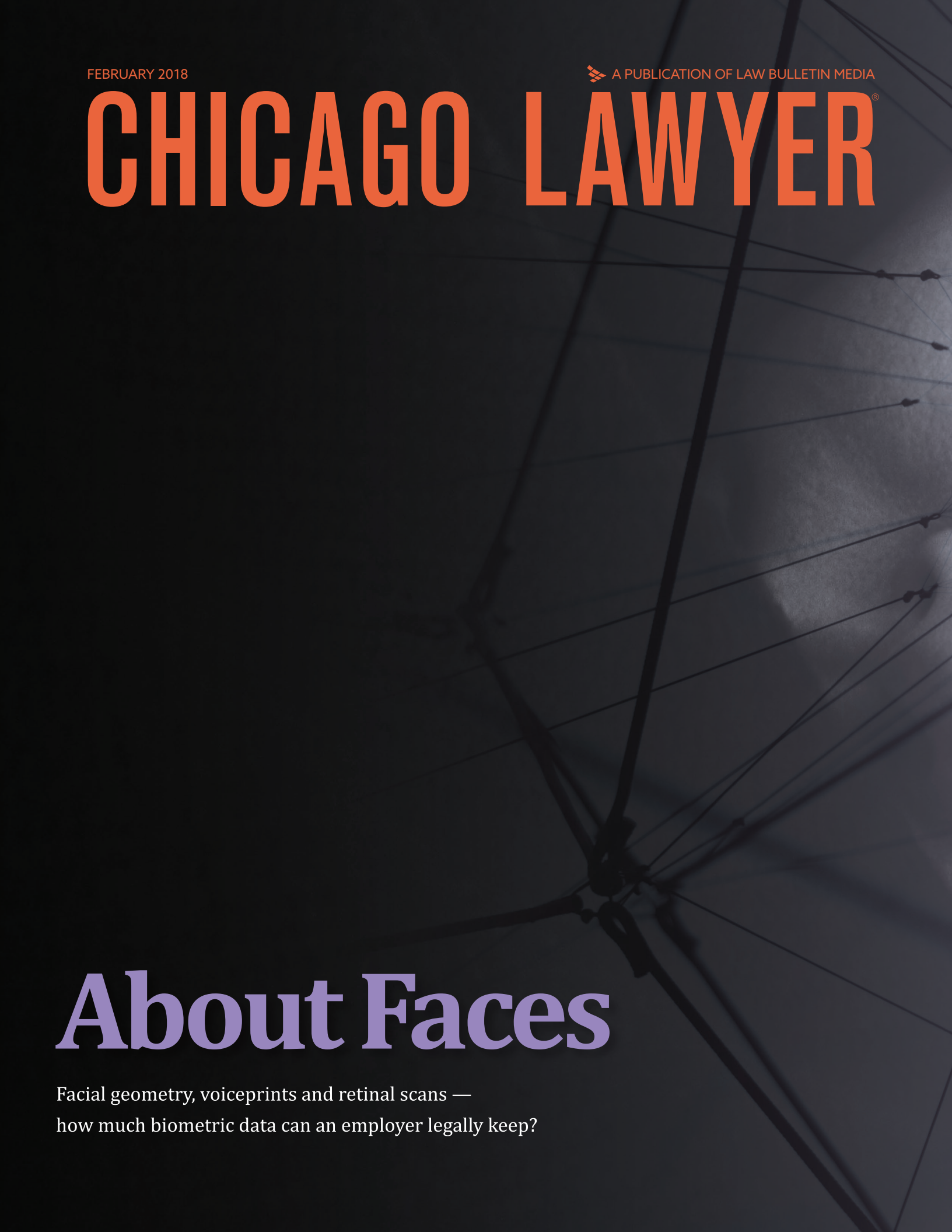
FEBRUARY 2018

A PUBLICATION OF LAW BULLETIN MEDIA

CHICAGO LAWYER®



About Faces

Facial geometry, voiceprints and retinal scans — how much biometric data can an employer legally keep?

By **Sarah Mansur**

If you want to see if your smile matches Mona Lisa's or if the biometrics say Ivan Albright drew your double, Google has an app for that — but not for you.

One of the hottest apps of the new year has been Google Arts & Culture, particularly a feature that scans users' selfies to find dopplegangers among famous works of art in museums around the world. Happy users have been flooding social media with the twins Google's facial recognition software found among Trumbulls and their biometric clones from Caravaggio.

But you can't have it. It's not available in Illinois.

Although Google has declined to comment on the reason Illinois and Texas can't access the app, those are two of the three states with biometrics laws restraining the amount of data that companies can collect about customers' and employees' bodies.

Google is fighting lawsuits in Illinois over its facial recognition technology, which provides the framework for the art-clone matching service. The basis for the pending litigation against Google is Illinois' Biometric Information Privacy Act — the first state or federal law to codify a person's ability to sue over biometric privacy rights.

The law, which became effective in October 2008, recognizes the rights of employees and consumers to extend privacy protections to biometric identifiers, such as a fingerprint, a voiceprint, a scan of the hand or face geometry. Since then, Chicago law firms have filed dozens of lawsuits for act violations in Cook County Circuit Court and federal district court in Illinois.

It's not just digital companies like Google, Facebook and the online photo service Shutterfly that are facing suits over Illinois' biometrics law. Mariano's supermarkets, Speedway gas stations, American Airlines — even Six Flags Great America — are facing or have faced suits over how they collect the ridges on our fingertips, the shapes of our faces or hands, the flutters of our voices and the hues of our eyeballs.

As the technology increases, as case law evolves and as people become inured to gas stations and amusement parks digitizing our faces, Chicago attorneys battling over these cases expect more disputes will come.

THE RETINAL TIME CLOCK

Illinois has become a national testing ground for these cases because it is the only state to grant an individual's private right of action for violations of the law. While Washington state and Texas have similar biometric privacy laws, civil cases there can only be filed by the state attorney general.

"[Illinois'] law came out of the fact that companies are increasingly collecting biometric information from both customers and employees. The cases are mostly coming up in context of employees, in particular for punching in and out of work," said Gary M. Miller a partner at Shook, Hardy & Bacon, who is representing defendants in BIPA cases.

BIPA regulates the way that biometrics are collected, stored and destroyed by any entity that possesses this information. It defines "biometric identifier" as a retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry. It defines "biometric information" as any information based on an individual's biometric identifier used to identify him or her.

Myles P. McGuire, whose firm McGuire Law represents plaintiffs in several BIPA lawsuits, said he thinks the law is sensible and progressive.

"I think it's a recognition about how permanent the injury can be if biometrics fall into the wrong hands," he said.

In the past, workers would check in and out by inserting a time card into a time clock, said McGuire.

"Today, it's something much different," he said.

Now, employees are asked to punch in and out of work by scanning their face, retina or finger. Basically, it's a biometric time clock.

The 2008 law requires that entities in possession of biometric information must develop a public, written policy establishing a schedule and guidelines for permanently destroying the information "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first."

It also mandates that these entities have written consent from a person before collecting and storing their biometric information, and that they store

biometric info as securely as other confidential information like Social Security numbers.

The law also allows anyone who is "aggrieved by a violation of this [a]ct" has a private right of action in a state circuit court or as a supplemental claim in federal district court.

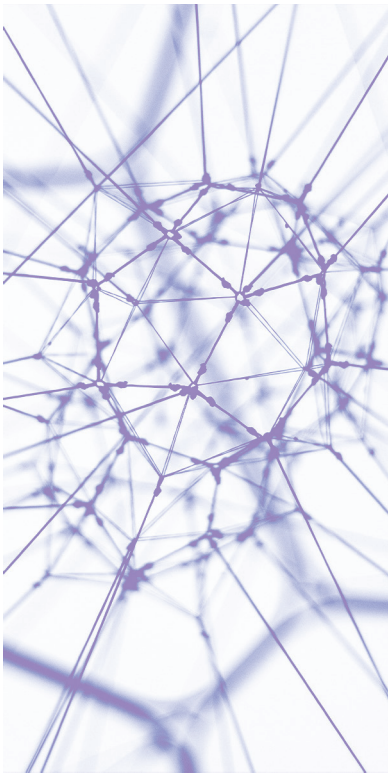
It provides damages of $1,000 for each negligent violation and $5,000 for each intentional or reckless violation.

Advocates of biometric privacy protections like attorney Adam D. Schwartz say that biometric information is especially deserving of protections because, among other reasons, a person's biometrics are permanent.

Unlike some of our confidential information, like credit card numbers, biometric information can't be changed if it is stolen, said Schwartz, an attorney for the Electronic Frontier Foundation, which lobbies for privacy rights over biometric data, among other issues.

"We think the rule should be, before anyone takes our biometrics from us, they have to get our permission and if we give them permission to use our biometrics for one thing, they only have consent to do that," Schwartz said.

TAGGING WITHOUT CONSENT



Last year alone, more than 30 BIPA complaints were filed in Cook County Circuit Court, with Intercontinental Hotels and Mariano's supermarket chain owner Roundy's becoming the latest defendants to face lawsuits.

Federal district court judges have already ruled favorably for some plaintiffs on motions to dismiss in several cases, including lawsuits against Google, Facebook and Shutterfly.

Three cases still pending in federal district court — *Alejandro Monroy v. Shutterfly Inc*., *In re: Facebook Biometric Privacy Litigation* and *Lindabeth Rivera and Joseph Weiss v. Google Inc*. — represent at least partial wins for biometric privacy advocates and plaintiffs bringing cases alleging violations of BIPA. In these cases, federal judges have denied defendants' motions to dismiss based on a failure to state a claim and demonstrate actual damages.

The *Shutterfly* complaint was filed in U.S. District Court for the Northern District of Illinois by Alejandro Monroy, who claimed that in September 2014, an unnamed Shutterfly user in Chicago uploaded a photograph of him onto the site. Users upload photos to the site to create and purchase prints, photo books and merchandise such as mugs, phone cases and T-shirts featuring their images.

According to the complaint, "Shutterfly automatically located [Monroy's] face, analyzed the geometric data relating to the unique contours of his face and the distances between his eyes, nose and ears, and used that data to extract and collect [Monroy's] scan of face geometry."

The complaint also states that Shutterfly then stored Monroy's biometric data in its database, and that based on the scan, it extracted and stored additional information regarding his gender, age, race and geographical location.

Monroy argues Shutterfly's collection and storage of his biometric data is a violation of BIPA, as he never consented to Shutterfly's extraction and storage of data representing his face geometry.

Among its arguments for dismissal, Shutterfly maintained that Monroy failed to allege that he suffered actual damages as a result of Shutterfly's conduct.

Northern District of Illinois Judge Joan B. Gottschall was not persuaded by Shutterfly's argument, and she declined "to hold that a showing of actual damages is necessary in order to state a claim under BIPA," in her opinion issued Sept. 15, 2017.

Shutterfly also claimed that the law does not apply to biometric data obtained from photographs, like the photo central to Monroy's lawsuit.

But Gottschall was also unconvinced by this argument, finding "the court sees nothing in BIPA's statutory text to indicate that it lacks application to data of the sort obtained by Shutterfly's facial-recognition technology."

This argument that BIPA excludes photos and any information derived from those photographs was also made by Facebook and Google in motions to dismiss pending litigation against them.

The case against Facebook, *In re: Facebook Biometric Privacy Litigation*, challenges the company's Tag Suggestions program, which allows Facebook users to identify other users and nonusers in photos uploaded to the site. The case was originally filed in the U.S. District Court for the Northern District of Illinois but has since moved to U.S. District Court for the Northern District of California.

While Facebook argued that its biometric data is derived exclusively from uploaded photographs and therefore it cannot be subject to BIPA, Judge James Donato disagreed.

On May 5, 2016, Donato denied Facebook's motion to dismiss on the basis that photos are excluded from BIPA.

"The [c]ourt accepts as true plaintiffs' allegations that Facebook's face recognition technology involves a scan of face geometry that was done without plaintiffs' consent. Consequently, they have stated a plausible claim for relief under BIPA," he wrote.

A similar argument was made by Google when Lindabeth Rivera and Joseph Weiss sued after photos of them were allegedly taken by a Google device in Illinois and automatically uploaded to Google Photos.

Rivera and Weiss claim Google scanned their facial features to create a unique face "template," and they maintain that Google violated BIPA by taking a scan of their facial geometry without consent.

Google asked the court to dismiss Rivera's and Weiss' complaints for failure to state a claim because the Privacy Act does not apply to photographs or information derived from photographs.

Like the judges in *Monroy* and *In re: Facebook*, Northern District of Illinois Judge Edmond E. Chang denied the motion to dismiss. His order was issued Feb. 27, 2017.

STOCKPILING FACES

Judges at the state and federal level have also issued decisions favorable to defendants in BIPA lawsuits.

One of these company-friendly decisions on motions to dismiss in federal court comes from *Adina McCollough v. Smarte Carte Inc*.

In *McCollough*, a federal district judge dismissed the case on the grounds that the court plaintiff did not satisfy the requirements of Article III standing and failed to state a claim.

Adina McCollough sued Smarte Carte after she used a locker operated by the company at Union Station in Chicago. Her complaint in U.S. District Court for the Northern District of Illinois alleges that Smarte Carte retained McCollough's biometric fingerprint information without written consent in violation of BIPA.

"We think the rule should be, before anyone takes our biometrics from us, they have to get our permission and if we give them permission to use our biometrics for one thing, they only have consent to do that."

Smarte Carte argued that the court lacked subject-matter jurisdiction over the complaint because McCollough failed to allege that she suffered any injury to satisfy Article III standing. The company also argued that McCollough lacked statutory standing to bring the claim because she is not an "aggrieved" individual within the meaning of BIPA.

Judge Sharon Johnson Coleman determined that McCollough did not face a "concrete" harm required for Article III standing.

"How can there be an injury from the lack of advance consent to retain the fingerprint data beyond the rental period if there is no allegation that the information was disclosed or at risk of disclosure? It was simply retained," Coleman stated in her decision issued Aug. 1, 2016.

Coleman found that McCollough "has alleged the sort of bare procedural violation that cannot satisfy Article III standing."

Coleman also agreed with Smarte Carte that McCollough lacked statutory standing.

"She is essentially claiming that the very fact of a technical violation is the adverse effect. Accordingly, this [c]ourt finds that McCollough also lacks statutory standing. Since a state statute cannot confer constitutional standing, even if McCollough is an aggrieved person under BIPA, she would not necessarily have Article III standing to maintain federal jurisdiction," Coleman wrote in her decision.

But biometric privacy advocates like Schwartz view BIPA violations as similar to eavesdropping or unauthorized surveillance, like a Peeping Tom.

"Those are invasions of privacy and a violation of common law tort of intrusion upon seclusion," he said. "Some have said 'If someone gathers your biometric [information] but doesn't do anything with it, then that's not invasion of privacy. It only becomes invasion of privacy if someone does something with it.' "

He said the Electronic Frontier Foundation disagrees.

"When a company is stockpiling people's faces without their permission, that *is* the injury," he said.

FIVE FINGERS, SIX FLAGS

The first opinion out of an Illinois Appellate Court was handed down late last year. Many lawyers representing defendants in BIPA cases view it as helpful to their cause.

The case, *Stacy Rosenbach v. Six Flags Entertainment Corp. and Great America LLC*, involves a biometric fingerprint-scanning and identification process for season-pass holders at Great America.

Rosenbach's juvenile son Alexander was fingerprinted and had his biometric data collected, recorded and stored as part of Six Flags' security process for entry into the Gurnee amusement park.

Rosenbach sued the park in January 2016, arguing it violated BIPA by taking her son's fingerprints without properly obtaining written consent or disclosing their plan for the collection, storage, use or destruction of his biometric identifiers or information.

Six Flags filed a motion to dismiss, claiming that a person who suffers no actual harm has not been "aggrieved" under the statute.

Lake County Circuit Judge Luis A. Berrones denied the motion to dismiss but later certified two questions relating to whether an "aggrieved" person under the law must allege some actual harm or whether a technical violation of the law is sufficient.

The 2nd District Appellate Court cited the *McCollough* decision and it concluded that if the Illinois legislature intended to allow for BIPA lawsuits based on every technical violation of the statute, it could have omitted the word "aggrieved."

"A determination that a technical violation of the statute is actionable would render the word 'aggrieved' superfluous," the Dec. 21, 2017, decision stated. "Therefore, a plaintiff who alleges only a technical violation of the statute without alleging some injury or adverse effect is not an aggrieved person under [S]ection 20 of the [a]ct."

McGuire said his firm disagrees with the ruling but doesn't think it will be problematic.

"I doubt it's going to be the last word on it but even if it was I don't think it's too challenging to comply with," he said.

McGuire said alleging an injury, in addition to a violation of the statute, isn't difficult because a breach of biometric data is permanent and vulnerable to extended and irreversible injury.

"Essentially, you might have a situation where someone has to have new fingerprints in order to use a different product because their old fingerprints were comprised somehow," he said.

But attorneys representing defendants, like Miller, think this decision will provide them with a much stronger argument for dismissal.

"This is likely to make a significant difference in pending BIPA cases, as

Rosenbach is the first and only Illinois Appellate Court decision to interpret BIPA, and the Illinois Supreme Court has not yet done so," Miller said. "Meanwhile, the majority of recent BIPA cases allege only technical non-compliance without an underlying injury, presumably with an eye toward clearing the motion to dismiss stage and obtaining an early settlement in the shadow of potentially expansive statutory liquidated damages."

It's not clear whether Rosenbach will file a petition for leave to appeal to the Illinois Supreme Court, which could affirm or vacate the appellate court's ruling. Phillip A. Bock of Bock, Hatch, Lewis & Oppenheim represented Rosenbach in the case. He did not respond to requests for comment.

SCANNING THE FUTURE

Miller said the issues of law that BIPA has raised are brand new and unresolved by the courts

"It's new ground. There are analogous cases or situations but no courts have ruled on these questions yet," he said. "The decisions in the Illinois courts on this will certainly affect decisions in other courts but maybe more important will be looked at by the legislative bodies in other states that are considering adopting similar statutes and how they word the statutes."

Some states have started to consider legislation in the realm of biometric privacy but Illinois remains a leader in this regard, said Schwartz.

"We hope other states will follow Illinois leadership and pass the same kind of laws," he said.

Questions about whether BIPA lawsuits in Illinois will continue, and whether other states will adopt a similar law are open to debate.

Jenny R. Goltz, an employment lawyer at Cozen O'Connor, said she can't imagine that biometric privacy will become a prominent issue in employment law once more labor employment lawyers become aware of the rules.

"I know that there has been a huge wave of these lawsuits and I think that's in part just because many employers were not aware of the law's requirements," she said. "There is such minimal cost to putting together that [written] policy [under BIPA]. It's not like the law requires them to completely change their timekeeping system."

Jay Edelson, whose firm Edelson has filed several BIPA lawsuits, agreed that complying with the provisions of BIPA is not costly or difficult.

"I would be surprised if companies continue to violate the law," said Edelson, who is representing the plaintiffs in *In re: Facebook Biometric Privacy Litigation*.

McGuire said companies often face a learning curve when new laws are enacted, and it may take time for them to ensure that they are complying.

"Eventually, companies will simply comply with the law rather than risk subsequent litigation," he said.

But Thomas E. Ahlering, an associate at Seyfarth Shaw, said he doesn't see the lawsuits over BIPA are going anywhere.

"As far as the field generally, I think that biometric privacy is very relevant and I think that there are other states that are drawing from Illinois and determining whether or not they want to put similar laws in place," he said. Seyfarth is representing several defendants in BIPA lawsuits.

He said the use of biometric information is an emerging technology that companies will want to use.

"I think the laws will continue to develop and there will be a lot more developments to come in the future," he said. CL

smansur@lawbulletinmedia.com