Illinois Biometric Information Privacy Act
"BIPA"

SANDBERG PHOENIX

ST. LOUIS, MO
CLAYTON, MO
KANSAS CITY, MO
CARBONDALE, IL
EDWARDSVILLE, IL
O'FALLON, IL

www.sandbergphoenix.com

Timm Schowalter, CIPP/US

Presenter

PROFESSIONAL AFFILIATIONS

Missouri Bar Association

Illinois Bar Association

Bar Association of Metropolitan St. Louis

Defense Research Institute Cybersecurity and Data Privacy Group

Defense Research Institute Labor and Employment Practice Group

International Association of Privacy Professionals

Mackrell International

Sandberg Phoenix's internal Cybersecurity & Privacy Risk Management Group, Chair

EDUCATION

J.D., University of Missouri-Columbia

B.A., Southeast Missouri State University

Certified Information Privacy Professional/United States (CIPP/US)

SANDBERG PHOENIX

Background of BIPA

- BIPA became effective on October 3, 2008.
- Its purpose is to protect the public welfare through regulation of the use of biometric information.
- This is due to the growth of the use of biometric information in businesses in Illinois, especially Chicago.

Why do we have BIPA?

The legislature explicitly stated their intent within the Act:

"Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions…The full ramifications of biometric technology are not fully known." 740 ILCS 14/5(c), (f)

Definitions: Biometric Identifier 740 ILCS 14/10

Includes:

- Retina scan
- Iris scan
- Fingerprint
- Palm print
- Voice recognition
- Facial geometry recognition
- DNA recognition
- Gait recognition

Does not Include:

- Human biological samples
- Writing samples
- Written signatures
- Photographs
- Demographic data
- Tattoo descriptions
- Physical descriptions
- Donated organs
- Blood or serum stored for transplants
- Biological materials regulated under the Genetic Information Privacy Act
- Patient information or scans gained in a healthcare setting

Definitions: Biometric Information 740 ILCS 14/10

- Any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

  - The definition of "biometric identifier" (on the previous slide) is relevant in determining "biometric information."

Why are the requirements of BIPA important to know?

- When a company violates BIPA, the aggrieved individual has a right of action against the company. 740 ILCS 14/20

- If the individual prevails, then for "***each***" violation:
  - For negligence, the company will be assessed a $1,000 fine or actual damages, whichever is greater.
  - For intentional or reckless violations, the company will be assessed $5,000 or actual damages, whichever is greater.
  - The company is responsible for reasonable attorneys' fees and costs.
  - The company is responsible for any other relief, such as injunction.

Illinois BIPA Cases

- The majority of the cases involving BIPA violations have been filed in Cook County. However, St. Clair County is also becoming a popular venue for BIPA cases.

- Class Action cases can include hundreds or thousands of class members and companies can be assessed damages for each violation.
  - Highest settlement fund: $7 million
  - Lowest settlement fund: $35,000
  - Median range: ~ $450,000 to $900,000

- This does not include attorneys' fees and costs, which often are 35% or more of the judgment.
  - For instance, in *Sekura v. L.A. Tan*, the attorneys' fees were $600,000.

Requirements Under BIPA

740 ILCS 14/15(a)

- Any private entity that is in possession of “biometric identifiers” or “biometric information” must comply with the BIPA requirements.

- Create a written policy made available to the public establishing:
  - A retention schedule
  - Guidelines for permanently destroying biometric identifiers and biometric information. The policy must include that:
    - It will be destroyed when the initial purpose of retaining it has been satisfied

    OR
    - Within 3 years of the individual’s last interaction with the private entity; whichever occurs first

- The policy must be adhered to unless there is a valid warrant or subpoena issued by a court.

Requirements Under BIPA

740 ILCS 14/15(b)

- No private entity can obtain biometric identifiers or information unless the following requirements are met:
  - The individual must be informed in writing.
  - The individual must be informed in writing of the specific purpose and length of term for which it will be collected, stored, and used.
  - The individual must sign a written release.

Requirements Under BIPA

740 ILCS 14/15(c)

- No private entity can do the following with biometric information and/or identifiers:
  - May sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

Requirements Under BIPA

740 ILCS 14/15(d)

- No private entity can do the following with biometric information and/or identifiers
  - disclose, ***redisclose***, or otherwise disseminate a person's or a customer's biometric identifier or biometric information
- However, dissemination of the information or identifiers can occur where:
  - The individual consents, OR
  - Completes a financial transaction requested or authorized by the subject
  - It is required by State or Federal law, OR
  - It is required pursuant to a valid warrant or subpoena issued by a court.

Requirements Under BIPA

740 ILCS 14/15(e)

- Every private entity in possession of a biometric identifier or information must do the following:
  - Reasonably store, transmit, and protect it from disclosure.
  - Store, transmit, and protect it from disclosure in the same manner or in a more protective manner in which the private entity does for other confidential and sensitive information.

Definitions: Private Entity

740 ILCS 14/10

Includes:

- Individuals
- Partnerships
- Corporations
- Limited Liability Companies
- Associations
- Any other group, however organized

Does not include:

- State government agencies
- Local government agencies
- Illinois courts
- Clerk of Illinois courts
- Judge or Justice of Illinois courts

Definitions: Written Consent
740 ILCS 14/10

- Any informed written consent.

- However, when it is in the context of employment, it can include a release executed by an employee as a condition of employment.

Construction of BIPA
740 ILCS 14/25

- BIPA does not impact discovery in any court action.

- BIPA does not apply to:
  - X-Ray Retention Act
  - Patient information in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under HIPAA
  - Financial institutions subject to Title V of the Gramm-Leach-Bliley Act
  - Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act
  - Contractors, subcontractors, or agents of a State agency or local government when working for that State agency or local government

Plaintiffs' Lawyers "Dream" Statute

- *To date both state and federal courts have consistently and on nearly every legal issue found in favor of the Plaintiffs*

- *Please don't kill the messenger but let's take a look….*

Standing

Doesn't the individual need to be harmed or have an "injury in fact" to bring a claim?...Nope

- In *Rosenbach v. Six Flags Entertainment Corporation* (Jan. 2019), the Illinois Supreme Court unanimously held that a plaintiff may be "aggrieved" under BIPA — with statutory standing to sue for significant statutory damages— even without alleging an "actual injury" caused by the BIPA violation.
- In *Fox v. Dakkota Integrated Sys., LLC*, (Nov. 17, 2020) the Seventh Circuit found standing existed without an injury in fact

Statute of Limitations

- BIPA itself does not include a statute of limitations

1 year

- Invasion of privacy claims come with a one-year statute of limitations. Id. (citing 735 ILCS 5/13-201). And because BIPA is, fundamentally, a privacy statute, the argument is that BIPA should be subject to a one-year limitations period

2 year

- Statutes that carry a statutory penalty come with a two-year statute of limitations. And because almost all BIPA actions claim the statutory damage amount (rather than seeking actual damages), the argument is that BIPA should be subject to a two-year limitations period.

5 year

- Most federal courts and the Illinois trial courts have concluded that BIPA is subject to the five-year catchall limitations period

Statute of Limitations – Per Swipe

Financial Devastation …..

"Each time that White Castle disclosed biometric information to a third patty without consent it violated Section 15(d)….. the Court fully acknowledges the large damage awards that may result from this reading of the statute…. If the Illinois legislature agrees that this reading of BIPA is absurd, it is of course free to modify the statute to make its intention pellucid. But it is not the role of a court—particularly a federal court—to rewrite a state statute to avoid a construction that may penalize violations severely." *Cothron v. White Castle Systems, Inc.* (N.D. Ill, Aug. 7, 2020)

Preemption- Workers Compensation

If fingerprints are captured in the scope of employment for payroll purposes, then isn't this a workers' compensation claim?

No… On September 18, 2020 an Illinois Appellate Court struck down this key defense. *McDonald v. Symphony Bronzeville Park LLC*, 2020 IL App (1st) 192398

Preemption- NLRA

Are BIPA claims preempted by a grievance and arbitration provisions in a Labor Agreement?

Maybe… in certain circumstances. The specificity of the language will control

See, *Peatry v. Bimbo Bakeries USA, Inc.*, (N.D. Ill. Feb. 2020) and *Miller v. Southwest Airlines Co.,(N.D. Ill, June 2019)* but see *Treadwell v. Power Solutions Int'l, Inc.*, (N.D. Ill. Dec. 16, 2019)

Arbitration

Can you use an arbitration agreement to preclude these class action lawsuits?

- Possibly, but carefully draft your agreements with assistance of counsel:
  - *In Liu v. Four Seasons Hotel, Ltd*., (Ill. App. Ct. 1st Dist. 2019) the Court found that the arbitration clause in the employer's employment agreement DID NOT cover BIPA claims

Joint Employer

Is a parent company liable under BIPA for its subsidiary's violations?

Is a franchisor liable for a franchisee's BIPA violation?

> Possibly, In *Wordlaw v. Enterprise leasing Co of Chicago, LLC*, (N.D. Ill, Dec, 21, 2020) a federal court recently allowed a case to pursue against a parent company under a joint employer theory because the Complaint sufficiently alleged the parent significantly controlled the work environment in several important respects.

Retroactive Application of Consent

Can I cure BIPA violations by going back and obtaining signed consent forms from all employees?

Good try but no. In *Lenoir v. Little Caesar Entreprises, Inc.,* (N.D. Ill. Aug. 7, 2020) the Court held consent provided by two former employees after their biometrics were already collected does not apply to the collection retroactively.

There is Hope

A Court actually dismisses a BIPA claim

In *Vo v. VSP Retail Dev. Holding, Inc*. the Court held that defendant's software application that scans user's face geometry and then overlays digital eyewear on the scan, allowing the user to remotely "try on" both prescription and non-prescription glasses. The software offered both prescription eyewear and replicated services that would typically be performed by an eye care professional, and thus the defendant "collected biometric information from a patient in a health care setting" akin to an initial medical evaluation.

Best Practices: Protect Your Company

- Contact your state representatives and/or hire a lobbyist to effectuate change in the law.
- Contact insurance broker to confirm or obtain insurance coverage to cover BIPA claims.
- Review third-party vendor agreements and seek indemnification language
- Consider whether use of biometric data is necessary and appropriate for your business.

Best Practices: Protect Your Company

- If relying on biometric data, have your policies and consent forms reviewed by counsel to ensure they are broad in scope and address all BIPA requirements.
  - Ensure that the notice adequately discloses why you collect, how you use, how you store, and how you disclose biometric data.
  - Ensure policy covers redisclosures
  - Ensure policy includes retention and disposal guidelines
- If relying on biometric data, provide advance notice to the individuals and obtain written informed consent.
- Include BIPA policies, notice and consent forms in the onboarding process.
- Include biometric policies in your handbooks/manuals/bulletin board.

Best Practices: Protect Your Company

- Closely monitor and comply with data retention/destruction policy.
- Allow individuals to opt out of biometric information collection.
- For employees who have not provided consent obtain their written consent along with a legal release of BIPA claims (provide consideration such as vacation day, small bonus, etc.).
- Stay abreast of the latest legal developments in this area and work with your attorney.
- Follow me on LinkedIn and Sandberg Phoenix's blogs

And, of course COVID-19

Does BIPA Apply to COVID-19 Screening?

- BIPA specifically excludes several categories of information from the definition of "biometric identifier," including "biological samples used for valid scientific testing or screening.“

- So generally, BIPA does not govern COVID-19 testing or temperature screening that may be administered by an employer. The act does apply, however, if an employer uses screening technology that captures a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," such as a contactless thermometer that uses face scan technology to identify employees before taking their temperatures.

Thank you.
Please contact us with any questions.

Timm W. Schowalter, CIPP/US
600 Washington Avenue, 15th Floor
St. Louis, MO 63101
314.425.4910 (Direct)
314-609-7552 (Cell)
tschowalter@sandbergphoenix.com
https://www.linkedin.com/in/tschowalter

ST. LOUIS, MO
CLAYTON, MO
KANSAS CITY, MO
CARBONDALE, IL
EDWARDSVILLE, IL
O'FALLON, IL