. Therefore, those same HIPAA definitions also apply in the BIPA context. As defined in HIPAA, these terms relate to activities performed by the healthcare provider, not the patient.[148] Biometric data of healthcare employees, when

---

142 Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

143 *See generally, e.g.*, Watson v. Legacy Healthcare Fin. Servs., LLC, 196 N.E.3d 571 (Ill. App. Ct. 2021) (failing to consider any exemption for a nursing assistant).

144 740 ILL. COMP. STAT. 14/10 (emphasis added).

145 *Mosby*, 234 N.E.3d at 119.

146 *Id.* at 120–21 (alterations omitted) (quoting Mosby v. Ingalls Mem'l Hosp., 207 N.E.3d 1157, 1169–70 (Ill. App. Ct. 2022), *rev'd*, 234 N.E.3d 110 (2023)).

147 *Id.* at 120–22 (quoting *Under*, MERRIAM-WEBSTER ONLINE DICTIONARY, https://perma.cc/6LVX-25E6).

148 *Id.* at 122–23.

collected, used, or stored for "health care treatment, payment, or operations,"[149] thus falls under the exemption.

2. The combined influence of employee and consumer cases.

Whereas the Illinois legislature was influenced by employer cases, the Illinois Supreme Court's shift was influenced by consumer cases as well. *Mosby's* holding, while involving an employer defendant, also related to an increasing number of cases filed by consumers against technology defendants. From 2019 to 2020, there were two settlements in BIPA cases involving consumers, whereas from 2022 to 2023, there were eighteen.[150] The first half of 2023 saw the highest number of consumer lawsuits filed in federal court since the statute's enactment, with corresponding increases in state courts as well.[151]

Cases brought by consumers against defendants offering services like virtual try-on technologies—where online shoppers can overlay sunglasses or other items on their face to see how those items look before purchasing them—may have led courts to parse the healthcare exemption more closely. These technologies took off during the COVID-19 pandemic and spurred related litigation in 2021 and 2022.[152] Around this time, technology defendants started to successfully advance the argument that the healthcare exemption applies to these services, primarily to items like sunglasses.[153] Along with the obvious interest of healthcare employers, these consumer cases created another reason for courts to confront the scope of this exemption—the carve-out would exempt major technology companies from liability regarding virtual try-on services. And recently, defendants in consumer cases have argued that the healthcare exemption excludes even more biometric data from BIPA's reach, arguing it extends to virtual try-ons for items like makeup and skincare products.[154]

---

149 740 ILL. COMP. STAT. 14/10.

150 *See* Kheyfets, *supra* note 133.

151 *See* BRIDGET RODDY, *AI Becomes New Focus of Employer Biometric Lawsuits*, *in* BIOMETRIC BATTLES: RISING AI & EMPLOYMENT LITIGATION TRENDS 6, 6 (2024).

152 *See* Jake Holland, *As Virtual Try-On Fashion Technology Grows, So Do Legal Risks*, BLOOMBERG L. (July 8, 2022), https://news.bloomberglaw.com/privacy-and-data-security/as-virtual-try-on-fashion-technology-grows-so-do-legal-risks.

153 *See, e.g.*, Svoboda v. Frames for Am., Inc., 2022 WL 4109719, at *2–3 (N.D. Ill. Sept. 8, 2022).

154 Jonathan Bilyk, *Amazon Can't Escape Potentially Huge Biometrics Class Action over Virtual Try-On Tool*, COOK CNTY. REC. (Apr. 5, 2024), https://perma.cc/UT7Z-7QLW.

Beyond the healthcare exemption, *Mosby* is just one instance of the interests of employers and consumer technology companies defending BIPA claims becoming increasingly intertwined. BIPA cases filed against employers have started to migrate away from simple fingerprinting scenarios toward situations that involve technologies more similar to those at issue in consumer cases, like artificial intelligence (AI). In 2021, there were no employer cases that involved AI voice or facial recognition software manufactured and marketed by these technology defendants.[155] In 2023, over one-third of employer-related BIPA lawsuits involved this technology.[156] Plaintiffs in these cases appear to be using BIPA as a tool to combat the rise in workplace surveillance via voiceprints and face scans.[157] As more employers turn to the use of AI in the workplace, these merged defendant interests may lead to even greater combined forces intent on weakening BIPA.

C. Ninth Circuit

In June 2024, the Ninth Circuit in *Zellmer* ruled in favor of technology giant Meta,[158] marking the culmination of this defendant-favorable swing. *Zellmer* brought the mounting pressure caused by consumer cases to the forefront: consumer cases have features that significantly expand BIPA's scope, both in terms of the sheer number of plaintiffs and geographic reach. Notably, these cases allow Illinois residents to sue defendants outside of Illinois, including some of the biggest and most influential companies like Meta. Recognizing the distinctive new threat facing consumer technology companies, the Ninth Circuit, like the Illinois legislature and Illinois Supreme Court, ruled against the plaintiff. District courts had reached differing conclusions as to whether a biometric identifier must be able to uniquely identify in order to fall under BIPA's reach, with some arguing this is inconsistent with BIPA's text. But the Ninth Circuit held that the ability to uniquely identify was required and that this requirement was not met in *Zellmer*. As Part III addresses in detail, while all of these recent developments are noteworthy, *Zellmer*

---

[155] BRIDGET RODDY, *Employees Fought for Biometric Privacy from AI in 2023*, *in* BIOMETRIC BATTLES, *supra* note 151, at 10, 10 [hereinafter RODDY, *Employees Fought for Biometric Privacy*].

[156] *Id.* There were also multiple lawsuits against the companies that *created* the technologies used by these employers. *Id.* For one example, see *infra* Part III.C.

[157] *See* RODDY, *Employees Fought for Biometric Privacy*, *supra* note 155, at 11.

[158] *See Zellmer*, 104 F.4th at 1126.

was not the final say on this question, and thus presents courts with an especially strong opportunity to further erode BIPA's strength.

1. *Zellmer* and the ability-to-identify issue.

In *Zellmer*, the plaintiff Clayton Zellmer filed a lawsuit in California, where Meta is headquartered, on behalf of himself and other Illinois residents.[159] Zellmer was a nonuser, meaning he himself did not have a Meta account or interact with the platform.[160] Instead, he claimed that Meta obtained his biometric identifiers when his friends uploaded pictures of him to the platform.[161] He argued that Meta did so by collecting his "face signature," a numerical sequence that represents an image of an individual's face.[162] These strings of numbers could not be reverse engineered to identify individuals.[163]

Prior to *Zellmer*, and consistent with their plaintiff-friendly slant, Illinois courts had been willing to interpret BIPA's text literally to adopt expansive conceptions of key provisions like the statute of limitations and claim accrual, despite this imposing major burdens on defendants. But here, the court did not do so when deciding whether a biometric identifier must be able to identify an individual, providing an advantage for defendants. The Ninth Circuit held that because the face signatures used by Meta were not able to identify a person,[164] BIPA did not apply, and Meta was not liable for capturing these face signatures without consent from those in the photos.[165]

The court articulated numerous justifications to reach this holding. First, Zellmer had argued that while the statutory definition of "biometric information" requires the ability to "identify an individual," the statutory definition of "biometric identifier" contains no such requirement.[166] This difference, Zellmer

---

159 *Id.* at 1121.

160 *Id.*

161 *Id.*

162 *Id.* at 1120–21.

163 *Zellmer*, 104 F.4th at 1125–26.

164 *See id.* at 1125–26.

165 *Id.*

166 *Id.* at 1123. Recall that BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier *used to identify an individual*," and "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILL. COMP. STAT. 14/10 (emphasis added).

claimed, must be considered under the canon of meaningful variation. However, the court found this argument to conflate necessary and sufficient conditions: The defined term establishes a set of necessary conditions—criteria that something must meet to be a biometric identifier.[167] But BIPA does not include items that meet these criteria if they cannot actually be used to identify someone.[168]

Next, the Ninth Circuit drew upon the U.S. Supreme Court case *Bond v. United States*[169] to look beyond the statutory definition of biometric identifier. In *Bond*, the Court relied on the ordinary meaning of "chemical weapon" rather than the statutory definition because the statutory definition was so broad as to encompass the common kitchen chemicals the defendant spread around her house.[170] As in *Bond*, the Ninth Circuit reasoned that "it is not unusual to consider the ordinary meaning of a defined term, particularly when there is dissonance between that ordinary meaning and the reach of the definition."[171] Applying this principle, the ordinary meaning of "identifier" is "one that identifies."[172] Note that this reasoning sharply diverges from cases like *Cothron*, where the court accepted the statute's plain language despite potentially absurd results.[173] Here, in contrast, the Ninth Circuit refused to accept an interpretation that would lead to (in its view) unreasonable or absurd consequences, namely that Meta would be "forced to abandon key services . . . or risk perpetual liability."[174]

The court additionally noted that the enumerated terms in BIPA's list of biometric identifiers (a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) are all unique to a person, and courts should interpret all as similarly having

---

167 *Zellmer*, 104 F.4th at 1123.

168 *Id.*

169 572 U.S. 844 (2014).

170 *See id.* at 861–62. The statute in *Bond* defined "chemical weapon" as "[a] toxic chemical and its precursors . . . ." *Id.* at 851. The kitchen chemicals used, which fell under this definition of chemical weapon, had caused the victim to "develop an uncomfortable rash." *Id.* at 852. The Supreme Court looked beyond the statutory definition to the broader context, finding that the defendant was not liable as "the global need to prevent chemical warfare does not require the Federal Government to reach into the kitchen cupboard." *Id.* at 866.

171 *Zellmer*, 104 F.4th at 1123 (quotation marks omitted) (quoting *Bond*, 572 U.S. at 861).

172 *Id.* at 1124.

173 *See Cothron*, 216 N.E.3d at 928.

174 *Zellmer*, 104 F.4th at 1124.

the ability to identify.[175] Finally, it used a federal district court decision to illustrate its holding. In *Hazlitt v. Apple, Inc.*,[176] the court held that even if a company *does not* use face scans to identify a person, BIPA applies if the company *could* do so.[177] The *Hazlitt* court rejected the defendant's argument that because it does not use customers' biometrics to identify them, it is exempt from liability.[178] The Ninth Circuit distinguished *Hazlitt* from *Zellmer* on the basis that Meta had argued it could not identify nonusers, rather than merely choosing not to do so.[179]

Zellmer countered that, even accepting this conception of a biometric identifier as capable of identifying an individual, the face signatures met this narrower definition. Zellmer provided evidence that the face signatures could be used to predict a person's age and gender.[180] But the court noted that age and gender, whether standing alone or together, are not enough to identify a person.[181]

Zellmer was the first federal appellate decision to confront the question of whether BIPA's definition of biometric identifier requires the ability to uniquely identify. Some federal district court judges have come to the opposite conclusion.[182] And the Illinois Supreme Court and legislature have not yet weighed in on the question, which would supersede *Zellmer*'s holding. On the other hand, Zellmer is still likely to influence courts in Illinois. Given that such a small number of BIPA cases have reached the Illinois Supreme Court, it is likely that courts outside the Ninth Circuit will draw on its holding.[183] Thus, it stands as a landmark decision that, depending on how other courts interpret it and whether out-of-circuit courts choose to follow it, will impose a substantial hurdle to BIPA plaintiffs.

---

175 *Id.*

176 500 F. Supp. 3d. 738 (S.D. Ill. 2020).

177 *Id.* at 749.

178 *Id.*

179 *Zellmer*, 104 F.4th at 1125.

180 *Id.* at 1126.

181 *Id.*

182 *See, e.g.*, Konow v. Brink's Inc., 721 F. Supp. 3d 752, 757 (N.D. Ill. 2024) (Pallmeyer, C.J.) (concluding that the "uniquely identifying" requirement is not "supported by BIPA's plain language"); Brown v. AS Beauty Grp. LLC, 2024 WL 2319715, at *5 (N.D. Ill. May 22, 2024) (Hunt, J.) (rejecting a "narrow[ ]" reading that requires a biometric identifier to be "capable of identifying particular individuals").

183 For an illustration of how *Zellmer* has already influenced district courts outside of the Ninth Circuit, see *infra* Part III.A.2.

2. The growing influence of consumer cases and the unique threat they pose.

In *Zellmer*, the influence of employer cases receded, and the influence of consumer cases came fully to the fore. As discussed, *Zellmer* is one of an increasing number of consumer-related cases that have altered BIPA litigation and accordingly drawn a judicial response.[184] While the majority of BIPA settlements still involve employer-employee claims, claims by consumers have grown far more influential.[185] BIPA now impacts additional powerful business interests, particularly those of social media and technology giants like Meta. The largest settlements in the past couple of years have all involved such defendants.[186]

These consumer cases often involve more class members, larger settlements, and a wider geographic reach, all of which threatened to make BIPA even more powerful for plaintiffs. Class actions involving many employees are surely common, but classes that encompass all consumers using a social media platform or website, and often even include nonusers like the plaintiff in *Zellmer*, throw the courthouse doors open to far more plaintiffs. The median class size for BIPA employment cases is 777, while the median class size for digital-consumer cases is 63,450.[187] Many class actions against social media platforms involve potentially millions of class members.[188] And unlike most claims against employers, BIPA cases brought against platforms like Meta do not require that the company be based in Illinois. Illinois residents who use these platforms can often sue no matter where the company is physically located. Therefore, unlike employee cases, these consumer cases often involve large classes of Illinois residents that sue in the defendant company's home state or where it conducts business. This opens up an entirely new class of defendants, including the major technology companies clustered on the west coast, to BIPA liability. So while claims filed by employees remain the most popular type of BIPA lawsuit, consumer claims, even in smaller numbers, are extremely impactful. The Ninth Circuit recognized the unique burdens that these cases posed to defendants, especially cases involving

184 *See supra* notes 155–57 and accompanying text.

185 *Id.*

186 *See* Seth D. Rothman, *Biometric Privacy Trends in the United States*, HUGHES, HUBBARD & REED LLP (Nov. 17, 2022), https://perma.cc/52LH-YG5Q.

187 Kheyfets, *supra* note 133.

188 *Id.*

virtual users[189] or nonusers from whom technology companies cannot easily obtain consent.

In sum, from November 2023 to August 2024—just nine months—the BIPA landscape transformed from one nearly universally favoring plaintiffs to one vindicating the interests of defendants, propelled by landmark employee and consumer cases. And these defendants' interests are becoming increasingly intertwined.[190] Employers and technology companies will continue to defend against these cases vigorously as long as they remain implicated by BIPA, and their combined incentives could weaken the statute's power even more.

* * *

The future of BIPA is now at a crossroads. Will courts build on recent developments to further undermine BIPA? Will they revert back toward the plaintiff-friendly approach that previously characterized BIPA litigation? Or will they settle somewhere in between?

The remainder of this Comment focuses on the major question left open after *Zellmer*: what it means for a biometric identifier to be able to identify an individual, thereby bringing it under BIPA's reach. This question is especially central now for three reasons. First, given that the Illinois Supreme Court and Illinois legislature have yet to settle the question, it is still live; *Zellmer* is not the final say on the issue, but it is still likely to influence lower courts. Second, it directly involves consumer cases, which are newer and less litigated, thus presenting more open questions. And third, the stakes of this question are especially high as it has the potential of weakening BIPA in cases involving nonusers and third parties.

Where courts land on this question will therefore largely dictate which path is charted. The purpose of this analysis is thus twofold: to suggest a sensible answer to courts and to illustrate how addressing these questions will enable courts post-*Zellmer* to shape BIPA's future.

---

[189] While the BIPA amendment clarified that companies may obtain consent via electronic signature, this was not the definitive interpretation of BIPA's consent requirements when the Ninth Circuit was deciding *Zellmer*.

[190] *See supra* text accompanying note 155.

III. POTENTIAL PATH FORWARD: A MIDDLE-GROUND CONCEPTION OF THE ABILITY TO IDENTIFY

This Part turns to the primary question facing courts and BIPA plaintiffs: What exactly does it mean for a biometric identifier to be able to identify an individual? *Zellmer* did not fully settle the question. On one hand, courts have and will continue to look to *Zellmer* as important authority because of the very limited number of cases that have reached the Illinois Supreme Court. On the other hand, some courts could still viably go in a different direction, as *Zellmer* is not binding on courts outside the Ninth Circuit. The Ninth Circuit established that a biometric identifier must do more than determine general demographic information, such as the age and gender of an individual,[191] but it did not explicitly hold that the standard requires the ability to identify a person by name. Lower courts have disagreed as to whether biometric identifiers must be able to uniquely identify and what this entails.[192] It therefore remains unclear where courts should draw the line.

The lower courts that have cited *Zellmer* so far have all applied it narrowly, suggesting this defendant-friendly trend could be exacerbated. These courts have found that the entity collecting the biometric identifier must *itself* be capable of identifying an individual, as opposed to it being feasible for *any* entity to do so, despite the fact that *Zellmer* did not suggest this was required. This interpretation risks weakening BIPA almost entirely, given the prominence of BIPA cases now involving (1) nonusers who by definition do not provide any other personal information to collecting entities and (2) third-party vendors that collect biometric data and pass it onto other entities that could use it to identify. The rise of aggregated databases of personal data increases the likelihood that biometrics could be compromised in a personally identifying way, but with the defendants escaping liability under BIPA because they themselves cannot use the data to uniquely identify. Companies could evade liability while collecting biometric data from millions of nonusers or while passing the biometric data on to a third party that itself uses it to identify individuals, so long as the collecting company cannot. Because

---

[191] *See Zellmer*, 104 F.4th at 1126.

[192] Some lower courts have dismissed the "uniquely identifying" requirement as unsupported by BIPA's text, articulating an even more plaintiff-friendly understanding. *See supra* note 182.

Zellmer itself neither explicitly mandated nor rejected such a narrow approach, lower courts have gone both ways on the question.[193] The Illinois Supreme Court and legislature have not weighed in, but it is not too late for other courts to draw on *Zellmer*'s holding without adopting this narrow requirement.

This Part proposes a two-step middle-ground approach to determine if a biometric identifier can identify within the meaning of BIPA. At step one, biometric identifiers are narrowly defined to include only those enumerated in BIPA's statutory definition, which requires that the identifier be linkable to a specific individual. This is consistent with *Zellmer*'s holding. But at step two, these biometric identifiers encompass those that the collecting entity or others could use to uniquely identify an individual. The *Zellmer* court did not rule on this point. Part III.A details how this two-step framework remains faithful to *Zellmer*'s holding, while reaching it under a more straightforward application of BIPA's text. Then, Part III.B draws on two recently filed BIPA cases to demonstrate the benefits of the framework. Lastly, Part III.C responds to counterarguments that this two-step framework would be impractical to administer or would expose entities to excessive liability. Again, this discussion aims to both (1) clarify what constitutes a biometric identifier under BIPA and (2) exemplify the crucial role of courts in dictating whether future BIPA developments further favor defendants or swing back toward a more plaintiff-friendly conception.

A. The Framework

To ascertain what constitutes a biometric identifier falling under BIPA's statutory definition, courts should require that (1) a biometric identifier must be able to uniquely identify, but that (2) a biometric identifier falls under BIPA if *any* entity can use it to uniquely identify. Once a court has determined at step one that a biometric identifier falls under BIPA's statutory definition and can uniquely identify an individual, then at step two, the court must ask who is capable of using this data to identify. If any entity is able to use the identifier to uniquely identify, rather than just the collecting entity itself, then BIPA applies to these biometric identifiers.

---

[193] *See supra* note 182.

1. Step one: a biometric identifier must be able to uniquely identify an individual.

Step one asks whether a biometric identifier can be linked to a *specific* individual, rather than just a demographic profile or portion of the population. Here, the term biometric identifier is limited to the categories enumerated in BIPA's statutory definition (i.e., retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry). This ability to be linked to a specific individual means that biometric identifiers must be able to uniquely identify.

The ability to uniquely identify an individual is therefore inherent in BIPA's definition of biometric identifier. All of these enumerated terms can be linked to a specific individual. However, the Ninth Circuit in *Zellmer* relied primarily on the ordinary meaning of "identifier," despite the statute's specific definition. After discussing the Supreme Court's *Bond* decision to justify this conclusion, the court briefly noted:

> Each of the listed items—retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry—are unique to a person. Each can thus be used to identify a person in the proper context. Generally, the words in a list should be given similar meanings. The unifying theme behind each term here is that each identifies a person.[194]

This reasoning alone, without looking beyond the statutory definition, is persuasive. The Ninth Circuit's interpretation of this definition is enough to support the conclusion that the text requires a biometric identifier to uniquely identify an individual. The definition only encompasses—and thus BIPA only implicates—identifiers that an entity could use to uniquely identify an individual.[195] To uniquely identify means that the biometric identifier can be used to link back to one specific person, rather than merely their age, gender, or other demographics.

This understanding helps differentiate the face signatures at issue in *Zellmer* from the "scans of face geometry" that are able to uniquely identify, like those used for many virtual try-on features. Meta's face signature, a string of numbers representing an image,

---

[194] *Zellmer*, 104 F.4th at 1124 (citation omitted).

[195] BIPA also lists a number of items ("writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color") that are beyond the statute's reach. 740 ILL. COMP. STAT. 14/10.

was not a "scan of face geometry" falling within the statutory definition. As Judge Ryan Nelson noted in *Zellmer*, face signatures are abstract, numerical representations of a face, but they cannot reveal information about actual face geometry.[196] Not all "face scans" are a "scan of face geometry" under BIPA because "scans of face geometry" are, by definition, able to uniquely identify.

As an additional example of this narrow step one inquiry, in *Martell v. X Corp.*,[197] the plaintiff alleged that the social media platform X created a unique digital signature (called a hash) of a photograph he uploaded to the platform without his consent.[198] This hash was then compared against hashes of other photographs to find copies of the same image.[199] The plaintiff argued that the hash was a photo scan falling within BIPA's scope.[200]

However, a federal district court in Illinois rejected the plaintiff's claim at the motion to dismiss stage. The court found that because BIPA only applies to the list of identifiers enumerated in the statutory definition, the plaintiff was required to show that X scanned face geometry capable of identifying, and not just a photo:

> If the scan merely compares the image to see if it is the same as other images, that does not imply the use of facial geometry. If, instead, [X] identifies and scans the facial geometry of individuals in the photos and the hash saves those facial geometry scans, then it could be a biometric identifier under BIPA.[201]

Because the plaintiff's complaint failed "to sufficiently allege that the [ ] hashes consist of a scan of face geometry that could be used to identify an individual,"[202] these hashes did not fall within BIPA's definition of biometric identifier. In sum, at step one, a biometric identifier must be specifically enumerated in BIPA's statutory definition, meaning it must be "a retina or iris scan,

---

196 *Zellmer*, 104 F.4th at 1120–21.
197 2024 WL 3011353 (N.D. Ill. June 13, 2024).
198 *Id.* at *2.
199 *Id.*
200 *Id.* at *1.
201 *Id.* at *3.
202 *Martell*, 2024 WL 3011353, at *4.

fingerprint, voiceprint, or scan of hand or face geometry"[203] able to uniquely identify an individual.[204]

2. Step two: a biometric identifier is able to uniquely identify an individual if any entity can use it to do so.

Once a court has determined at step one that a biometric identifier falls under BIPA's statutory definition and can uniquely identify an individual, the court at step two must ask *who* is capable of identifying. At this stage of the inquiry, courts should deem a biometric identifier able to uniquely identify if any entity could use it to uniquely identify an individual. Given the power of data aggregation, there is a significant difference between a rule that the entity that collects biometric information must itself be able to link it to a unique individual and a rule where the collector is liable so long as anyone could use the biometrics, along with other personal information, to do the linking.

With the pervasiveness of data aggregators and brokers, it does not matter if the entity collecting the identifier has the means to link it to an individual's name. If some other entity does, the potential damage would be equally severe. Again, this step two requirement comports cleanly with BIPA's statutory definitions and text, which simply prohibit an entity from collecting information that could possibly identify, without specifying by whom. While *Zellmer* seems to suggest that any entity being able to identify an individual would be enough to meet the statutory definition, the language in *Zellmer* could also support the alternative narrower interpretation, requiring the collecting entity to

---

203 740 ILL. COMP. STAT. 14/10.

204 Additionally, this conception of a biometric identifier as able to *uniquely* identify an individual brings BIPA in line with state laws across the country. *See* WASH. REV. CODE § 19.375.010(1) (covering "data generated by automatic measurements of an individual's biological characteristics . . . that is used to *identify a specific individual*" (emphasis added)); CAL. CIV. CODE § 1798.140(c) (defining biometric information to include "an individual's physiological, biological, or behavioral characteristics . . . that is used or is intended to be used . . . to establish *individual identity*" (emphasis added)); VA. CODE ANN. § 59.1-575 (covering "data generated by automatic measurements of an individual's biological characteristics . . . that is used to *identify a specific individual*" (emphasis added)); COLO. REV. STAT. § 6-1-1303(24)(b) (covering "biometric data that may be processed for the purpose of *uniquely identifying an individual*" (emphasis added)); CONN. GEN. STAT. § 42-515(3) (covering "data generated by automatic measurements of an individual's biological characteristics . . . that are used to *identify a specific individual*" (emphasis added)); UTAH CODE ANN. § 13-61-101(6)(b) (covering "data . . . that are generated by automatic measurements of an individual's . . . unique biological pattern or characteristic that is used to *identify a specific individual*" (emphasis added)).

itself be able to uniquely identify. The *Zellmer* court did not have to address the question—it was enough that no one could use the face signatures to uniquely identify an individual. So, given the lack of input from federal courts of appeals, the Illinois Supreme Court, or the Illinois legislature on the issue, courts can remain consistent with *Zellmer*'s holding while adopting this more expansive second step.

But all of the lower court decisions citing *Zellmer* have adopted this alternative narrow approach, concluding that the defendant company must itself have the means of uniquely identifying individuals. These lower courts focused heavily on what additional identifying information the plaintiffs had given the defendant companies beyond just their biometric data.

First, in *Tibbs v. Arlo Technologies, Inc.*,[205] plaintiff delivery drivers claimed that Arlo—which sells home security cameras—collected their face and hand scans without their consent whenever they delivered to a home equipped with Arlo's system.[206] Arlo argued the plaintiffs had failed to allege that "Arlo itself is capable of using the scans to determine Plaintiffs' identities—*e.g.*, their names, phone numbers, email addresses."[207] Rather, the plaintiffs had merely alleged "an implausible hypothetical situation in which Arlo could use its facial recognition technology to match Plaintiffs' faces to their photos on public facing social media profiles."[208] The court seemingly agreed with this interpretation, but it held that the plaintiffs had met their burden by providing allegations "regarding Arlo's capacity to identify individuals using its scans," therefore denying Arlo's motion to dismiss.[209]

Second, in *G.T. v. Samsung Electronics America, Inc.*,[210] a federal district court in Illinois dismissed the plaintiffs' complaint alleging that Samsung failed to obtain their consent before creating a digital representation called a "face template" on photographs taken with their devices.[211] Although the face template would pass at step one (since one could use individuals' images and compare them with known identities in other photos to uniquely identify),[212] the court noted that the plaintiffs must also

---

205 2024 WL 3218650 (N.D. Cal. June 27, 2024).
206 *Id.* at *1–2.
207 *Id.* at *7.
208 *Id.*
209 *Id.* at *7, *9.
210 742 F. Supp. 3d 788 (N.D. Ill. 2024).
211 *Id.* at 793.
212 *Id.*

"allege that [the] defendant's collection of their biometric data made defendant capable of determining their identities."[213] In addition to relying on *Zellmer*, the court drew on a district court case, *Daichendt v. CVS Pharmacy, Inc.*[214] In *Daichendt*, plaintiffs argued that CVS collected scans of face geometry via their photo system used for passport photos.[215] However, the plaintiffs failed to allege that CVS had an identifier, "such as their names or physical or email addresses, that could connect the voluntary scans of face geometry with their identities."[216] The *Daichendt* court concluded that the plaintiffs thus "failed to plead the most foundational aspect of a BIPA claim."[217] But in the *Daichendt* plaintiffs' amended complaint, the plaintiffs explained that they had entered "their names, email addresses, and phone numbers into a computer terminal inside defendant's stores prior to scanning their biometric identifiers."[218] This was sufficient to state a claim.[219] Similarly to the *Daichendt* plaintiffs, because the *G.T.* plaintiffs failed to assert that they provided any information that would allow for identification by Samsung, the court dismissed their claim.[220]

Third, in *Hartman v. Meta Platforms, Inc.*,[221] the plaintiffs argued that Meta collected scans of face geometry to superimpose filters onto users' faces without their written consent.[222] Meta responded that they did not have personal information that would enable them to actually match the scans to individual users.[223] As in *Tibbs*, the court accepted that Meta must itself have the ability to link the scans to users, but found this requirement was satisfied. The plaintiffs had adequately alleged that they provided Meta with such data: while "more information would have been helpful," the plaintiffs had at least explained that they created usernames and passwords and provided children's names for the kids version of the account.[224] In *Hartman*, as in *Tibbs* and *G.T.*,

---

213 *Id.* at 801 (emphasis omitted) (quoting Daichendt v. CVS Pharmacy, Inc., 2022 WL 17404488, at *5 (N.D. Ill. Dec. 2, 2022)).

214 2022 WL 17404488 (N.D. Ill. Dec. 2, 2022).

215 *Id.* at *1.

216 *Id.* at *5.

217 *Id.*

218 *Id.* at *1.

219 *Daichendt*, 2022 WL 17404488, at *1.

220 *Samsung*, 742 F. Supp. 3d at 801.

221 2024 WL 4213302 (S.D. Ill. Sept. 17, 2024).

222 *Id.* at *1–2, *11.

223 *Id.* at *11.

224 *Id.* at *12.

the court inquired into what identifying information beyond biometric data had been provided to the defendant companies.

Hartman further demonstrates that there will inevitably be hard cases even under this framework. In *Hartman*, Meta had also contended that their technology merely estimated the locations of parts of a person's face, without the capability to identify.[225] The court acknowledged that "[t]his contention may well be validated in discovery."[226] But at the motion to dismiss stage, it was sufficient that an "estimation of the location of parts of users' faces based on a scan of their face is intrinsically unique and could plausibly be used to identify them."[227] Additional fact-finding and investigation will be needed for these edge cases, and more of these cases may therefore survive the motion to dismiss stage if the biometric identifiers could possibly be used to uniquely identify. However, the purpose of discovery should be to determine whether it is feasible for any entity to identify an individual, at which point summary judgment will often be dispositive.

These three courts are not the only federal district courts that have concluded that the collecting entity must itself be able to identify individuals,[228] even though *Zellmer* itself did not address this question. But because of the increasing number of BIPA cases involving virtual users and nonusers, this conception is too narrow. If there is a chance another entity could uniquely identify, the risks of compromising this data still loom large. Other courts can and should viably adopt this two-step approach, while still remaining faithful to *Zellmer*'s holding.

B. Application

This Section applies the two-step framework to two recent BIPA cases—one in the employee context and one in the consumer context. First, the plaintiff employees in *Perry v. Omnitracs, LLC*[229] alleged that Omnitracs's in-vehicle cameras collected scans of their face geometry to detect their behavior while driving.[230] Second, the plaintiff consumers in *Pierce v.*

---

[225] *Id.* at *11.

[226] *Hartman*, 2024 WL 4213302, at *11.

[227] *Id.* (quotation marks omitted).

[228] *See, e.g.*, Castelaz v. Estée Lauder Cos., 2024 WL 136872, at *7 (N.D. Ill. Jan. 10, 2024); Clarke v. Aveda Corp., 704 F. Supp. 3d 863, 866 (N.D. Ill. 2023).

[229] No. 1:24-CV-07998 (N.D. Ill. *dismissed* Feb. 25, 2025).

[230] Complaint at 1–4, *Perry*, No. 1:24-CV-07998 (N.D. Ill. Sept. 3, 2024) [hereinafter Perry Complaint].

Photobucket, Inc.[231] alleged that Photobucket's photo-sharing platform collected their biometric identifiers, which were sold to companies developing generative AI models.[232] These cases both help exhibit how the framework operates in practice.

In *Perry*, the plaintiff truck drivers worked for various employers, all of which used Omnitracs's cameras to detect driver behavior.[233] Omnitracs, not these employers, allegedly collected the biometric identifiers. The plaintiffs argued that Omnitracs (1) collected "scans of facial geometry" in violation of BIPA § 15(b) and (2) transferred this biometric data to the company that acquired Omnitracs in violation of § 15(d).[234] The plaintiffs did not consent to this collection or disclosure.[235]

While *Perry* was voluntarily dismissed before the court reached the merits, the two-step framework would have suggested that Omnitracs was not liable under BIPA. These face scans, like the data at issue in *Zellmer*, do not appear able to uniquely identify. The plaintiffs made multiple claims about how Omnitracs uses the face scans to "identify driver behaviors": they "identify drowsiness, sleep, phone use, cigarette use, seatbelt use, and other safety-critical behaviors, as certain critical trigger events"[236] and "identify, for example, if the driver's eyes are closed or if the driver is looking down."[237] However, it does not appear that the face scans can be used to identify specific drivers. Instead, Omnitracs is using algorithms to detect where eyes and other face features are located, and to detect movements and behaviors, rather than unique features themselves. This is more akin to object detection than to identifying and storing information regarding specific faces of the drivers. If a "scan of face geometry" must be able to uniquely identify, then all of these allegations fall short, and step one of this approach is not met. These are not "scans of face geometry" within BIPA's enumerated list, as required by step one. To be sure, *Perry* would have been a closer case on the merits than *Zellmer*, where the face signatures could at most identify age and gender. But the ability to

---

231 No. 1:24-CV-03432 (D. Colo. *filed* Dec. 11, 2024).

232 Complaint at 1–3, 26–28, *Pierce*, No. 1:24-CV-03432 (D. Colo. Dec. 11, 2024) [hereinafter Pierce Complaint].

233 Perry Complaint, *supra* note 230, at 1, 6.

234 *See id.* at 4, 7–8.

235 *Id.* at 4.

236 *Id.* at 2.

237 *Id.* at 3.

determine only *behaviors* and not *identities* is insufficient to ultimately bring the face scan under BIPA's reach.

Notice that, if step one was in fact met, the inquiry at step two depends only on whether any entity can use the biometric data (here, the face scan) to uniquely identify. The employers using these cameras are presumably able to link the captured behaviors to their individual drivers, because they have additional information on their own employees. Omnitracs, the company that provided the technology used to capture the face scans, is seemingly unable to link these face scans to individual drivers because these drivers have no separate connection with Omnitracs. But if these face scans could uniquely identify drivers and not just their behaviors, then Omnitracs, even as the technology supplier and not the entity *using* the data, should have still been liable, as it collected the biometric identifiers via its cameras. It would contravene BIPA's purpose not to hold Omnitracs liable just because it has no other information that could identify these drivers, as a narrow interpretation would suggest. If Omnitracs were allowed to collect this biometric data, drivers would be left without redress if the data was compromised and used to uniquely identify them. On the other hand, assuming there is no ability to link driver behaviors to driver identities, these benefits flow without risk that, say, if Omnitracs leaked the data regarding behaviors and movements captured by these cameras, outside parties could use it to identify individuals. Then, companies like Omnitracs can continue to use driver monitoring technology for important functions like vehicle safety, efficiency monitoring, productivity, and customer service.

Turning next to *Pierce*, the case presents the same underlying question as *Perry*: whether the face scans collected by a technology company—here, Photobucket—can uniquely identify. Photobucket sold these face scans to third parties for "artificial intelligence and machine learning training."[238] The complaint names two distinct classes of plaintiffs, (1) users who uploaded their images to Photobucket's website and (2) nonusers who appeared in these photos but did not have Photobucket accounts.[239] Photobucket's policy gives it the right to license this content "to third parties for . . . extracting physical features, e.g. measurements, of [ ] Biometric Information (e.g., face, iris, etc.)."[240] The

---

238 Pierce Complaint, *supra* note 232, at 21.

239 *Id.* at 22.

240 *Id.* at 16.

plaintiffs claim that they did not consent to this policy.[241]

Unlike *Perry*, the crux of the complaint is that parties can use this biometric data to uniquely identify. Recall that if there is the ability to uniquely identify, then step one of this approach is satisfied—these are scans of face geometry that fall under BIPA's definition of biometric identifier. The plaintiffs claim that third parties can use the biometric data "to create biometric facial recognition databases that intrude on Plaintiffs' privacy by identifying them wherever they go."[242] The point of these AI systems is facial recognition, which presumably involves the ability to use the face geometry to identify specific individuals. If these scans of face geometry can uniquely identify, then BIPA applies to the face scans of both user and nonuser plaintiffs.

To reiterate once more, at step two, the identity of the party with the ability to identify individuals should not be dispositive. The complaint names as defendants both Photobucket and the entities that used the data to train AI systems.[243] Even if certain defendants do not have the ability to uniquely identify, liability flows to the collector if any entity could do so, including these AI systems. The contrary result—allowing these companies to escape liability while still collecting and using biometric identifiers without consent—weakens BIPA's protection in these increasingly common situations involving nonusers and third parties.

These case studies are generalizable. Employee-monitoring technology like that at issue in *Perry*, especially combined with the use of AI, is becoming common across industries and as the subject of BIPA lawsuits.[244] As for *Pierce*, some of the highest-profile BIPA cases of late involve the use of biometric data for AI training. For example, *Pierce* is comparable to the ongoing "Diversity in Faces" saga, in which plaintiffs claim many of the largest technology companies used datasets that contained their

---

[241] *See id.* at 18–19. *Pierce* displays a fortuitous benefit of the two-step framework: harmony across state lines. The *Pierce* plaintiffs are suing under BIPA "and similar provisions of New York, California, and Virginia law." *Id.* at 3. Their complaint extensively draws on BIPA when discussing claims under these other laws. Using a consistent conception of biometric identifiers as able to uniquely identify keeps the analysis for parties and courts applicable across states.

[242] Pierce Complaint, *supra* note 232, at 1.

[243] *Id.* at 4–5.

[244] *See* BRIDGET RODDY, *AI Surveillance Gains Ground in Employees' BIPA Suits*, *in* BIOMETRIC BATTLES, *supra* note 151, at 8–9.

biometric identifiers.[245] The framework bears on ongoing cases and those that will likely become more prevalent in future years.

C. Counterarguments

One potential concern raised by this two-step approach is that it will sweep too broadly—leading to the exact impacts the Illinois legislature and courts pushed back against—overwhelming courts, imposing excessive liability on businesses, and being infeasible to administer. A narrow approach, requiring that the collecting entity itself be able to do the linking, would allay these concerns.

To be clear, BIPA was not meant to deter the use of biometric data entirely. The legislature recognized that the use of biometric data "appears to promise streamlined financial transactions and security screenings."[246] And it acknowledged that the public's concern arises "when such information is tied to finances and other personal information."[247] Biometric data can serve as an extra layer of security and make transactions more convenient for entities, consumers, employers, and employees.[248] Businesses should not lose the incentive to employ these technologies properly. Excessive liability would also end up harming consumers who enjoy using these types of time- and laborsaving services.

Two points together mitigate the concern that this test will sweep too broadly. The first is the narrowness of the step one inquiry. Because identifiers are limited to the list enumerated in BIPA, entities like Meta, Omnitracs, and X will steer clear of liability as long as the technologies deployed are akin to face signatures in *Zellmer* that cannot identify. As technology evolves, features like face signatures and hashes will ideally become more feasible, courts will develop a better understanding of technology that is not capable of uniquely identifying, and companies will be incentivized to use these technologies to provide benefits to their consumers. If these technologies cannot uniquely identify, then step one is dispositive, with no need for further examination of liability at step two. Even though it might be time intensive to discover whether a biometric identifier can uniquely identify, this is relevant only to the step one inquiry, which *Zellmer* suggests

---

[245] *See* Vance v. Google LLC, 2024 WL 5011611, at *1–2 (N.D. Cal. Dec. 5, 2024).

[246] 740 ILL. COMP. STAT. 14/5(a).

[247] *Id.* 14/5(d).

[248] *See* Duball, *supra* note 18.

must be conducted in every case. There is little additional work or discovery that would overwhelm courts at step two. And, while consumer cases have recently become much more prominent, most BIPA cases are still employee-fingerprint cases, where the ability to uniquely identify an employee is almost always met. That the test is more relevant to consumer cases suggests there will not be so many of these cases as to overwhelm courts with unwieldy discovery.

Second, it is important to recall that BIPA establishes an informed consent regime. Even if entities do not wish to or cannot feasibly use technologies like those at issue in *Zellmer*, they can instead collect and use biometric data, even data that meets step two of the framework, as long as they obtain consent to do so. The majority of BIPA cases are those involving claims by plaintiffs that companies did not obtain their consent under § 15(b) and (d), meaning that all the companies had to do to avoid these claims was obtain customer consent. And consent is now even more feasible via written signature, online form, or check box. Obtaining consent still presents a hard question in the case of nonusers, from whom obtaining written consent is infeasible, if not impossible. But the fact that most users will likely opt in when asked for consent gives companies the flexibility to at least collect and use the biometrics of these consumers.

The narrowness of the step one inquiry, coupled with BIPA's informed consent regime, suggests the following: Companies will often be able to collect biometrics from users, as long as they take the minimally burdensome steps to obtain consent. Relatedly, in cases involving third-party vendors, companies can communicate with vendors to require that those vendors obtain consent. If a company uses a vendor to collect biometric identifiers, the company should ensure that the vendor obtains consent from users as a condition of their contract. It is in these increasingly common nonuser contexts where companies will have to limit their use of biometrics. But again, this comports with the purpose of BIPA's informed consent regime; it is *more* problematic if individuals have their biometric data collected and potentially compromised without even knowing they provided this data in the first place. Therefore, companies could either (1) move toward technologies like those in *Zellmer*, *Martell*, and *Perry* or (2) adopt *different* technologies for different parties, using technological features that require biometric data for users but not nonusers.

Another closely related concern involving the workability of this two-step approach involves the need for a limiting principle to avoid imposing liability on an endless string of defendants: How far does liability extend? If biometric data passes from one party to another, is the receiving party liable for the former's BIPA violation? What about a cloud provider that stores the biometric database of a BIPA violator—is it liable? Again, given the rise of data aggregation, it is important to deter *all* companies who could potentially mishandle biometric information. This is often where the real injury will occur: once other companies beyond the initial collector take possession of the biometric data and can use it to uniquely identify. However, liability should be reduced for those companies that do not need to be deterred as much from future BIPA violations.

Two points alleviate this worry about endless liability. First, BIPA has a mens rea requirement,[249] meaning entities that are not at least negligent in their collection or use of biometric data will not pay liquidated damages. For example, if biometric identifiers are stored on a party's cloud server where it would be unreasonable for the party to even know they had come into possession of this data, this should exempt them from BIPA's liquidated damages provisions. Courts have generally concluded that BIPA plaintiffs do not need to allege mens rea on the face of their complaints,[250] meaning some of these cases may move through litigation before mental state can be proven. But there is at least some mechanism for making sure that damages are not imposed beyond those companies that acted negligently or recklessly.

Second, the Illinois Supreme Court's articulation in *Cothron* that damages are discretionary, rather than mandatory, under BIPA has taken hold.[251] This gives judges the ability to hear

---

[249] Recall that parties may recover damages against an entity that negligently, intentionally, or recklessly violates BIPA. 740 ILL. COMP. STAT. 14/20(a).

[250] *See, e.g.*, Kyles v. Hoosier Papa LLC, 2023 WL 2711608, at *7 (N.D. Ill. Mar. 30, 2023) (holding that the plaintiff does not have to "allege state-of-mind for his BIPA claims to proceed"); Sosa v. Onfido, Inc., 600 F. Supp. 3d 859, 875 (N.D. Ill. 2022) (holding that the plaintiff "is not required to plead facts showing negligence, recklessness, or intentional conduct to state a BIPA claim").

[251] *See, e.g.*, Rogers v. BNSF Ry., 680 F. Supp. 3d 1027, 1040 (N.D. Ill. 2023) ("It [ ] appears that the General Assembly chose to make damages discretionary rather than mandatory under [BIPA]."); Svoboda v. Amazon.com, Inc., 2024 WL 1363718, at *12 (N.D. Ill. Mar. 30, 2024) ("Amazon argues that it has unique defenses to every member of the putative class because damages are 'discretionary rather than mandatory' under BIPA, citing *Cothron*."); Howe v. Speedway LLC, 2024 WL 4346631, at *14 (N.D. Ill. Sept. 29,

evidence on liability and determine a proper damages award based on culpability and the need for deterrence. Again, the combination of these two factors suggests that, accepting the premise that courts will take the time to accurately determine culpability, parties will face liability to the extent appropriate. For example, the collecting entity may be subject to BIPA's full statutory damages, whereas a party that unintentionally stores biometrics down the line would be exposed to little or no damages.

While this two-step framework may impose broader liability for defendants than a narrower articulation would, companies and courts have ways to ensure that the purpose of BIPA—to protect biometric data before it is too late to provide redress—is fulfilled without deterring use of biometrics entirely or imposing endless liability. Of course, this tasks courts with determining what the underlying technology is capable of, how far liability extends, and what damages awards are proper to deter but not annihilate companies.

In sum, this two-step approach—requiring the ability to uniquely identify but considering this requirement met if any entity can to do so—is workable in practice. And while it may create broader liability in certain situations involving nonusers and third parties than a narrower conception would, there are barriers that will keep this conception from overwhelming courts or imposing endless liability on companies.

* * *

A middle-ground approach that protects biometric identifiers that *any* entity could use to uniquely identify an individual comports with BIPA's text and purpose. Deviating from it in either direction does not. Deeming technologies that merely identify age and gender to qualify as biometric identifiers would push the statute toward an even more plaintiff-friendly interpretation. The more likely alternative, however, given how lower courts have reacted post-*Zellmer*, is that courts continue to find that the collecting entity must itself be able to uniquely identify. This risks greatly weakening BIPA's utility for plaintiffs, rendering it near powerless in cases involving nonusers and third parties. But again, this misguided conception is not so engrained that courts cannot still viably chart this middle path.

2024) ("[T]he Illinois Supreme Court has interpreted BIPA's damages provisions to recognize . . . trial courts have discretion to fashion appropriate awards under the statute.").

CONCLUSION

The full consequences of recent pro-defendant shifts in BIPA litigation are as yet unclear, but some early impacts have already come into view. Courts have issued conflicting opinions over whether the BIPA amendment applies retroactively,[252] with the question anticipated to make its way through the court system.[253] Defendants have argued that virtual try-ons, skincare and makeup assessments, and the like are exempt from BIPA's requirements, despite the tenuous link between these technologies and BIPA's healthcare exemption.[254] Most concerningly, lower courts have cited *Zellmer* to suggest that the collecting entity must itself be able to identify an individual to fall within BIPA's scope.[255] All the while, public concern over biometrics,[256] as well as risks at the intersection of AI and biometrics,[257] appear to be on the rise.

Further decisions, whether favorable toward plaintiffs or defendants, will not just impact parties embroiled in BIPA litigation. In July 2024, a district court issued the first decision interpreting New York City's Biometric Identifier Information law, parsing that statute's text in a suit against Amazon and Starbucks.[258] In February 2025, the first lawsuit was filed under Washington's MHMDA, where the plaintiff alleges that Amazon collected her biometric data and geolocation information.[259] Both of these statutes bear more similarity to BIPA than any other biometric privacy laws. As jurisdictions continue to model

---

[252] *Compare, e.g.*, Gregg v. Cent. Transp. LLC, 2024 WL 4766297, at *2–3 (N.D. Ill. Nov. 13, 2024), *vacated*, 2025 WL 907540 (N.D. Ill. Mar. 21, 2025) (holding that the BIPA amendment applies retroactively because it merely clarifies existing law), *with* Schwartz v. Supply Network, Inc., 2024 WL 4871408, at *4–5 (N.D. Ill. Nov. 22, 2024) (holding that the BIPA amendment does not apply retroactively because it is substantive rather than procedural).

[253] *See* Kevin Bessler, *Illinois' Controversial Biometric Privacy Law Continues to Be Challenged in Court*, THE CTR. SQUARE (Dec. 18, 2024), https://perma.cc/4CPT-99QK.

[254] *See* Bilyk, *supra* note 154.

[255] *See supra* Part III.A.

[256] *See* Jim Nash, *Survey Sees US Consumer Confidence Fall for Biometrics*, BIOMETRIC UPDATE (Feb. 21, 2024), https://perma.cc/7A7T-SB29 (explaining that survey data indicates "comfort with sharing fingerprint, face and voice scans . . . fell sharply from 2022 to 2024").

[257] *See* Cassandre Coyer, *Privacy, Security Clash as Companies Seek Proof Users Are Human*, BLOOMBERG L. (Dec. 20, 2024), https://news.bloomberglaw.com/privacy-and-data-security/privacy-security-clash-as-companies-seek-proof-users-are-human.

[258] Mallouk v. Amazon.com, Inc., 2024 WL 3511015, at *4–5 (W.D. Wash. July 23, 2024).

[259] *See* Complaint at 22, Maxwell v. Amazon.com, Inc, No. 2:25-CV-00261 (W.D. Wash. Feb. 10, 2025).

statutes like these after BIPA, and as these cases increasingly impact entities outside of Illinois, having BIPA as a model is more important now than ever.

In 2024, a federal district court judge in Illinois remarked that he was ruling on yet "another drop in the tidal wave of cases under the Illinois Biometric Information Privacy Act that has crashed down and flooded courthouses."[260] BIPA is undoubtedly now famous—or infamous—in the privacy world. Parties continue to raise novel, unlitigated arguments under the statute. And the ramifications of biometric technology are not fully known.[261] So while recent developments are meaningful, this is unlikely the last time such shifts will occur in the biometric privacy landscape.

[260] Rowe v. Papa John's Int'l, Inc., 2024 WL 3925411, at *1 (N.D. Ill. Aug. 23, 2024).
[261] *See* 740 ILL. COMP. STAT. 14/5(f).