Thumbs Up: Fundamentals of Illinois' Biometric Information Protection Act

The Apex Jurist, **www.ApexJurst.com** is
Published by ApexCLE, Inc.
www.ApexCLE.com

119 South Emerson St., # 248
Mount Prospect, Illinois 60056

Ordering Information:

Copies of this monograph may be ordered direct from the publisher for $64.95 plus $4.25 shipping and handling. Please enclose your check or money order and shipping information. For educational, government or multiple copy pricing, please contact the publisher.

Library of Congress Cataloging-in-Publication Data

ApexCLE, Inc.

1. ApexCLE, Inc. 2. Law-United States – Guide-books.

3. Legal Guide 4. Legal Education.

About the Presenter

Todd M. Rowe

Todd M. Rowe has worked on cyber/privacy matters ranging from pre-breach consultation, breach response to cyber insurance. Todd created Tressler's Privacy Practice Group before most law firms were even aware of the privacy issues facing their clients. Over the years, Todd has assisted clients in nearly every industry and level of government to formulate their strategy for privacy and data issues. Todd's articles and presentations provide insight for others grappling with the emerging privacy issues in the legal, insurance, government and business communities.

In addition to assisting with breach responses, Todd assists clients on the following:

Cyber-Risk Insurance Claims: Working with underwriters on policy provisions and counseling clients on issues in this emerging area of law.
Cyber Response: Working with small and medium sized businesses on cyber/privacy issues both before and after incidents.

In addition to chairing Tressler's Privacy Practice Group and Insurance Practice Group, Todd handles insurance matters related to liability, first party property and E&O/D&O insurance.

Todd still draws on his significant commercial litigation experience and assists business and industrial clients on contract/indemnity issues, resolving disputes prior to litigation and handling litigation in a number of jurisdictions. Todd also counsels clients on the potential for cyber risk liability and compliance with state and Federal privacy laws.

MEMBERSHIPS & AFFILIATIONS

- Illinois State Bar Association, Member
- Michigan State Bar Association, Member
- Wisconsin State Bar Association, Member

Email Address: trowe@tresslerllp.com

Website: www.tresslerllp.com

Mailing Address: 233 S. Wacker Drive, 61st Floor, Chicago, IL 60606

Phone Number: 312-520-2521

Table of Contents

Contents

Course Description

Illinois' privacy laws are leading the way across the nation in privacy. The Biometric Information Protection Act, or BIPA, is a unique law that protects the biometric information of Illinois residents. While many states have taken steps to protect personal information, many state legislatures and courts are watching the development of BIPA. This course will provide a basic understanding of BIPA and the best strategies to get clients in compliance with these requirements.

Course Presentation

This course is an introductory level course discussing which is good for a new attorney or new area for any attorney.

This course provides a base of skills, knowledge and perspectives regarding privacy/cyber laws.

Course Material

This material is intended to be a guide in general and is not legal advice. If you have any specific question regarding the state of the law in any particular jurisdiction, we recommend that you seek legal guidance relating to your particular fact situation.

The course materials will provide the attendee with the knowledge and tools necessary to identify the current legal trends with respect to these issues. The course materials are designed to provide the attendee with current law, impending issues and future trends that can be applied in practical situations.

Course Learning Objectives and Outcomes

The ability to understand the duties, roles and responsibilities of counsel in situations involving personal and biometric information belonging to Illinois residents.

Participants will learn practice tips regarding compliance with BIPA and how to spot possible violations.

Participants will develop an understanding about the technology that collects biometric information and the laws protecting the use and storage of this information.

Participants will gain practical skills in the area of BIPA litigation, which is flourishing in Illinois, and the number of issues related to standing to bring these cases and the best ways to evaluate the evidence.

This course does not touch upon ethics or professionalism.

Upon completion of the course, participants should be able to apply the course material; improve their ability to research, plan, synthesize a variety of sources from authentic materials, draw conclusions; and demonstrate an understanding of the theme and concepts of the course by applying them in their professional lives.

Timed Agenda:

Presenter Name: Todd M. Rowe

CLE Course Title: Thumbs Up: Fundamentals of Illinois' Biometric Information Protection Act

Time Format (00:00:00 - Hours:Minutes:Seconds)	Description
00:00:00	ApexCLE Company Credit Introduction
00:00:20	CLE Presentation Title: Thumbs Up: Fundamentals of Illinois' Biometric Information Protection Act
00:00:32	CLE Presenter Introduction
00:00:52	CLE Substantive Material Presentation Introduction
00:02:59	Illinois' Biometric Information Protection Act: Its Origin Story
00:03:58	740 ILCS 14 et seq.
00:05:30	BIPA: Section 10 Definitions
00:11:48	The Recent Prevalence of The Use of Our Biometric Data
00:17:10	BIPA: Purpose of the Act
00:25:42	BIPA: Section 15 Data Protection
00:34:48	BIPA: Penalty for Non-Compliance
00:39:09	BIPA: Damages
00:46:21	BIPA Claims Against Employers
00:49:16	BIPA: Evolution and Constitutionality
00:57:11	BIPA: Proper Statute of Limitations
01:05:50	Presenter Closing
01:07:04	ApexCLE Company Closing Credits
01:07:10	End of Video

Thumbs Up: Fundamentals of Illinois' Biometric Information Protection Act

1. Introduction to The Illinois Biometric Information Protection Act

It is difficult to believe the Illinois Biometric Information Protection Act, 740 ILCS 14, ("BIPA") has been in effect since October 3, 2008. Many data collectors are surprised BIPA has been in effect for seven years as it has only grown into a major concern because the equipment that collects biometric data has evolved to the point that it can be found in a number of Illinois workplaces and businesses.

Analysis of BIPA Section 740 ILCS 14/5

The best place to start with an analysis of BIPA is the statute. Section 740 ILCS 14/5 provides the following key points as the "Legislative Intent" behind enacting this law:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) 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.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

Section 10 of BIPA

Section 10 of BIPA, entitled definitions, provides insight into the information that is considered a "biometric identifier" and, therefore, is subject to the protections of BIPA. First, information that is protected under BIPA includes: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. More tellingly, BIPA specifically lists the following information that is not protected to BIPA

> …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. Biometric identifiers do not include 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. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. 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 the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an 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 test.

Section 15 of BIPA

Section 15 of BIPA, entitled "retention; collection; disclosure; destruction," requires a "private entity in possession of biometric identifiers or biometric information [to] develop a written policy, made available to the public, establishing 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."

2. The Recent Prevalence of The Use of Our Biometric Data

Taylor Swift has a stalker problem. In April 2018, a man broke into her New York City loft and took a shower before falling asleep in her residence. The same stalker attempted to break Taylor Swift's front door down with shovel in February 2018. Other stalkers have sent emails threatening to kill Taylor Swift's entire family. Suffice to say, Taylor Swift and other public personalities should take all reasonable steps to protect themselves and their families. And, thankfully, it appears Taylor Swift is taking these threats seriously. In addition to taking a variety of other security measures, a number of news reports indicate Taylor Swift has installed a face-recognition camera at her concerts that cross-references pictures of her known stalkers.

A recent Rolling Stone article provides the following information concerning this new security measure:

> *Taylor Swift fans mesmerized by rehearsal clips on a kiosk at her May 18th Rose Bowl show were unaware of one crucial detail: A facial-recognition camera inside the display was taking their photos. The*

> *images were being transferred to a Nashville "command post," where they were cross-referenced with a database of hundreds of the pop star's known stalkers, according to Mike Downing, chief security officer of Oak View Group, an advisory board for concert venues including Madison Square Garden and the Forum in L.A. "Everybody who went by would stop and stare at it, and the software would start working," says Downing, who attended the concert to witness a demo of the system as a guest of the company that manufactures the kiosks.*

While there is no reasonable argument against Taylor Swift taking reasonable steps to protect herself from stalkers, we cannot ignore the privacy questions related to this new security method. Specifically, there are significant questions involving the privacy of individuals that have their images captured, the vast majority are not stalkers. And, unfortunately, there is little guidance on how this new technology should be used.

While we do not have substantial legal guidance on this new security method using biometric data, there are at least a couple of sources that provide some insight. At present, most protections for biometric data arises out of state laws and regulations such BIPA. BIPA states that "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." As it stands, the technology that allows for the storage and collection of biometric data may be outpacing the development of protections for this information. For example, by using the term "aggrieved," there is a possible violation under at least one or any of the following scenarios:

- The collection of biometric data without the individual's consent;
- The collection and use of biometric data without the individual's consent;
- The collection of biometric data with consent but use without consent;
- The collection of biometric data with consent and use of the data outside the limited consent provided by the individual.

While BIPA clearly states any person "aggrieved by a violation" of BIPA has a potential cause of action, there is little guidance as to when a person should bring suit.

Privacy Issues

The privacy issues are clear even when viewed outside of the various biometric data laws. For example, the Rolling Stone article on Taylor Swift's use of the images asks: "Despite the obvious privacy concerns — for starters, who owns those pictures of concertgoers and how long can they be kept on file?"

And, that is a reasonable question for any data collector or individual having their data collected. In addition to the concerns discussed in Rolling Stone, there are a number of other questions that quickly come to mind: Can Taylor Swift keep the images and cross-reference them down the road when new stalking cases arise? Are the images limited to be used in only stalking cases? Can Taylor Swift use the images for marketing purposes? Do concertgoers need to give consent to have their images taken? In simpler terms, Taylor Swift's security team will need to analyze the likelihood that non-stalker concert-goers are going to be "aggrieved" by having their photos taken without consent. Suffice it to say, the parent in Rosenbach may be just as angry if she sent her teenager to a Taylor Swift concert and her child was photographed without consent. Consequently, even though courts are increasingly providing clarification on these issues, we can expect to see technology continue to outpace the law on biometric issues.

3. Illinois Is the State to Watch for BIPA Law Developments

While many states are still struggling to enact comprehensive cyber/privacy laws and the federal government still lacks a uniform framework, Illinois data collectors have been working under the most advanced privacy statutes and common law in the United States. Specifically, the Illinois legislature has taken steps through the Personal Information Protection Act and the Biometric Information Protection Act ("Biometric Act") that will put data collectors and courts at the forefront of privacy law for years to come.

The Latest Development In Illinois Privacy Law

The latest development in Illinois privacy law was the Illinois Supreme Court issued its decision in Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Jan. 25, 2019) which provides insight on what is necessary to bring a cause of action under the Biometric Act. In Rosenbach, the Illinois Supreme Court analyzed the provision in the Biometric Act which states that "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." The central question for the Supreme Court was whether the use of the term "aggrieved" in the Biometric Act requires a plaintiff assert that they suffered an injury in addition to having their biometric data collected. In reversing the Illinois Court of Appeals, the Supreme Court found a violation of

the Biometric Act when a data collector merely took information from a minor without proper consent. The most important aspect of this case is a data collector can be liable without breaching any information.

The Facts in *Rosenbach*

The Defendant, Six Flags Entertainment Corporation ("Six Flags"), operates an amusement park located in Gurnee, Illinois. The Plaintiff, Stacy Rosenbach ("Rosenbach"), is a parent of a 14-year-old boy that visited Six Flag's amusement park for his class trip. Before the trip, Rosenbach purchased a season pass for her son using Six Flag's website. Rosenbach claims she was surprised to find out that her son was directed to scan his thumbprint to gain access to Six Flags and to receive his season pass card. Rosenbach claims she would not have purchased the season pass for her son if she knew Six Flags intended to collect his thumbprint without obtaining written consent or disclosing their plan to collect such data. Rosenbach claimed she was "aggrieved" under the Biometric Act without any allegation that Six Flags breached any data.

In Rosenbach, The Illinois Supreme Court provided the following analysis of the term "aggrieved" as in the Biometric Act:

> *More than a century ago, our court held that to be aggrieved simply "means having a substantial grievance; a denial of some personal or property right." Glos v. People, 259 Ill. 332, 340 (1913). A person who suffers actual damages as the result of the violation of his or her rights would meet this definition of course, but sustaining such damages is not necessary to qualify as "aggrieved." Rather, "[a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment." (Emphasis added.) Id.¶*

The Illinois Court of Appeals' Decision Is Reversed

The Illinois Court of Appeals held the allegations that Six Flags took patrons' thumbprints without proper consent was not a violation of the Act because the patrons were not "aggrieved" as required by the Biometric Act. In reversing the Court of Appeals, the Illinois Supreme Court held:

> *In sum, defendants' contention that redress under the Act should be limited to those who can plead and prove that they sustained some*

actual injury or damage beyond infringement of the rights afforded them under the law would require that we disregard the commonly understood and accepted meaning of the term "aggrieved," depart from the plain and, we believe, unambiguous language of the law, read into the statute conditions or limitations the legislature did not express, and interpret the law in a way that is inconsistent with the objectives and purposes the legislature sought to achieve. That, of course, is something we may not and will not do.

Potential Impact Of This Decision

The Rosenbach decision will undoubtedly cause ripples in privacy law for years to come as a party can conceivably maintain a viable cause of action without pleading any "actual injury or damage." This decision may close the door on data collectors being held liable only when they breach biometric data. Rather, data collectors will need to review all processes that may collect biometric data to confirm they are complying with the Biometric Act. For example, Six Flags may now need to revamp its use of thumbprints to make sure it obtains consent from a minor's guardian and they make clear how the data will be used.

Further, this decision may undercut the usefulness of expensive equipment used to collect biometric data if a majority of people withhold their consent to have their information collected. For example, many workplaces have started to track employees' hours by using biometric data including fingerprints and thumbprints. These new systems that rely on biometric data make "clocking in" more convenient than systems that may rely on employee numbers or time cards. It will be interesting to see how employers will work with employees that refuse to consent to having their biometric information collected after the employer purchased the expensive equipment. Suffice it to say, we can expect Illinois to continue to be the source of many influential developments in privacy law in the coming years.

4. BIPA Lawsuits

BIPA Claims Against Employers

Biometric data is playing a larger role in employment law as more employers begin using equipment to scan employees' fingerprints to clock in for work. Each

week more employers are defending themselves against claims by the employees such as the class action lawsuit filed against Patriot Medical Transport in Cook County Circuit Court last month. The employees in the Patriot Medical litigation claim they "have suffered injury from the unlawful collection and storage of their fingerprints, hand geometry or other biometric data." We can expect these class actions to continue to increase with the increased use of equipment that collects and stores biometric data.

While many of these cases are still in their early stages, the parties in Miller v. Southwest Airlines Co., 18-3476 (7th Circ. 2018) have already had a decision and are in the midst of an appeal related to equipment used to track employees through biometric data. In their brief submitted to the Seventh Circuit Court of Appeals, the Class Action Plaintiffs, who are "ramp and operations agents who worked and/or work for Southwest at Chicago's Midway International Airport," claim Southwest Airline's timekeeping system violates the Illinois Biometric Information Protection Act ("BIPA").

Southwest adopted a timekeeping system that uses biometric identifiers and biometric information (fingerprints) to track their employees' time at work. The Class Action Plaintiffs claim Southwest's timekeeping system requires them to scan their biometric data into the system even though Southwest "did not obtain the requisite written consent, and did not publish a publicly available retention and destruction schedule." In addition to claiming injuries from the alleged BIPA violation, the Class Action Plaintiffs "also alleged that they lost compensation as a result of Southwest's actions as they 'would not have agreed to work for [Southwest], at least not for the compensation they received, had they been informed pursuant to BIPA of the nature of Defendant's biometric timekeeping system.'"

The Class Action Plaintiffs stated the question for the Seventh Circuit Court of Appeals as follows:

Did the district court err when it ruled that Plaintiffs-Appellants' claims under the Illinois Biometric Privacy Information Act, 740 ILCS 14/1, et seq., were preempted by the Railway Labor Act, 45 U.S.C. § 151, et seq., because they constitute a "minor" dispute?

While this litigation is primarily based on employment law and related to issues between Southwest and its employees, there are a number of points where the Seventh Circuit will conceivably need to consider the reach of BIPA. Specifically, this litigation ended up before the Seventh Circuit when the U.S.

District Court for the Northern District of Illinois held the Class Action Plaintiffs' BIPA claim was preempted as a minor dispute under the Railway Labor Act ("RLA").The RLA is intended "to promote stability in labor-management relations by providing a comprehensive framework for resolving labor disputes" by establishing a "mandatory arbitral mechanism for the 'prompt and orderly settlement' of two classes of disputes, characterized as 'major' and 'minor' disputes.'"

Specifically, the District Court reasoned that the Class Action Plaintiff's Collective Bargaining Agreement ("CBA") would govern whether the Class Action Plaintiffs were injured by the alleged BIPA violation:

> *…Plaintiffs further allege they 'would not have agreed to work for Defendant, at least not for the compensation they received, had they been informed pursuant to BIPA of the nature of Defendant's biometric timekeeping system.' (Id.) Among the relief Plaintiffs seek is compensation for the commercial value of their biometric information.*
>
> Because the CBAs govern the rates of pay, rules, and working conditions of Plaintiffs' employment, Plaintiffs' BIPA claim 'requires interpretation of the CBA to determine whether [Defendant] has the authority to use a particular timekeeping system for employees.' Johnson, 2018 WL 3636556, at *2. Specifically, the CBAs dictate employees' wage rules, rates of pay, and bonuses. (See CBA, Jordan Decl. Ex. A (Dkt. No. 281) at Art. 28.) Defendant and TWU 555 negotiated the wage scales applicable to Plaintiffs, as well as other pay provisions relating to premium pay. (Jordan Decl. Ex. A (Dkt. No. 28-1) ¶ 8.)
>
> ***
>
> *Plaintiffs' BIPA claim cannot be resolved without interpreting the wage provisions of the CBAs and the relevant bargaining history to determine whether the wages TWU 555 and Defendant negotiated were intended to compensate employees for all conditions of their employment, including use of the biometric timekeeping system. Likewise Plaintiffs' challenge to Defendant's decision to implement the biometric timekeeping system requires an interpretation as to whether the decision falls within the scope of Defendant's right to 'manage and direct the work force.'"…*

In short, the District Court ruled the Class Action Plaintiffs' BIPA claim was a "minor dispute" under the RLA and dismissed their claim.

While there are a number of points where BIPA and employment intersect in this litigation, the Class Action Plaintiffs take positions that will undoubtedly test the reach of BIPA. For example, in addressing whether Southwest gave proper notice of the new timekeeping system, the Class Action Plaintiffs argue:

> *First, Southwest's alleged notice was given in 2005, three years before BIPA had even been enacted into law, and therefore had nothing to do with BIPA (or with the information required to be disclosed under BIPA). Second, Southwest produced no evidence that such notice was given in writing as required under BIPA. See 740 ILCS 14/15. Third, when it notes merely that the Union "did not object or seek an amendment" to the CBA in response (ECF No. 28-3 ¶ 10), Southwest conceded that it did not obtain written consent under BIPA to collect biometrics. In short, Southwest provided no evidence whatsoever of BIPA-compliant notice to, or BIPA compliant consent from, anyone—be it the Union or otherwise. As such, interpretation of the CBAs is not required to resolve Appellants' BIPA claim. The District Court erred when it found otherwise.*

The use of biometric data by employers is one of the first areas we can expect to see BIPA be tested by litigants. We have already seen a number of developments in 2019 related to BIPA when the Illinois Supreme Court in Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Jan. 25, 2019). The scheduling order in Southwest Airlines indicates the briefing should be complete by April 11, 2019. Business owners and their insurers will need to watch the progression of this litigation in this decision and many other lawsuits in Illinois in order to fully access whether their use of biometric data exposes them to liability from customers and employees.

B. Defenses: BIPA Customer Lawsuits

While there has been a huge increase in class action cases based on alleged violations of the Illinois Biometric Information Act ("BIPA"), it has not gone unnoticed that the vast majority of the recent cases are limited to allegations brought by employees against their employers rather than by customers. That is, the case law is developing into two distinct branches: BIPA customer cases and BIPA employment cases.

The rapid development of BIPA employment cases is surprising to the extent the Illinois Supreme Court's decision in Rosenbach v. Six Flags, 2019 IL 123186 (Jan 25, 2019) involved a customer of the Six Flags amusement park. It is still unclear if the BIPA customer lawsuits are not developing as quickly because equipment that collects biometric data is not being used for customers or customers are still unaware that their data is being gathered. Either way, there is little question that data collectors must brace for the next wave of BIPA cases brought by customers.

BIPA lawsuits related to photo storage applications provided by Google LLC ("Google") and other social media companies are providing some guidance on BIPA customer cases. In particular, Google Photos collects and stores photographs and promises to provide "[f]ree storage and automatic organization for all your memories." There are allegations that this technology uses "face templates" of the subjects in the photographs. This photo application has provided a number of BIPA cases outside the employment cases currently working through the courts.

On February 6, 2020, Brandon Molander ("Molander") filed a Class Action Complaint against Google LLC in the District Court for the Northern District of California based on alleged BIPA violations. Molander claims Google "created, collected, and stored, in conjunction with its cloud-based 'Google Photos' service, millions of 'face templates' (or 'face prints')—highly detailed geometric maps of the face—from millions of Google Photos users." (Molander Complaint at ¶ 5). The Molander Complaint continues: "Google creates these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces that appear in photos taken on Google Android devices and uploaded to the cloud-based Google Photos service." In particular, the Molander Complaint alleges that with this technology, "[e]ach face template that Google extracts is unique to a particular individual, in the same way, that a fingerprint or voiceprint uniquely identifies one and only one person."

The Molander Complaint provides the following concerning Google's technology:

- "In May 2015, Google announced the release of its photo sharing and storage service called Google Photos. Users of Google Photos upload millions of photos per day, making photographs a vital part of the Google experience." (Complaint at ¶ 19)

- The Google Photos app is pre-installed on all Google Android devices and "is set by default to automatically upload all photos taken by the

Android device user to the cloud-based Google Photos service." (Complaint at ¶ 20)

- "Unbeknownst to the average consumer, and in direct violation of [Illinois' Biometric Information Protection Act], Google's proprietary facial recognition technology scans each and every photo uploaded to the cloud-based Google Photos for faces, extracts geometric data relating to the unique points and contours (i.e. biometric identifiers of each face, and then uses that data to create and store a template of each face – all without ever informing anyone of this practice." (Complaint at ¶ 21)

Based on these allegations, Molander claims Google improperly collected, used and stored his biometric data without obtaining a written release, used his information without properly notifying individuals that his information was being gathered and used his information without providing a public "retention schedule or guidelines for permanently destroying the biometric identifiers and/or biometric information."

We have seen similar lawsuits filed against Google before Molander v Google LLC. For example, the Eastern District for the Northern District of Illinois analyzed BIPA claims related to Google Photos in Rivera v Google, Inc.,16 C 02714 (N.D. Ill 2016). In Rivera, the District Court found claims by Plaintiffs that Google collected, uploaded and scanned photographs to create "facial templates" were sufficient to survive Google's motion to dismiss. The District Court rejected Google's argument that Plaintiffs' class-action lawsuit should be dismissed because BIPA does not "apply to photographs or information derived from photographs." Plaintiffs countered that face geometry scans constitute "biometric identifiers" under BIPA and, thus, must be protected. Ultimately, on December 29, 2018, the Eastern District granted Google's motion for summary judgment finding "Plaintiffs have not suffered an injury sufficient to establish Article III standing and their claims are dismissed." Therefore, based on this case, Molander may have an uphill battle to establish Google violated BIPA with the collection, storage and use of his photographs.

Recent Developments

While only the Class Action Complaint has been filed at this point in Molander v. Google LLC, case no. 20-cv-918, there are some recent developments that may provide guidance in the Molander case and BIPA customer cases.

First, we have seen many of the biometric data cases, outside the employment context, reach a resolution since Rivera was decided by the District Court for the Northern District of Illinois. The most recent example was seen a couple of weeks ago when it was widely reported in January 2020 that Facebook settled its own class-action lawsuit for $550 million based on claimed violations of Illinois' Biometric Information Protection Act. The Facebook lawsuit seems to be based on technology that is similar to the technology at issue in Molander v. Google LLC: "The suit said the Silicon Valley company violated an Illinois biometric privacy law by harvesting facial data for Tag Suggestions from the photos of millions of users in the state without their permission and without telling them how long the data would be kept." Therefore, it will be important to watch the Molander case to see if a large settlement for this technology is a trend that continues. The Facebook settlement will undoubtedly get plaintiffs' class actions lawyers thinking about BIPA customer cases.

Additionally, there are questions as to how this technology will be used by companies for marketing or other unapproved uses. For example, we can expect to see more news about Clearview AI. Clearview AI created a massive database of photographs (estimates of 3 billion photographs so far) "scraped" from social media. At this point, Clearview AI has made this database only available to law enforcement. Since the Rivera case, companies such as Clearview AI provide a glimpse of how this technology can be used and the control people may lose over their biometric data. These new uses for this technology may view how courts decide these cases. Over the next few months, we will see if the initial wave of BIPA employment cases crests and if BIPA customer cases pick up the pace.

C. Is BIPA Unconstitutional?

There is little dispute that the Illinois Biometric Information Protection Act ("BIPA") is a unique privacy law to the extent that it creates a private cause of action for any failures to notify individuals before their biometric information is collected and stored. That is, BIPA potentially creates a liability regardless of whether there was a breach of private information. Further complicating matters is the fact that many data collectors that qualify as "financial institutions" or "local and state governments" are exempted from BIPA. A recent motion to dismiss filed by New Albertson's, Inc. ("Albertson's), a defendant named in a BIPA action, has put the constitutionality of this exemption for financial institutions and state governments at issue.

As with many employers in Illinois, Albertson's was named as a defendant in a lawsuit based on alleged violations of BIPA. In a lawsuit entitled Bruhn v. New Albertson's, Inc, Case No. 2018 CH 1737, filed in the Circuit Court of Cook County, Illinois, a class action plaintiff alleged he worked as a pharmacist at a Jewel-Osco store located in Elgin, Illinois. Plaintiff claims Jewel required him to provide a scan of his fingerprints on a biometric device in order to access the pharmacy's computer system. Plaintiff further claims Jewel violated BIPA when it collected and stored his biometric information without providing the proper notification. On August 20, 2019, Albertson's filed a motion to dismiss which will push Illinois courts to examine the constitutionality of BIPA.

As for a quick refresher on Illinois Constitutional law, the Illinois Constitution provides the following which is generally referred to as the "special legislation clause:"

> *The General Assembly shall pass no special or local law when a general law is or can be made applicable. Whether a general law is or can be made applicable shall be a matter for judicial determination.*

In support of its motion to dismiss, Albertson's analyzes the legislative intent behind BIPA and argues "[i]n short, the legislator felt BIPA was necessary to protect consumers' biometric data, particularly connected with financial information." And, while the legislature's intent behind BIPA was to protect information by placing burdens on entities that collect and store biometric data, Albertson's questions how that purpose is served when the statute does not include many entities that may qualify as a "financial institution or an affiliate of a financial institution" and contractors, subcontractors and agents of state or local governments. Based on these exclusions to BIPA, Albertson's argues that BIPA violates the special legislation clause and, is therefore unconstitutional because "Broad Groups" of individuals are excluded from the statutory framework. In particular, Albertson's claims BIPA's exclusions for financial institutions and local governments give way to an unfair result that is unconstitutional.

In its brief, Albertson's argues the question of whether a law violates the special legislation clause and is void includes the following two-step analysis: "…whether the statutory amendments discriminate in favor of a select group" and "if so, whether the classification created by the statutory amendments is arbitrary." As for the exception of financial institutions, Albertson's argues BIPA excludes essentially the entire financial industry. Albertson's asserts the use of the term "financial institution" in BIPA could exclude a number of entities ranging from retailers that happen to issue credit cards to car dealerships and mortgage brokers and, therefore, BIPA is unconstitutional.

Albertson's further asserts the BIPA exception for governments unconstitutionally "eliminates a wide swath of entities from the BIPA." Albertson's argues the exclusion for governmental entities is overly broad to the extent it exempts contractors, subcontractors and agents of state and local governments while they were working for the government. Consequently, the stated purpose of BIPA is not served with these exclusions.

Albertson's claims BIPA's impact, which excludes a potentially large number of entities from protecting the public's biometric data, "constitutes special legislation in violation of the Illinois Constitution. Albertson's argues it is entitled to have the action against it dismissed since "[a] general law could have been passed, and was in fact originally proposed to apply to both the government and financial institutions."

Regardless of whether the court finds BIPA unconstitutional, Albertson's still brings a valid point to light about the confusion BIPA causes for data collectors. For example, Albertson's poses a hypothetical where a janitorial company providing services to a government building would not have to comply with BIPA while another janitorial service providing services to a private building would incur the costs to comply with BIPA. It will be interesting to see how the trial court, and most likely the Illinois appellate court, addresses this question.

D. A Snapshot of Motions to Dismiss on BIPA Claims.

The latest decision related to Illinois' Biometric Information Protection Act ("BIPA") was issued by the Illinois Court of Appeals on June 16, 2020, in a matter entitled Cothron v. White Castle System, Inc, 2020 WL 3250706 (June 16, 2020). Latrina Cothron ("Cothron") began working at White Castle in 2004 and was still a manager at the time she filed suit. As a side note, the Cothron matter differs from many BIPA suits to the extent the plaintiff remains an employee before and after filing suit. Many BIPA cases involve claims by former employees that were terminated prior to bringing suit. As with most BIPA cases, Cothron claims White Castle violated BIPA when it installed a "fingerprint-based computer system that required Cothron, as a condition of continued employment, to scan and register her fingerprints in order 'to access the computer as a manager and access her paystubs as an hourly employee.'"

This decision provides a snapshot of where the courts are on this body of law. In short, the Court held Cothron had standing to bring this action and her Complaint had allegations that at least allow a portion of her BIPA claims to survive White Castle's motion to dismiss. It is important at this stage to

remember that the Court did not find that Cothron is entitled to damages. Rather, the Court merely held Cothron should be given the opportunity to demonstrate she was injured by White Castle's biometric information-gathering equipment.

The Court held Cothron could push forward with her claim on the following basis:

Cothron Did Not Have Standing To Bring A Claim Under Section 15(a) Of BIPA.

Section 15(a) *requires that a private entity "in possession of" biometric data (1) develop a written, publicly available policy that includes a retention schedule and destruction guidelines and (2) permanently destroy data upon the satisfaction of the "initial purpose for collecting or obtaining" it or "within 3 years" of the entity's last interaction with the person, whichever comes first.*

As for standing to bring this litigation, the Court first held that Cothron's Complaint did not have allegations to support a violation of Section 15(a) of BIPA. In particular, the Court opined that "the failure to make available a written retention and destruction policy was a harm to the public, not a harm particular to Ms. Cothron." Therefore, there was no violation under 15(a). The Court also found that Cothron could not allege a violation under 15(a) when she alleges that she continues to work at White Castle as a manager and, therefore, White Castle is not obligated to destroy her data. Therefore, the Court held Cothron lacked Article III standing to bring a claim under Section 15 (a) of BIPA.

Cothron Has Standing And Can Bring A Claim Under Section 15(b) and 15(d) Of BIPA.

Section 15(b) provides that, prior to collecting biometric data, entities must first (1) inform the person in writing that the information is being collected or stored; (2) state the "specific purpose and length of term for which" the data "is being collected, stored, and used"; and (3) receive a written release from the person.

As for standing to bring this litigation, the Court found Cothron had standing to bring this action under Section 15(b) of BIPA. Specifically, the Court opined that "Cothron's alleged Section 15(b) injury is concrete and particularized for the reasons summarized above: White Castle failed to provide her with

substantive, personal information about the collection, storage and use of her fingerprint data and armed with this information, Ms. Cothron may well have chosen to forgo the automated system." Therefore, the Court held Cothron had standing to bring a claim under Section 15(b) of BIPA.

Section 15(d) states that entities in possession of biometric data may only disclose or "otherwise disseminate" a person's data upon obtaining the person's consent or in limited other circumstances inapplicable here.

As for standing to bring this litigation, the Court held that "Section 15(d) forms a piece of the 'informed-consent regime' at the heart of BIPA." Under this reasoning, the Court held Cothron had standing to bring an action under 15(d) because her "informational injury" was concrete and particularized. The Court held Cothron should have been provided the right "to object to the way her data was being handled or to opt-out of the system entirely." Therefore, the Court held Cothron had standing to bring a claim under Section 15(d) of BIPA.

White Castle also argued that Cothron's Complaint should be dismissed because it did not contain any allegations that White Castle "acted with the mental state required for statutory damages." Here, the Court held "even absent specific allegations about White Castle's mental state," Cothron has stated a claim seeking litigation expenses and injunction relief under BIPA. That is, the Court did not require Cothron to specifically allege she is entitled to damages based on negligent, reckless or intentional conduct. Therefore, Cothron's Complaint survived White Castle's motion to dismiss based on the assertion that White Castle lacked the proper mental state for a viable BIPA violation.

White Castle also sought dismissal of Cothron's Complaint by arguing BIPA is preempted by the Illinois Workers' Compensation Act ("IWCA"). The IWCA provides the exclusive remedy for injuries sustained by employees in the course of their employment. Here, the Court opined the test to determine if an employee suffered a "compensable injury" is "whether there was a harmful change in the human organism—not just its bones and muscles, but its brain and nerves as well." The Court held the IWCA did not preempt BIPA claims to the extent it did not find BIPA violations caused physical or psychological injuries which would be typically covered under the IWCA.

It is important that data collectors do not get discouraged by these decisions when a court denies a motion to dismiss. As stated by the Cothron Court, "the question at this stage is simply whether the complaint includes factual allegations that state a plausible claim for relief." The analysis takes plaintiff's allegations as plead. For example, in this case, the parties will now start litigating issues that may involve statute of limitations, class certification and the technical aspects of whether a template of a small portion of a fingerprint/thumbprint constitutes biometric information.

5. Insurance Coverage For BIPA Claims

There are a number of questions whether a BIPA claim is covered under a commercial general liability insurance policy. For example,

Coverage B in a typical CGL policy will provide that an insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of "personal injury" and "advertising injury" to which this insurance applies." The term "personal injury" may be defined in relevant part as "[o]ral or written publication of material that violates a person's right of privacy." Even though a typical CGL Policy does not provide a definition for the term "publication", there is developing case law that provides instruction as to how to define the term.

The Illinois Appellate Court, First District, recently examined the definition of "publication" as it pertains to BIPA action coverage. In West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc., 2020 IL App (1st) 191834, the underlying BIPA class action alleged the defendant, tanning salon, required customers to scan their fingerprints and that the named plaintiff was never provided with, nor signed, a written release allowing disclosure of her fingerprint to any third party. Id. at ¶10. Notably, the underlying suit also alleged the tanning salon violated BIPA by disclosing her fingerprint data to an out-of-state third-party vendor without her consent. Id. at ¶11. The court primarily examined whether the policy's definition of "personal injury" encompassed the allegations in the underlying BIPA class action.

West Bend's policy defined "personal injury" to include claims arising out of "oral or written publication of material that violates a person's right of privacy." Id. at ¶27. The court noted the term "publication" was undefined under the policy. Id. at ¶28. Ultimately, the court reviewed the plain meaning of "publication" and found that it includes both the broad sharing of information to multiple recipients and a more limited sharing of information with a single third party. Id. at ¶35.

While the West Bend case provides some insight into the court's interpretation of the term "publication" in CGL policies, it is currently unpublished and therefore, its authority is questionable. In general, we anticipate insureds will argue the West Bend case stands for the proposition that BIPA claims trigger coverage under CGL policies. While Illinois courts may be called upon to address whether BIPA claims trigger coverage as a "personal injury," we do not need to address the reasoning found in West Bend. West Bend, as with many cases addressing insurance coverage for BIPA claims, focuses on what the insured did with the data. For example, the insured in West Bend allegedly "provide[ed] fingerprint data to a single third-party vendor…" which prompted the question of whether providing data to a single party is "publication."

Resources

Resources Specific to this Course

In addition, please see the resources cited within the material.

Resources for the Legal Professional

ABA Center for Professional Responsibility - www.abanet.org/cpr

Chicago Bar Association - www.chicagobar.org

Commission on Professionalism - www.2civility.org

Judicial Inquiry Board - http://www.illinois.gov/jib

Illinois Board of Admissions to the Bar - www.ilbaradmissions.org

Illinois Department of Financial and Professional Regulation - www.idfpr.com/default.asp

Illinois Lawyers' Assistance Program, Inc - www.illinoislap.org

Illinois State Bar Association - www.isba.org

Illinois Supreme Court - www.state.il.us/court

Lawyers Trust Fund of Illinois - www.ltf.org

MCLE Program - www.mcleboard.org