Seyfarth

The Biometric Information Privacy Act In the Era of COVID-19

A Legal and Legislative Update

Thomas E. Ahlering
Ada W. Dolph
Randel Johnson
Clark Kaericher, Illinois Chamber of Commerce

Seyfarth Shaw LLP

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this presentation should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Topics

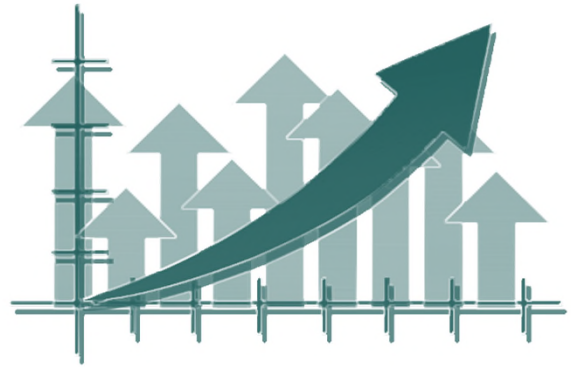
Overview of the Illinois Biometric Information Privacy Act (BIPA)

Origins of BIPA

- The legislative history surrounding the bill suggests that the statute was implemented to protect consumers.
- Originally enacted in 2008, motivated by the bankruptcy of Pay by Touch (largest fingerprint scan system in Illinois)
- Regulates the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and biometric information.
- Because it has only recently generated litigation, courts are still interpreting BIPA.

The Rise in BIPA Litigation

- Uptick began in 2017 – more than 50 BIPA cases filed in 2017 alone
- All Industries
  - Hospitality/Service
  - Manufacturing
  - HealthCare
  - Retail
- BIPA provides for possibly significant penalties (and attorneys' fees)
- Also suing the manufacturer and/or provider of the Biometric System at issue



Who Is Covered

- **"Private entity"** means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.
- Section 25 of the statute exempts:
  - Certain financial institutions
  - A contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government

BIPA Does Not Override Certain Statutes

- BIPA does not impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, or agency.
- BIPA expressly cannot be interpreted to override any of these statutes or regulations under these statutes:
  - Illinois X-Ray Retention Act
  - Illinois Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA).

“Biometric Identifier” Defined

- **"Biometric identifier"** appears to squarely include:
  – a retina or iris scan,
  – fingerprint,
  – voiceprint, or
  – scan of hand or face geometry.

“Biometric Identifier” Defined

- **"Biometric identifier"** does **not** include:
- writing samples
- written signatures
- photographs (note: face scans created from photographs have been held to be biometric information)
- human biological samples used for valid scientific testing or screening
- demographic data
- tattoo descriptions
- physical descriptions such as height, weight, hair color, or eye color
- donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency
- biological materials regulated under the Genetic Information Privacy Act
- 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
- X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening

“Biometric Information” Defined

- **BUT, there is a catch-all in the statute:**
- **"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.

Section 15(a) Written Policy

- A private entity in possession of biometric identifiers or biometric information must:
  - Develop a **written policy** that establishes a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first; and
  - Make the policy available to the public; and
  - Comply with the retention schedule and destruction guidelines absent a valid warrant or subpoena.

Section 15(b) Requirements Before Collection

- 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.

Section 15(b) Requirements Before Collection

- **Written Release** means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

Section 15(c) No Profit From Biometric Information

- No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

Section 15(d) Requirements Before Dissemination

- No private entity in possession of a biometric identifier or biometric information may disseminate a person's or a customer's biometric identifier or biometric information unless:
  - The subject or their legally authorized representative consents to the disclosure;
  - The disclosure completes a financial transaction requested by the subject;
  - The disclosure is required by State or federal law or municipal ordinance; or
  - The disclosure is required pursuant to a valid warrant or subpoena.

Section 15(e) Retention Standard of Care

- Private entities must:
  - store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
  - store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

Section 20 Enforcement

- BIPA provides a private right of action allowing plaintiffs to recover liquidated damages and attorneys' fees.
- BIPA Statutory Penalties
  - Authorizes $1,000 or actual damages (whichever is greater) for negligent violations.
  - Authorizes $5,000 or actual damages (whichever is greater) for intentional or reckless violations.
  - Authorizes injunctive relief and reasonable attorneys' fees (including for expert witnesses) and costs to a "prevailing party."

BIPA In the Time of COVID-19

Relevant COVID-19 Agency Guidance

- Centers for Disease Control and Prevention has guidance that employers “measure the employee's temperature and assess symptoms prior to them starting work.”
- U.S. Equal Employment Opportunity Commission has return-to-work guidance recognizing that employers “may include continuing to take temperatures . . . of all those entering the workplace.”
- Similar state and local guidance requiring health assessments like these.

Types of Technology At Issue

- **No Contact Temperature Taking Devices**, like a no-contract infrared scanner. Involves placing the scanner a few inches from an individual's forehead and pushing a button.
- **Facial Recognition Combined with Thermal Scanning**. Device uses facial recognition technology to identify the individual and conducts a thermal scan to take her temperature.
- **Wearables** such as watches, rings and stick-on sensors. Primarily being used to collect temperature but may also incidentally collect information on heart rate, sleep, steps, calories.

Whether BIPA Applies Depends on What is Being Collected

- As discussed previously, biometric identifier has a specific definition under the statute.
- The closer the technology at issue is to any of the categories that are covered, the more likely you will be sued under BIPA.
- Therefore, if the technology conducts a scan of any of these areas directly or incidentally, we advise erring on the side of compliance:
  - a retina or iris scan,
  - fingerprint,
  - voiceprint, or
  - scan of hand or face geometry.

Whether BIPA Applies Depends on What is Being Collected

- Again, even if the technology doesn't fall squarely under any of the main categories, be wary of the "catch-all."
- The key for the catch-all, is that it covers biometric information "based on an individual's biometric identifier used to identify an individual."
- Only a few cases interpreting this provision. A few decisions have interpreted "biometric information" broadly to encompass portions of biometric identifiers (i.e., data points).

Due Diligence Before Implementation

- **Understand the technology**
  - What is being collected?
  - If a vendor represents that one part of the technology is being “shut-off,” confirm independently
  - Note that the perception of a face scan being collected is enough to lead to a lawsuit
- **Research the vendor**
  - Data privacy protections in place?
  - Appropriate contract provisions in place for data breaches?
  - What data, if any, is being shared with the vendor?
  - Obtain independent legal review of any representations that BIPA would not apply
- **Adequate protections in contracts** for clear coverage in the case of a data breach, unauthorized dissemination, clear responsibility for data.
- **Insurance coverage**
  - What, if any, insurance coverage do you have in place that would cover a data breach involving biometric information?

Err On the Side of Compliance With BIPA

- Statute remains ambiguous and a number of provisions have not yet been interpreted.
- We expect an increase in lawsuits in this area because of the allure of automatic statutory penalties and no requirement to show actual damage to plaintiffs.
- Other ambiguities in the statute (no applicable statute of limitations) continue to make these cases high-exposure cases.
- Cost of defense has the potential to be high including extensive expert discovery regarding the technology and how biometric information is collected, stored, retained and disseminated.
- Overall recommendation is to comply whenever possible to deter potential lawsuits.

Evolution of BIPA Litigation

The *Rosenbach v. Six Flags* Ruling

- On January 25, 2019, the Illinois Supreme Court issued its first ever ruling related to the BIPA statute – *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (Ill. Jan. 25, 2019)
- Key Holdings:
  - To proceed with their claims, a plaintiff does ***not*** need to allege some actual injury or adverse effect, beyond violation of his or her rights under BIPA.
  - Technical violations of BIPA alone sufficient to qualify as "aggrieved" to seek damages and injunctive relief under the Act.
  - BIPA gives individuals the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent.
- As expected BIPA lawsuits increased after the *Rosenbach* ruling.

State or Federal Court

Patel v. Facebook, No. 18-15982 (9th Cir. 2019)

- Lawsuit originally brought in federal court alleging Facebook's facial recognition software allowing "Tag Suggestions" violated BIPA.
- Facebook argued that the plaintiff failed to allege a concrete injury sufficient for the federal court to continue to exercise federal jurisdiction.
- Ninth Circuit reversed, finding that there was an Article III injury and that the class could be certified.
- Class included all Facebook users located in Illinois for whom Facebook created or stored a face template after June 2011, resulting in a class of millions.
- Supreme Court denied Facebook's petition for a writ of certiorari.
- Case settled for $550 million shortly after the U.S. Supreme Court declined to intervene. Estimated exposure with BIPA's statutory penalties was $34 billion.
- In connection with the parties seeking preliminary approval of the settlement, the district court has raised questions about low level of recovery by class members as compared to the available statutory penalties.

Miller v. Southwest, Johnson v. United Airlines, No. 18-3476, No. 19-1785 (7th Cir. 2019)

- Case initially brought in Cook County Circuit Court and removed by Defendants to federal court.
- Moved to dismiss on grounds that the claims were preempted by the Railway Labor Act. District court originally granted the motion to dismiss, but later reversed itself after Plaintiff argued that there was no concrete injury and ordered the case remanded to Cook County Circuit Court.
- Defense attorneys sought a special appeal under the Class Action Fairness Act – one of the only methods for reviewing a remand order – and were successful.
- Seventh Circuit panel held that there was a concrete injury alleged, upheld the removal and dismissed the BIPA claims as completely preempted by the Railway Labor Act.

Bryant v. Compass Group, Inc., No. 20-1443 (7th Cir. May 5, 2020)

- Much of the debate since these cases began being filed *en masse* in 2017 has raged around whether there was a sufficient concrete injury for the federal courts to continue to exercise jurisdiction.
- At times, put defendants in the unusual position of arguing that a complaint alleged a concrete injury while plaintiffs denied it.
- Debate largely settled recently, in *Bryant v. Compass Group*, in which, following the *Miller v. Southwest* decision, the Seventh Circuit concluded that claims brought under BIPA Section 15(b), regulating the collection, use, and retention of a person's biometric identifiers or information, state a concrete injury.
- However, the Seventh Circuit generally held that plaintiff's claim under Section 15(a), regarding developing and making publicly available a retention policy regarding collected biometric information, did not allege a concrete injury sufficient to establish federal court jurisdiction.
- Defendant in *Bryant* has sought further review of this decision. Other defendants are arguing that plaintiffs have Article III standing based on differing case-specific factual circumstances.

Defenses to BIPA Claims

Compel Arbitration

- Arbitration agreements with class waivers can provide a defendant with an avenue to limit the scope of a BIPA class action.
- The U.S. Supreme Court's decision in *Lewis v. Epic Systems* held that arbitration agreements with class action waivers are enforceable.
- Accordingly, a defendant in a BIPA class action can move to compel arbitration where the named plaintiff has signed such an agreement.
- The result is typically that the named plaintiff must pursue his or her claim individually in arbitration (instead of a class action in court) which can be effective in limiting potential exposure.

Compel Arbitration - *Miracle-Pond et al. v. Shutterfly, Inc.*, No. 19-04722 (N.D. Ill. May 15, 2020)

- In *Miracle-Pond v. Shutterfly, Inc.,* a federal court in the Northern District of Illinois granted Shutterfly's motion to compel arbitration, holding that the plaintiff previously agreed to allow unilateral modifications of the agreement without notice, and that she agreed to arbitrate by continuing to use the defendant's website.
- About three months after the lawsuit was filed, Shutterfly sent an email to all of its users nationwide notifying users that the terms of use had been updated. The email also indicated that if users did not close their accounts by a specific date, the user would be deemed to have accepted the terms (which included an arbitration agreement with a class waiver).
- The Court granted Shutterfly's motion to compel arbitration finding that the plaintiff agreed to be bound by Shutterfly's terms of use by failing to close her account and continuing to use the website.
- This ruling provides a potential new angle of attack for companies already facing a pending BIPA class action to compel a plaintiff to individually arbitrate his or her claims (even if an individual did not previously expressly agree to arbitration).

Compel Arbitration – *Acaley v. Vimeo, Inc.*, No. 1:19-cv-07164 (N. D. Ill. June 1, 2020)

- In *Acaley*, a federal court in Illinois denied the defendant's motion to compel arbitration.
- Class action alleged that Vimeo's video editing platform, Magisto, improperly compiled user's "face prints" in violation of BIPA.
- Vimeo's terms of service including a binding arbitration provision
- Court rejected the plaintiff's argument that he had not received notice of the provision or consented to it
- However, the terms and conditions contained a provision titled "Exceptions to Arbitration" that exempted claims related to or arising from "allegations of theft, piracy, invasion of privacy or unauthorized use."
- Court concluded that provision excluded BIPA claims from binding arbitration.

Preempted by a Collective Bargaining Agreement

- One of the first cases to address this issue was *Johnson v. United Airlines*, No. 17-8858 (N.D. Ill. 2017).
- District court initially found the collective bargaining agreement preempted the state law claims at issue under the management rights clause of the agreement, but later reversed herself focusing on the federal court subject matter jurisdiction.
- On appeal, Seventh Circuit reversed, holding that the state law claims were preempted by the Railway Labor Act which, in turn, provides that the CBA contains the exclusive dispute resolution procedure for disputes arising under the agreement. *Miller v. Southwest Airlines*, No. 18-3476 (June 13, 2019).

Preempted by a Collective Bargaining Agreement

- Following *Miller*, courts have found BIPA claims preempted by collective bargaining agreements under Section 301 of the Labor Management Relations Act.
- *See, e.g., Gail v. University of Chicago Medical Center, Inc.*, No. 19-CV-04229, 2020 WL 1445608 (N.D. Ill. Mar. 25, 2020) (granting motion to dismiss Plaintiff's BIPA claims as preempted by collective bargaining agreement in the context of the Labor Management Relations Act (LMRA)); *Peatry v. Bimbo Bakeries USA, Inc.,* No. 19 C 2942 (Cook County Circuit Court, Feb. 26, 2020) ("The Court finds that § 301 of the LMRA preempts Peatry's claims arising after May 8, 2018, when a collective bargaining agreement governing Peatry's employment went into effect. But Peatry may proceed on her pre-May 8, 2018 claims, which neither the NLRA or IWCA preempt and sufficiently allege BIPA violations.")

Preempted by the Illinois Workers' Compensation Act

- Employers have also argued that BIPA claims are preempted by the Illinois Workers' Compensation Act. Thus far, courts have concluded BIPA claims do not allege an emotional or physical injury covered by the IWCA.
- *See McDonald v. Symphony Bronzeville Park, LLC,* No. 2017 CH 11311 (Cook County Circuit Court, June 17, 2019) (no preemption by IWCA), *interlocutory appeal pending*; *Robertson v. Hostmark Hospitality Group*, No. 18-CH-5194 (Cook County Circuit Court, July 31, 2019) (no preemption by IWCA); *Treadwell v. Power Solutions,* Int'l, No. 18 C 8212 (N.D. Ill. Dec. 16, 2019) (no preemption by IWCA).

Anticipated Battlegrounds

Statute of Limitations

- There is no statute of limitations contained in BIPA
- Plaintiffs have argued for a five-year “catch-all” limitations period.
- Defendants have argued for a one year limitations period based on the statute of limitations applicable to a similar privacy tort found in 735 ILCS 5/13-201 titled “Defamation – Privacy.”
- 735 ILCS 5/13-202 is another statute that has been argued provides the applicable limitations period. It is titled “Personal Injury – Penalty” and provides for two years to file suit.
- Only Illinois state courts have decided this issue so far-no federal courts.
- Two courts have ruled that the five year limitations period applies. *Heard v. THC-NorthShore, Inc. d/b/a Kindred Chicago* Lakeshore (Cook County Circuit Court, Dec. 12, 2019); *Robertson v. Hostmark Hospitality Group* (Cook Cty. July 31, 2019).
- The issue of the appropriate limitations period for BIPA claims is currently pending in Illinois appellate courts, including the First Appellate District. *Cortez et al. v. Headly Mfg. Co.*, No. 2019-CH-04935 (Cir. Ct. Cook County) (certifying a question regarding the appropriate limitations period which was subsequently granted by the First Appellate District); *Tims v. Black Horse Carriers*, No. 2019-CH-03522 (Cir. Ct. Cook County) (same).

Whether the Technology Collects or Captures “Biometric Information”

- Defendants have argued that the data at issue is not in fact a biometric identifier as defined by BIPA but have thus far been unsuccessful.
- *See Rivera v. Google Inc.,* 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017) (denying motion to dismiss based on Google's argument that a scan of facial geometry from a photograph was not a biometric identifier); *Monroy v. Shutterfly, Inc.,* No. 16-cv-10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017) (denying motion to dismiss based on Shutterfly’s argument that a scan of facial geometry from a photograph was not a biometric identifier).

Extraterritorial Application of BIPA to Acts That Occurred Outside of Illinois

- Defendants have argued that BIPA cannot be applied to acts that occurred outside the state limits, what is referred to as “extraterritorial” application.
- Thus far, this argument has not been successful to the extent that there remains some connection to activity in Illinois.
- For example, in *Patel v. Facebook*, Facebook argues that its servers – which actually collected the face scan images at issue in the case – were located outside of Illinois and therefore, that the class should not be certified as individualized inquiries would need to be conducted to determine where the photo at issue was taken, where it was uploaded, etc. Ninth Circuit rejected that argument, holding that BIPA applies to individuals located in Illinois, even if some of the prohibited activities occurred outside of Illinois.

Calculation of Damages and Penalties

- To date, no known actual damages demonstrated by any plaintiff in any BIPA case (remarkable).
- Therefore, the damages debate centers around whether the statutory penalties mandated under BIPA accrue each time an employee swipes in and out, and whether an employee can recover damages for alleged separate violations of BIPA (failure to obtain consent, maintain a policy, and disclosing information without consent).Also debate regarding whether there can be multiple penalties per employee per violation (daily swipes in and out PLUS failure to maintain retention schedule)
- Plaintiffs are arguing for maximum penalties – per swipe – to maximum valuation of damages and coerce settlements.

Negligent Versus Willful Violations

- The law is still unsettled in this regard. To date, no Court has ruled on the merits what the difference/standard is for negligent v. willful violations.
- However, some courts have dismissed allegations of willful violations at the motion to dismiss stage. *Namuwonge v. Kronos, Inc*., 1:19-CV-03239, 2019 WL 6253807 at *5 (N.D. Ill. Nov. 22, 2019) ("[Plaintiff] does not allege any substantive details regarding whether the allegations were reckless or intentional….Thus, [Plaintiff]'s claim for damages based on intentional and reckless conduct is dismissed."); *Rogers v. CSX Intermodal Terminals, Inc*., No. 1:19 C 2937, 2019 WL 4201570, at *4 (N.D. Ill. Sept. 5, 2019) ("Rogers' conclusory statement of CSX's intent is insufficient to allow us to infer that CSX acted intentionally or recklessly and does nothing to distinguish this case from every possible BIPA case where the defendant is alleged to have failed to meet the strictures of Section 15."); *See*, *e.g.*, *Thurman v. Northshore Univ. Health System,* Case No. 18 CH 3544, at 14 (Cir. Ct. Cook Cty. Dec. 12, 2019) (Valderrama, J.) (same).

Class Certification

- Significant battles over the uniformity of a class to be certified have already begun.
- In *Patel v. Facebook*, for example, defendants argued unsuccessfully that individualized inquiries would need to be conducted regarding each class member's use of Facebook and the tagging feature.
- Likely that defendants will continue to focus on the individualized inquiries required in order to work to defeat class certification.

Settlement

- BIPA's mandatory statutory penalties have resulted in massive settlements despite no evidence that any plaintiff has experienced actual harm from the collection or use of the biometric information at issue.
- As noted, the *Patel v. Facebook* lawsuit, encompassing millions of Illinois class members, resulted in an incredible $550 million settlement, after the Supreme Court declined to review the Ninth Circuit's ruling upholding class certification and federal court jurisdiction.
- Recently, the district court has raised doubts about approving the settlement, remarking that it provides too little relief per class member as compared to the available statutory penalties.
- Many other settlements driven by the statutory penalties, and expect those to continue unless there is legislative relief.

Considerations When Getting Into Compliance

Getting Into Compliance

- Recommend working closely with counsel to ensure analysis of exposure and implementation of compliance is privileged as much as possible.
- In particular, consider whether litigation is pending. Certain privileges apply to efforts taken to get into compliance but these privileges are not absolute and should plan that these efforts could be introduced into litigation as evidence that defendant knows compliance was required.
- Practical issues with implementation include:
  - Written “release” required under the statute says that it must be a “condition of employment” – what to do with employees that refuse to consent
  - Consider implementing with all employees that touch Illinois – not just the ones primarily sited in Illinois
  - Consider how to make policy “publicly available”
  - Check with third party service providers to understand how they are using and sharing any data

Proposed Legislative Fixes

Pending Legislative Amendments

- Several bills introduced this legislative session, through the efforts of the Illinois Chamber, that attempt to fix the most significant issues with BIPA.
- Minority Leader Durkin's House Bill 5374/Senator Barickman SB 3593:
  - Allows employers 30 days to cure any reported violations.
  - Removes the automatic statutory penalties, requiring a plaintiff to show she was actually damaged by the alleged collection or dissemination of the biometric information.
  - Cleans up perplexing ambiguities in the statute that could be read to require that employers terminate employees who refuse to consent to providing biometric information (requiring that an employee sign a release "as a condition of employment").
  - Ensures sensitive policies governing biometric information are shared only with parties who have reason to know.
  - Makes clear that collectively bargained resolutions to these issues should be honored.

Pending Legislative Amendments

- House Minority Leader Durkin and Senator Barickman also introduced HB 5375/ SB 3591. This was the most employer friendly of the introduced legislation.
  - Eliminates the private right of action, with some clarifications to be sure all violations fall into just one of two categories, as well as must be acted upon within one year from the date of the violation. Enforcement with the Department of Labor.
  - Cleans up perplexing ambiguities in the statute that could be read to require that employers terminate employees who refuse to consent to providing biometric information (requiring that an employee sign a release “as a condition of employment”).
  - Ensures sensitive policies governing biometric information are shared only with parties who have reason to know.
  - Makes clear that collectively bargained resolutions to these issues should be honored.

Pending Legislative Amendments

- SB 3591, Senator Barickman, provides that a prevailing party in a BIPA suit may recover $1,000 or actual damages, whichever is greater, against a private entity that violates that Act. The $1,000 applies only to each unique biometric identifier (e.g. $1,000 for an index finger scan or $1,000 per facial scan) and not for every single time the biometric identifier was scanned.
- Senator Cunningham's SB 3776:
  - Limits damages for current and former employers to a plaintiff's "actual damages."
  - But fails to address the concerns regarding the plaintiffs' bar's excessive counting of violations over a too-long time period.
  - Response to a constituent issue after a lawsuit against a nursing home in the Senator's district
  - Intended as a starting point--not the final product

How You Can Get Involved

Get Involved To Advance BIPA Amendments

- As a business leader/owner, or work with your company's government relations department to:
  - Contact your state representatives and advocate for prioritizing passage of amendments to BIPA.
  - Author a short op-ed in local paper or on-line explaining how the law is unfair to your company (emphasize you are simply trying to run a business and can't afford huge legal bills).
  - Emphasize your company already complies with a matrix of complicated state and federal laws and that you want to protect biometric information but the laws need to be reasonable and not unduly punitive.
  - If possible, make personal visits to your representatives. There are companies doing this right now.
  - Partner with the Illinois Chamber of Commerce which has been advocating on this issue over the last year and partnering with lawmakers.

Poll Question

- Are you interested in being involved in the legislative efforts to amend BIPA?
  - **Yes**, I'd like to be an active participant in amending BIPA legislation and get regular updates.
  - **Perhaps,** I'd like to receive more information on how to be involved.
  - **No**, I do not want to be involved.

(Phone attendees may email any presenter to participate).

Questions?

Thomas E. Ahlering
Partner
Seyfarth Shaw LLP

tahlering@Seyfarth.com
312-460-5922

Ada Dolph
Partner
Seyfarth Shaw LLP

adolph@Seyfarth.com
312-460-5977

Randel K. Johnson
Partner
Seyfarth Shaw LLP

rkjohnson@Seyfarth.com
202-772-9730

Clark Kaericher
VP of Government Affairs
Executive Director Technology and Infrastructure
Illinois Chamber of Commerce

ckaericher@ilchamber.org
217-522-5512 Ext. 296