BIPA 007- BIOMETRIC PRIVACY LAWS OR **LICENSE TO KILL BUSINESSES**

BY GILLIAN LINDSAY

& IAN FISHER

& STEPHANIE ADDISON

Gillian Lindsay and Ian Fisher are Partners, and Stephanie Addison is an Associate in Taft Stettinius & Hollister LLP's Chicago Office. Their professional biographies are available here: Gillian G. Lindsay | People | Taft Stettinius & Hollister LLP (taftlaw.com); Ian H. Fisher | People | Taft Stettinius & Hollister LLP (taftlaw.com); Stephanie P. Addison | People | Taft Stettinius & Hollister LLP (taftlaw.com).

Visit www.competitionpolicyinternational.com for access to these articles and more!

BIPA 007- BIOMETRIC PRIVACY LAWS OR LICENSE TO KILL BUSINESSES

By Gillian Lindsay, Ian Fisher & Stephanie Addison

The uses for biometric information are fascinating, but the consequences are frightening. Illinois' Biometric Information Privacy Act is the most robust biometric privacy legislation in the country. It is a powerful tool for plaintiffs' class-action counsel, presenting astronomical risk and driving huge settlements. Businesses use employee thumbprint time clocks for accurate timekeeping, but without careful compliance, each scan could result in $1,000 (unintentional) or $5,000 (intentional) in statutory damages. These amounts quickly accumulate; indeed, a fast-food restaurant faces $17 billion in potential damages in a recent case. When it comes to biometric information, an ounce of prevention is worth a pound of cure.

Retina eye scans are no longer the exclusive purview of international agents. Biometric information provides convenient ways to accurately confirm a person's identity. Businesses from neighborhood nail salons to Big Tech collect and use biometric data for a variety of reasons. Biometric data, including fingerprints, hand scans, and face geometry, allows: office buildings to swap proxy cards for hand scans; employees to use thumbprints instead of punch cards; travelers to bypass the security line; truckers to stay awake and alert behind the wheel; and the forgetful to replace passwords with face recognition. Even Taylor Swift has used facial recognition to identify known stalkers.

The technological advances are thrilling, but the legal consequences can be terrifying. Illinois' Biometric Information Privacy Act ("BIPA") is the strongest biometric privacy law in the United States. BIPA provides a private right of action and BIPA claims lend themselves to class action treatment. A wave of BIPA lawsuits has hit court dockets across the country. As courts have recently been interpreting BIPA, they have provided clarity and guidance on previously unanswered questions, with ruinous results for businesses that find themselves on the wrong end of an employee or consumer class action. The settlements can be huge — Facebook settled a BIPA class action for $650 million — and the one defendant to go to trial was hit with a $228 million verdict.

The Illinois legislators have proposed a number of amendments to BIPA that could dampen some of the most catastrophic damages, but only one potential amendment has made it to the legislature's floor. That amendment received bipartisan support in the Illinois Senate and is pending in the House. If the House passes the amendment, the Governor will presumably sign it, providing some relief to BIPA defendants. Nevertheless, companies that interact with Illinois residents must adopt a compliant biometric data policy and obtain meaningful releases from all participants whose biometric data may be collected, used, transferred, or destroyed before implementing biometric technologies.

01

THE BIOMETRIC INFORMATION PRIVACY ACT

In response to the increasing collection and use of biometric data, some states enacted laws to regulate the collection, storage, use, disclosure, transfer, sale, and destruction of biometric information. Sixteen years ago, the Illinois legislature concluded that "the full ramifications of biometric technology are not fully known."[2] Biometric identifiers and biometric information are biologically unique to the individual, and unlike a password or bank account PIN, when biometric information is compromised, it cannot be changed.[3] "Once compromised, the individual has no recourse, is at heighted risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[4]

In 2008, the Illinois legislature unanimously passed BIPA to prevent the misuse of biometric information. BIPA: (1) establishes standards for private entities that collect, possess, use, disclose, or destroy biometric identifiers or biometric information; and, (2) provides a private right of action to any individual who is aggrieved by a violation.

Section 15(b) of BIPA, provides:

No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

1. informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

2. informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

3. receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[5]

2 740 ILCS 14/5(f).

3 740 ILCS 14/5(c).

4 740 ILCS 14/5(c).

5 740 ILCS 14/15(b).

Section 15(a) mandates that these entities create a publicly available written policy establishing a retention schedule and destruction guidelines for when the initial purpose for collecting the information has been satisfied or within three years of the individual's last interaction with the private entity.[6] Section 15(c) prohibits the sale, lease, trade, or profit from biometric identifiers and biometric information. And, Section 15(d) prohibits a private entity from disclosing or otherwise disseminating biometric information without first obtaining an individual's consent, unless the disclosure or dissemination was in furtherance of an authorized financial transaction, authorized by law, or pursuant to a valid warrant or subpoena.[7]

Other states have similar statutes, but they have generally limited the right of enforcement to governmental agencies, such as state attorneys general. BIPA is unique in that it is the most robust and the only one to expressly create a private right of action.[8] Indeed, BIPA provides a powerful private right of action. If a company fails to follow the requirements outlined in BIPA, then any "aggrieved" person can seek the greater of $1,000 or actual damages for each negligent violation, and the greater of $5,000 or actual damages for each violation that was recklessly or intentionally committed.[9]

02

WHAT ARE BIOMETRIC IDENTIFIERS AND BIOMETRIC INFORMATION

BIPA regulates "biometric identifiers" and "biometric information."[10] "Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[11] The definition of biometric identifier also defines what it is not. For example, biometric identifier does not include writing samples, photographs, tattoo descriptions, or physical descriptions like hair color, weight, and eye color.[12]

"'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers."[13]

In *Sosa v. Onfido, Inc*., the Northern District of Illinois ruled that liability can spring from the collection of biometric identifiers, even when no biometric information is captured. Onfido, a Delaware corporation primarily doing business in England, verified consumers' identities using facial recognition created from photographs. Consumers uploaded copies of their identification and photographs of their faces. Onfido's software scanned the images on each person's identification and photograph to create a unique numerical representation of the consumer's face geometry, i.e. a faceprint. When used, the software compared the faceprint to identify the consumer.

When Sosa filed a putative class action claiming BIPA violations, Onfido filed a motion to dismiss arguing it did not violate BIPA, because its faceprints were derived from photographs. Onfido relied on the text of the statute asserting that photographs are not biometric identifiers or biometric information. BIPA expressly excludes photographs from biometric identifier and biometric information "does not include information derived from items or procedures excluded under the definition of biometric identifier."[14]

The court, however, determined the information Onfido captured plausibly constituted a scan of face geometry.[15]

6 740 ILCS 14/15(a).

7 740 ILCS 14/15(d).

8 Washington recently enacted the "My Health, My Data" Act, which covers "biometric data" in addition to more traditional healthcare information. Although it does not expressly create a private right of action, it likely can be enforced by private parties under the state's consumer fraud statute. Unlike BIPA, however, a private plaintiff presumably must show actual damages.

9 740 ILCS 14/20.

10 740 ILCS 14/10.

11 *Id*.

12 *Id*.

13 *Id*.

14 740 ILCS 14/10.

15 *Illinois, Sosa v. Onfido, Inc.*, No. 20-cv-4247, 2022 WL 1211506 (N.D. Ill. Apr. 25, 2022).

Relying on the text of the statute, the court ruled that while information derived from photographs is excluded from the definition of biometric information, the definition of biometric identifier does not contain a similar exclusion. Moreover, the court concluded nothing in BIPA's text suggests that a face scan must be obtained in person.[16] Accordingly, a biometric identifier may be created, and trigger liability, even when derived from a photograph — by definition not a biometric identifier.

03
NO HARM; BIG FOUL

In 2019, the Illinois Supreme Court decided the landmark case *Rosenbach v. Six Flags*, and concluded a person may be "aggrieved" by a BIPA violation regardless of whether their biometric information was misused or compromised. Rosenbach alleged that a Six Flags amusement park utilized fingerprint scanners to "make[] entry into the park faster and more seamless," without obtaining consent from visitors to collect and store their biometric information.[17] Although plaintiffs did not allege actual injury from the collection, the court concluded that a claimant does not need to plead actual harm or injury resulting from an alleged BIPA violation to seek injunctive relief and liquidated statutory damages. "Through [BIPA, the Illinois] General Assembly . . . codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information."[18] "[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[19]

04
CATASTROPHIC CLASS ACTIONS

BIPA is a dream for class action plaintiffs: no injury is required, the statutory damages produce stunning results and prevent a defendant from avoiding class action treatment by arguing each unnamed class member must establish her injury, and crafty pleading can avoid federal jurisdiction.[20] Any technical violation of BIPA creates standing to sue. With no requirement that the plaintiff prove any actual injury or harm to recover statutory damages, she need only show a violation occurred, she can recover the greater of $1,000 in statutory damages (or actual damages, which plaintiffs do not do) for each unintentional violation. If a plaintiff can show that a violation was reckless or intentional, the statutory damages increase to the $5,000 per violation.

In February 2023, the Illinois Supreme Court settled a BIPA debate — what statute of limitations applies to BIPA claims. In *Tims v. Black Horse Carriers, Inc.*, the Court found that "the five-year limitations period contained in section 13-205 of the Code controls claims under the Act."[21] Thus, a class can include all people who have had their biometric information collected for the five years prior to the suit being filed. This also creates some opportunities for a defendant to look to older "occurrence based" insurance policies for potential coverage. Insurers, however, have begun including "BIPA-exclusions" in their newer policies.

In July, the Illinois Supreme Court answered another question and held that each violation carries damages. In *Cothran v. White Castle System, Inc.*, a much anticipated 2023 decision, the Illinois Supreme Court held that "the plain language of section 15(b) and 15(d) shows that a claim accrues under the Act with every scan or transmission of biometric identifiers or biometric information without prior informed consent."[22] Although this ruling was surprising to some, the Court explained that it has "repeatedly recognized the potential for significant damages awards under the Act . . the legislature intended to subject private entities who fail

16 *Id*.

17 *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 4.

18 Rosenbach, 2019 IL 123186, ¶ 33 citing *See Patel v. Facebook Inc.*, 290 F.Supp.3d 948, 953 (N.D. Cal. 2018).

19 *Rosenbach*, 2019 IL 123186, ¶ 40.

20 *Rosenbach,* 2019 IL 123186, ¶ 40; 740 ILCS 14/20; *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004, ¶ 45, 216 N.E.3d 918, 929, *as modified on denial of reh'g* (July 18, 2023); *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1248 (7th Cir. 2021).

21 *Tims v. Black Horse Carriers, Inc.,* 2023 IL 127801, ¶ 42.

22 *Cothron*, 2023 IL 128004, ¶ 45, 216 N.E.3d 918, 929.

to follow the statute's requirements to substantial potential liability."[23]

In 2004, White Castle introduced technology that allowed its employees to access paystubs and work computers by scanning their fingers. White Castle would then transmit the scans to a third-party vendor who verified each scan and authorized employee access. In the suit, the plaintiff alleged that although the scanning system was implemented in 2004, White Castle did not obtain her written informed consent as required by BIPA once the statute took effect in 2008. White Castle waited until 2018 to seek her consent. Although White Castle argued that Cothron's claims were untimely since the first violation had occurred in 2008, more than 10 years before she filed her complaint, Cothron argued — and the court agreed — that a new claim accrued each time she scanned her fingerprints and White Castle sent her biometric data to its third-party authenticator. The Illinois Supreme Court ultimately held that BIPA claims accrue each time biometric data is collected or transmitted, not just the first instance.

In the context of an employee class-action for time tracking devices, the damages add up quickly. Each employee may scan in to start the day, in and out for lunch and other breaks, and out for the day. Accordingly, each employee may have six scans per day. In a five-day work week, that amounts to 30 scans a week, or $30,000 for each employee, for unintentional violations, $150,000 for intentional violations in a single week. These damages can accrue for five years. In White Castle's case, potentially $17 billion dollars in damages.[24]

05

EMPLOYERS CANNOT ABDICATE BIPA RESPONSIBILITY TO THIRD-PARTY VENDORS

Employers once hoped they could dodge BIPA by pointing the finger at a third-party vendor. Courts have not let employers off the hook. In *Rogers v. BNSF Railway*, the lead plaintiff sued BNSF on behalf of a class of about 45,000 truck drivers. The lawsuit alleged that BNSF unlawfully collected fingerprint scans without consent from thousands of drivers using automated gate systems at the company's four facilities in Illinois. BNSF also failed to provide drivers with notice about what might happen with their scanned prints. BNSF attempted to escape liability by arguing it outsourced the collection of the biometric information to a third-party vendor, Remprex LLC, which it contracted to install and operate the equipment that captured the fingerprint scans. The court determined that because Remprex was an agent of BNSF, BNSF could be held liable for Remprex's actions. In the first-ever jury verdict in a BIPA class-action lawsuit, the jury found that BNSF recklessly or intentionally violated BIPA 45,600 times — an amount equal to the defense expert's estimated number of truck drivers in the class whose fingers were scanned from April 4, 2014, through January 25, 2020.

06

THIRD-PARTY VENDORS MAY BE ON THE HOOK

Courts have also struck down timekeeping vendors' attempts to point the finger at their employer customers. In *Ronquillo v. Doctor's Associates, LLC*, the Court considered the liability of third-party vendors. Subway franchisees paid a monthly fee to lease point-of-sale ("POS") equipment from third-party vendors, while the vendors retained ownership of the equipment. This equipment was used with third-party software to allow employees to use their fingerprints to unlock registers and clock in for shifts and breaks. The court determined that the third-party vendors "took an active step to collect, capture, or otherwise obtain [plaintiff's] biometric information."[25] The third-party vendors argued Section 15(b) did not apply to them, and claimed "that extending § 15(b)'s reach to such parties does not further BIPA's purpose and instead creates absurd results."[26] The court disagreed finding nothing in the statute limits BIPA's reach to employers and explaining that as a contractual precondition, vendors could have required Subway "to agree to obtain its employ-

23 *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004, ¶ 41, 216 N.E.3d 918, 928, *as modified on denial of reh'g* (July 18, 2023) citing *Rosenbach*, 2019 IL 123186, ¶¶ 36-37, 432 Ill.Dec. 654, 129 N.E.3d 1197; *McDonald*, 2022 IL 126511, ¶ 48, 456 Ill.Dec. 845, 193 N.E.3d 1253.

24 *Id*. at ¶ 40,

25 *Ronquillo v. Doctor's Assocs., LLC*, 597 F. Supp. 3d 1227, 1231 (N.D. Ill. 2022)

26 *Ronquillo*, 597 F. Supp. 3d at 1232.

ee's written consent to [the third-party vendors] obtaining their data."[27]

Many third-party timekeeping vendors have applied the court's guidance. Companies that use third-party vendors for timekeeping purposes should carefully review the contract to understand and implement and contractual preconditions to obtain employee consent and any potential indemnification provisions (i.e. agreements to undertake and compensate vendors for damages, costs, and expenses) for BIPA and other liability.

07
BIPA'S NATIONWIDE REACH

Although enacted in 2008, BIPA largely lay dormant until 2015, when plaintiffs filed a series of class-action lawsuits against Facebook alleging unlawful collection and use of consumers' biometric data to sell to third parties. These class actions were consolidated in the U.S. District Court for the District of Northern California in the case *In re Facebook Biometric Info. Privacy Litig*.[28] The Facebook lawsuits stemmed from its implementation of a new feature called "Tag Suggestions." If enabled by the user, the feature allowed Facebook to utilize facial recognition software to collect, analyze, and compare the facial features in user-uploaded photographs to create "face templates."[29] The face templates were then stored in one of Facebook's nine data centers, none of which are located in Illinois.[30]

In the lawsuit, the Illinois plaintiffs claimed that Facebook did not obtain prior written consent to collect biometric data or develop a retention schedule of the biometric information as required under BIPA. Facebook's argument that BIPA did not apply because Facebook's collection of biometric data and creation of face templates occurred on servers outside of Illinois, was ineffective.[31] The Ninth Circuit explained that "[w]hen a case is 'made up of components that occur in more than one state,' plaintiffs may maintain an action only if the events that are necessary elements of the transaction occurred 'primarily and substantially within' Illinois."[32]

In February 2021, Facebook settled the suit, agreeing to pay $650 million to the aggrieved users, one of the largest consumer privacy settlements in U.S. history. Facebook subsequently shut down the Tag Suggestions feature. Notably, the judge in the case deemed Facebook's prior offer of $550 million inadequate. Under the $650 million settlement, the roughly 1.6 million class members received at least $345 each under the final settlement ruling. A significant discount from BIPA's statutory damages.

BIPA's broad reach has been confirmed by other courts. In *Ronquillo v. Doctor's Associates, LLC*, the court also held that the "extraterritoriality doctrine" does not bar BIPA claims against non-Illinois residents. Non-resident defendants are subject to BIPA if the underlying facts "took place 'primarily and substantially in Illinois."[33]

Lawsuits have hit tech giants like Microsoft, Google, and Amazon, and small business and local clubs. To date, more than two thousand class action lawsuits have been filed under BIPA, making it the most litigated biometric privacy law in the United States.

08
EXCLUSIVITY OF THE ILLINOIS WORKERS' COMPENSATION ACT IS NOT A BIPA DEFENSES

The courts have ruled that BIPA and the Illinois Workers' Compensation Act can coexist. In *Marquita McDonald v. Symphony Bronzeville Park, LLC*, IL 126511, 2022, the plaintiff filed a putative class action complaint against her former employer, alleging that it collected, used, and stored

27 *Ronquillo*, 597 F. Supp. 3d at 1233.

28 *In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

29 *Id*. At 1158-1159.

30 *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1275 (9th Cir. 2019).

31 *Id*.

32 *Id.*

33 *Ronquillo*, 597 F. Supp. 3d at 1234.

employee fingerprints in an electronic system for timekeeping purposes, but never asked for her consent nor did it inform her of the purpose or length of time for which her information was to be stored in violation of BIPA. The defendants argued that the exclusivity provisions of the Illinois Workers' Compensation Act (IWCA) barred plaintiff's BIPA claims, because the IWCA is the exclusive remedy provision for injuries that arise in the scope of employment.

On February 3, 2022, the Illinois Supreme Court found that "personal and societal injuries" resulting from a violation of BIPA are distinguishable from the "nature and scope" of the physical and psychological workplace injuries compensable under the IWCA. In ruling on this defense, the Illinois Supreme Court seemingly expanded employer liability under BIPA.

09

DISCRETIONARY DAMAGES AND DUE PROCESS CHALLENGES

With such an explosion in BIPA cases, plaintiffs have explored new ways to calculate BIPA damages and defendants have tried to call such damages into question. After the jury delivered its verdict in *Rogers v. BNSF Railway Co.* (*infra*), the judge imposed a $228 million penalty on BNSF. BNSF requested that a jury set the damages; the judge agreed that BIPA damages are a question for the jury — implying that there is more discretion to the awards than simple arithmetic (the number of violations multiplied by the statutory damages amount). The judge scheduled a damages-only trial, but before that trial took place, the parties settled for $75 million. Notably, the judge's finding that damages are discretionary is from a federal court and, thus, not binding on the Illinois state courts.

The Illinois Supreme Court appeared to confirm the discretionary nature of BIPA damages, when the majority in *Cothran v. White Castle* (*infra*). Even though the Court stated that BIPA damages were not intended by the legislature to "authorize a damage award that would result in the financial destruction of a business[,]"[34] the opinion may be read to limit the finding that damages are discretionary — and not mandatory — to just class actions under the BIPA. In other words, the Court left open that the liquidated damages of $1,000 for negligent and $5,000 for reckless or intentional violations are mandatory in cases brought by individuals, not in class actions. Specifically, the Court wrote "a trial court presiding over a class action — a creature of equity — would certainly possess the discretion to fashion a damage award that (1) fairly compensated claiming class members and (2) included an amount designed to deter future violations, without destroying defendant's business."[35]

In the dissenting opinion, three justices criticized the majority for interpreting BIPA in a way that would lead to a "consequence that the legislature could not have intended."[36] Additionally, Justice Overstreet, in a separate dissent, criticized the majority's interpretation of BIPA because not only does the majority's opinion pose practical concerns for businesses but also presents constitutional due process concerns for Illinois courts.[37] "The legislature never intended the Act to be a mechanism to impose extraordinary damages on businesses or a vehicle for litigants to leverage the exposure of exorbitant statutory damages to extract massive settlements. Yet, [the Illinois Supreme Court] construed the Act to allow these unintended consequences, and as a result, this construction raises serious issues as to the Act's validity."[38]

Defendants have recently been using Judge Overstreet's guidance to challenge the constitutionality of BIPA. They have filed motions to dismiss arguing due process requirements limit the legislature's authority to establish statutory damages that can be so ruinous in the aggregate. "When a statute authorizes an award that is so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable, it does not further a legitimate government purpose, runs afoul of the due process clause, and

34 *Cothron*, 2023 IL 128004, ¶ 42.

35 *Id*.

36 *Id*. at ¶ 48.

37 *Id*. at ¶70.

38 *Id*.

is unconstitutional."[39] Time will tell whether this argument gains acceptance in the courts.

10
PROPOSED AMENDMENTS TO ALLEVIATE THE BIPA BURDEN

Meanwhile, in an apparent effort to shield Illinois employers from catastrophic damages in BIPA lawsuits without rolling back the state's strict privacy protections, the Illinois legislature introduced legislation to change the liability guidelines under BIPA. A new bill, SB 2979, would limit the number of claims accrued should an employee bring a lawsuit against a company for a BIPA violation. Under the bill, BIPA violations would be counted on a per-person basis rather than per violation. The bill would also allow permission to be given electronically, rather than in writing.

If passed, SB 2979 will limit financial exposure for companies that have not violated BIPA. Given the widespread use of biometric timekeeping, many business owners are skeptical of its potential impact.

First, the amendment is silent on whether it would be retroactive, such that it would provide relief to defendants who have already been sued and are defending themselves. Plaintiffs will surely argue such legislation is only prospective. Courts seem reticent to apply new laws retroactively. Therefore, the amendment might not provide relief to businesses currently facing large potential judgments.

However, defendants do have valid arguments for retroactive application of the BIPA amendment (if the General Assembly passes it). Although the amendment does not expressly address its temporal reach, according to the Illinois' general savings clause, "those amendments that are procedural in nature may be applied retroactively, while those that are substantive may not."[40] This is not a certain outcome because although courts have considered amendments that affect remedies to be procedural, in some circumstances,[41] such amendments have been considered substantive changes to the law with no retroactive application.[42] Arguably, the amendment would not have retroactive impact to bar retroactivity. It could be argued that the amendment (1) would not impair rights a party possessed when he acted — "Illinois courts have long recognized there can be no vested right in any particular remedy;" (2) the amendment does not increase a party's liability for past conduct — the amendment limits liability; and, (3) the amendment does not impose a new duty for completed transactions — the amendment does not affect BIPA protections and requirements.[43] Moreover, as noted by the Illinois Supreme Court in *Cothran*, damages in BIPA class actions will quickly reach numbers that would result in the financial destruction of businesses. Businesses that rely on hourly workers — and use biometric timekeeping systems to keep accurate records to pay employees appropriately for their work — may be forced out of business resulting in lost jobs and a drain on the economy. Accordingly, public policy likely favors retroactive application.

Unlike most of its predecessors, many observers believe the bill has a reasonable chance of passage, partially because of the current state of the law and partially because the Senate President *Pro Tem*, Bill Cunningham, has sponsored it. On March 13, 2024, SB 2979 passed out of committee. The next day, the bill was read for the second time by the Illinois State Senate and placed on the calendar for its requisite third reading on March 20, 2024. On April 11, 2024, a bipartisan majority in the Senate passed the bill, 46-13. Time will tell what will happen in the House. The plain-

39 *Id*. at ¶75 *Citing see St. Louis, Iron Mountain & Southern Ry. Co.*, 251 U.S. at 67, 40 S.Ct. 71*; see also People v. Bradley*, 79 Ill. 2d 410, 417, 38 Ill.Dec. 575, 403 N.E.2d 1029 (1980) (pursuant to due process clause of the Illinois Constitution, the legislature properly exercises its police power when its statute is "'reasonably designed to remedy the evils which the legislature has determined to be a threat to the public health, safety[,] and general welfare'") (quoting *Heimgaertner v. Benjamin Electric Manufacturing Co.*, 6 Ill. 2d 152, 159, 128 N.E.2d 691 (1955)).

40 *Thomas v. Weatherguard Const. Co.*, 2015 IL App (1st) 142785, ¶ 65.

41 See, e.g. *Levy v. McKiel*, 185 Ill.App.3d 240, 133 Ill. Dec. 405, 541 N.E.2d 242 (1989) (applying retroactively a statute regulating hospitals' potential liability to agents and employees); *Dardeen v. Heartland Manor, Inc.*, 186 Ill. 2d 291, 299 (1999) (holding that the a plaintiff "has no vested right in any particular remedy or procedure" and thus a "change in law affecting the remedy or procedure will be employed without regard to whether the cause of action accrued before or after the change in the law or when the suit was instituted unless there is a savings clause as to existing legislation"); see also, e.g. *White v. Sunrise Healthcare Corp.,* 295 Ill. App. 3d 296, 300-302 (1998) (collecting cases to explain that changes to damages and other remedies are ordinarily "procedural" and thus a "change in the law that affects merely … remedies will ordinarily be applied to existing rights of action").

42 *People ex rel. Madigan v. J.T. Einoder, Inc.*, 2015 IL 117193, ¶ 35–37.

43 *Thomas,* 2015 IL App (1st) ¶ 67; *White*, 295 Ill. App. 3d at 300.

tiffs trial bar, however, will likely oppose the bill, and any other meaningful BIPA reform. Accordingly, no one knows for sure whether SB 2979 will result in any meaningful reform of BIPA.

11 TAKE AWAY

While other states have adopted biometric privacy regulation, BIPA continues to stand as the most protective biometric privacy law in the country, offering individuals a private right of action, even in cases where the consumer cannot show that he or she was actually harmed. Given BIPA's expansive reach and the regulation of biometric privacy across the county, any business using or considering implementing biometric technology should take careful action to ensure legal compliance.

While other states have adopted biometric privacy regulation, BIPA continues to stand as the most protective biometric privacy law in the country

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL