BIOMETRICS

Continued from Page 1

"It gets pretty massive, pretty quick and, of course, you also have the attorney fees," attorney Timm Schowalter said. "I've had cases go into the hundreds of millions of dollars, and they end up settling for relatively high amounts as well."

Schowalter is a Certified Information Privacy Professional/US and the chair of metropolitan area law firm Sandberg Phoenix's Cybersecurity and Risk Management Group. He has been making presentations on implications of Illinois' law, in light of new court cases.

Legislators were after a means of protecting individuals when they passed the measure, seeking to address how personally identifying information can be used. Key elements of the law deal with advance notice, consent, use of such information, and disposal of it after the fact.

Privacy laws also exist in the financial and health-care fields, Schowalter said.

Most employers get caught up in the notice and consent provisions, he said.

Schowalter addressed the issue this past month with members of Leadership Council of Southwestern Illinois, telling them "the plaintiffs' bar and employers in the state of Illinois are scared to death about where the statute is going to take them."

Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information, for example, Social Security numbers.

Biometrics are biologically unique to the individual. According to the law, identifiers include: retina scans, iris scans, fingerprints, palm prints, recognition of voice, facial geometry, DNA and gait.

Biometrics do not include such things as biological samples, handwriting, photographs, demographics, tattoos, physical descriptions or donated organs, among others.

The law applies to how the information is captured, converted, stored or shared.

In most recent legal cases, use of fingerprints and facial recognition have been the chief issues, Schowalter said. Fewer cases have dealt with gait or DNA recognition.

Schowalter said most of the cases with which he has been connected have involved companies using biometrics as part of their payroll and timeclock processes, such as those requiring a thumbprint. Software companies that use such a process claim that they are working with conversion algorithms and not actual prints, but that argument "isn't overly successful" in court, he said.

The BIPA law requires that any private entity in possession of biometric identifiers or information must create a written policy made available to the public; establish a retention schedule for that information; and have guidelines for permanently destroying biometric identifiers and biometric information. The policy must include that the data will be destroyed when the initial purpose of retaining the information has been satisfied OR within three years of the individual's last interaction with the private entity, whichever comes first.

A "private entity" is defined as an individual, a partnership, a corporation or a number of businesses and organizations, however grouped.

A company's policy must be adhered to unless there is a valid warrant or subpoena issued by a court.

No private entity can obtain biometric identifiers unless affected individuals have been informed in writing of the specific purpose and length of term the information would be collected and used; and those individuals have signed a written release.

No private entity can sell, lease, trade or otherwise profit on a person's or a customer's biometric information.

When a company violates BIPA, the aggrieved individual has a right of action against the company.

If an individual prevails, then for "each" violation:

- For negligence, the company will be assessed a $1,000 fine or actual damages, whichever is greater.
- The company is responsible for reasonable attorney fees and costs.
- The company is responsible for any other relief, such as an injunction.

That does not include local and state governmental agencies or the courts.

"Written consent" in the context of employment can be a release executed by an employee as a condition of employment.

In court actions, in terms of evidence, the law does not apply to information gained through X-ray, health settings (including employment-related COVID-19 screenings), certain financial institutions, private detectives and security services, and contractors working for government entities, among others.

Showalter said that, to date, federal and state courts have sided with plaintiffs in almost every legal action. In some cited cases, people did not have to prove actual injury to sue companies over alleged privacy invasions.

The business world didn't pay a lot of attention to Illinois' new law until 2019, when the Illinois Supreme Court went ignored precedent and ruled that the BIPA law is a strict liability statute, meaning victims do not have to show actual harm in order to sue over use of their information.

BIPA does not include a statute of limitations, but most federal and Illinois courts interpret the law as subject to a "catchall" five-year period.

That length of time could represent a lot of swipes of a timeclock, each a potential $1,000 penalty, Schowalter said.

Don't "kill the messenger," Schowalter said, during the recent presentation to Leadership Council. "I will tell you up front it's a very, very disturbing statute. It's causing a lot of companies economic harm."

Schowalter offers some best practices for companies:

- Contact a state representative or a lobbyist to address changes to the law.
- Contact an insurance broker to confirm or obtain coverage to cover BIPA claims.
- Review third-party vendor claims and seek indemnification language.
- Consider whether use of biometrics in your workplace is even necessary in the first place.
- If relying on biometric information, have your policies reviewed by counsel.
- Include BIPA policies, notice and consent in your onboarding process.
- Include policies in your handbook and manuals.
- Allow individuals to opt out of biometric information collection.
- Have security systems in place to prevent hacking of information.