ILLINOIS STATE BAR ASSOCIATION

FEBRUARY 2019 VOL 1 NO. 3

Privacy & Information Security Law

The newsletter of the Illinois State Bar Association's Privacy & Information Security Law Section

What does the Illinois Biometric Information Privacy Act require employers to do?

BY AMBROSE V. MCCALL

The Illinois state legislature passed the Biometric Information Privacy Act in 2008. The law covers private employers and specifically exempts local and state governmental employers from its scope.

The law, known as BIPA, covers and regulates employer use of biometric identifiers and biometric information of Illinois employees. Examples of BIPA covered employer interactions with employees' biometric identifiers include using retina or iris scans, fingerprints, voiceprints, or a scan of hand or face geometry for security scanning, time entry, and paying wages or salaries. When BIPA was passed, the use of biometric identifiers for security and financial transaction

Continued on next page

Take control: What every attorney should do to keep hackers at bay

BY RUTH E. SCHNEIDER

So often when we talk about cyber security and how to avoid being hacked, we think in terms of keeping client data secure within a corporation. Large and small businesses develop policies, hire IT experts, and purchase insurance in attempts to avoid being hacked and the subsequent loss of confidential, private information of their clients. In today's world, information security is no longer optional in an attorney's practice because our legal profession has not been immune from cyber attacks. In an industry where reputation is paramount, one report notes that around 40% of law firms were targeted for confidential client data in 2016-2017 but *did not know they were breached.* Further, top law firms are being hacked and data held for ransom in schemes costing millions. For instance, consider the recent DLA Piper data breach that left the firm without access to its own data. According to cyber security firm Mandiant, at least 80 of the 100 biggest firms in the country, by revenue, have been hacked since 2011.

Perhaps not every firm will be the subject of a multi-million dollar hacking heist, but the risks and consequences of failing to secure client data are every bit as

Continued on page 4

What does the Illinois Biometric Information Privacy Act require employers to do?

CONTINUED FROM PAGE 1

purposes was specifically described.

The signals for the potential broad construction of BIPA appear in its provision which states that the full range of potential consequences of using biometric technology "are not fully known." For example, when BIPA was passed, the legislators did not specifically anticipate the increasing use of biometric identifiers or biometric information by hourly employees to record when they start and end their work shifts.

Other concerns are also voiced in BIPA. For example, it declared that when a person's personal interests in their biometric identifiers was compromised, legal recourse was lacking even though such an event increased the risk of identity theft. In the absence of legal protections, a concern was that the public would avoid biometric related transactions unless their personal interests were addressed with regulations on the collection, use, safeguarding, retention, and destruction of biometric identifiers and information.

BIPA also covers "biometric information" which means any type of data from any source that is based on an individual's biometric identifier and that is used to identify an individual, subject to certain exclusions.

The law also references "confidential and sensitive information" which is personal data that can be used to uniquely identify individuals or their accounts or property. This means that under BIPA, confidential and sensitive information includes biometric identifiers such as fingerprints and other types of biometric data, and non-biometric data, including, but not limited to, genetic testing data and pass codes which are covered by other laws. Of significance to employers, BIPA defines a "written release" as meaning "informed consent, or, in the context of employment, a release executed by an employee as a condition of employment."

The statutory definitions matter because Illinois employers must have a public written policy that states a schedule for retaining biometric identifiers and biometric information and guidelines for destroying such data when the purposes for collecting such data have been satisfied or within 3 years of the employee's last interaction with the employer, whichever happens first. An employer is only excused from compliance with its retention policy and destruction guidelines by the issuance of a valid warrant or subpoena.

Illinois employers must take several steps before obtaining or transferring biometric identifiers or biometric information on their employees. First, an employer must inform an employee in writing that it is collecting or storing their biometric identifier and biometric information. The employer must also inform the employee of the applicable time span and specific purpose for collecting, storing, and using the employee's biometric identifier or biometric information. The employer must also receive a written release from the employee.

Illinois Employers may not sell, lease, trade or profit from an employee's biometric identifier or biometric information. In addition, they may not disclose or distribute the employee's biometric identifier or biometric information unless the employee consents or production of such data is required under state or federal law or a valid warrant or subpoena.

BIPA also requires Illinois employers to store, transmit, and protect from disclosure an employee's biometric identifiers and biometric information in a manner that meets two standards. The first standard is the reasonable standard of care within the employer's industry, and the second standard is what the employer uses for storing, transmitting, and protecting confidential and sensitive information.

What Potential Liabilities Does BIPA Impose on Illinois Employers?

BIPA gives every Illinois employee a right to sue a private employer who breaches its requirements. The employee must qualify as a person "aggrieved" by the employer's violation of the law. If qualified, the employee may file suit in an Illinois circuit court or add an action under BIPA as a supplemental

Privacy & Information Security Law

This is the newsletter of the ISBA's Privacy & Information Security Law Section. Section newsletters are free to section members and published at least four times per year. Section membership dues are $30 per year.

To subscribe, visit www.isba.org/sections or call 217-525-1760.

OFFICE
ILLINOIS BAR CENTER
424 S. SECOND STREET
SPRINGFIELD, IL 62701
PHONES: 217-525-1760 OR 800-252-8908
WWW.ISBA.ORG

EDITOR
David M. Adler

PUBLICATIONS MANAGER
Sara Anderson
sanderson@isba.org

claim in federal court.

An employee who wins a BIPA claim has a variety of possible remedies. If the private employer is shown to have negligently violated BIPA, the employee can recoup liquidated damages of $1,000 for each violation or actual damages, whichever is greater. For proven reckless or intentional violations, an employee can obtain liquidated damages of $5,000 for each violation or actual damages, whichever sum is more. In addition, a successful employee can recover attorneys' fees, costs, expert witness fees and other litigation expenses from an Illinois employer. Finally, an employee may obtain an injunction against the employer or other relief that a court finds appropriate.

Illinois private employers have little room to avoid compliance. In addition to excluding governmental employers, BIPA allows for a few specific exemptions. For example, an Illinois employer who can show that compliance with the X-Ray Retention Act or the federal Health Insurance Portability and Accountability Act of 1996 and their rules would conflict with BIPA may avoid liability. In addition, BIPA is not to be read as applying to a financial institution or its affiliate that is subject to Title V of the federal Gramm-Leach-Bailey Act of 1999 and its rules. Moreover, BIPA is not to be read as conflicting with requirements imposed by the Private Detective, Private Alarm, Private Security, Fingerprint Vendor and Locksmith Act of 2004 and its rules. In addition, BIPA does not apply to a contractor, subcontractor or agent of a State agency or local governmental unit when performing work on behalf of such governmental unit.

The many private Illinois employers who fall outside the referenced specific boundaries or limitations remain subject to the full scope of obligations and potential liabilities in BIPA.

How the Illinois Supreme Court Decides to Read BIPA Will Impact Illinois Employers

The Illinois Supreme Court recently heard oral arguments on an appeal of a ruling by the Second District of the Illinois Appellate Court that dismissed a claim as lacking the required pleading of an injury or negative effect beyond asserting a technical BIPA violation. In *Rosenbach,* the plaintiff mother purchased a season pass to an amusement park for her son. When he picked up the season pass, he was fingerprinted without any of the required BIPA disclosures or consents being provided or obtained. The BIPA suit did not allege an actual injury but asserted that the season pass purchase would not have occurred with foreknowledge of the BIPA violations. The *Rosenbach* court read the BIPA term "aggrieved" as requiring an injury in fact, even if non-pecuniary in nature, so as to establish more than a technical violation of the law. The court cited the Mortgage Act as a guide, where a cloud on title is considered a tangible harm. In the absence of a similar tangible harm, the Second District affirmed the dismissal of the complaint. The Illinois Supreme Court accepted an appeal and has held oral arguments. During those arguments, some comments by the Court indicate concerns over the fingerprinting of a minor and the legislative history that references persons made vulnerable by having their biometric identifiers or biometric information compromised. Until the Court rules, however, the extent and type of harm required to plead an action under BIPA remains in question.

In comparison, the first district of the appellate court ruled in *Sekura v. Krishna Schaumburg Tan, Inc.,* 2018 IL App (1st) 180175, ¶¶85-86, that alleged disclosure to an out-of state vendor and mental anguish each constitute a sufficient injury or adverse act to state a BIPA claim. Therefore, the Illinois Supreme Court will seek to resolve the differing interpretations.

While neither *Rosenbach* nor *Sekura* dealt with disputes between an employer and its employees, the disagreement appears in several actions filed in federal court. Like the pending Illinois Appellate Court analyses under review by the Illinois Supreme Court, the federal court rulings disagree over what qualifies an "aggrieved" party to proceed with a BIPA claim.

The sum effect is that all Illinois employers need to monitor and review their policy and consent procedures that they use for obtaining, storing, using, or transferring biometric identifiers and biometric information on their employees. In addition, Illinois employers will need to review with counsel their potential exposure under BIPA after the Illinois Supreme Court decides to read the term "aggrieved" so as to require an injury in fact or something less in order for an employee to proceed with a BIPA claim. Predicting the outcome of that ruling is difficult. What is reasonable to expect is that if the Illinois Supreme Court uses an English teacher sensibility when reading the term "aggrieved," the scope of BIPA may be defined within the traditional requirement of pleading an injury-in-fact. If, however, the Illinois Supreme Court relies on the legislative history behind BIPA that specifically references the lack of a remedy for acts that violate BIPA and that increase the risk of identity theft, then a broader reading of BIPA is likely in store for all Illinois employers. For now, the battle between the textual analysis and historical analysis is unresolved and supports Illinois employers that use and follow policies and procedures that comply with BIPA. ■

---

1. 740 ILCS 14/10.
2. *Id*.
3. 740 ILCS 14/5(f).
4. 740 ILCS 14/5(c)(d)(g).
5. 740 ILCS 14/10.
6. *Id*.
7. *Id*.
8. *Id*.
9. 740 ILCS 14/15(a).
10. *Id*.
11. 740 ILCS 14/15(b)(1).
12. 740 ILCS 14/15(b)(2).
13. 740 ILCS 14/15(b)(3).
14. 740 ILCS 14/15(c).
15. 740 ILCS 14/15(d)(1)-(4).
16. 740 ILCS 14/15(e).
17. 740 ILCS 14/20.
18. 740 ILCS 14/20(1).
19. 740 ILCS 14/20(2).
20. 740 ILCS 14/20(3).
21. 740 ILCS 14/20(4).
22. 740 ILCS 14/25(b).
23. 740 ILCS 14/25(c).
24. 740 ILCS 14/25(d).
25. 740 ILCS 14/25(e).
26. *Rosenbach v. Six Flags Entertainment Corp*., 2017 IL App (2d) 170317, ¶ 28, *leave to appeal granted*, 98 N.E.3d 36 (2018).
27. Compare *Dixon v. Washington & Jane Smith Cmty.-Beverly,* 2018 BL 191825, **15-16, 2018 WL 2445292 (N.D. Ill. May 31, 2018)(finding pled claim by employee of actual and concrete injury to right of privacy in and control over biometric data allegations meets "aggrieved" standard for pleading BIPA claim); with *Aguilar v. Rexnord LLC,* 2018 BL 236417, **3-4, 2018 WL 3239715 (N.D. Ill. July 3, 2018)(finding lack of standing due to absence of concrete harm where employee knew his biometric information was being collected to clock in and out without formal notice or consent and where no disclosure was alleged); *Goings v. UGN, Inc.*, 2018 BL 209897, 2018 WL 2966970 (N.D. Ill. June 13, 2018)(same analysis applied to collection of employee fingerprints and hand prints with remand order); *Howe v. Speedway LLC,* 2018 BL 191892, 2018 WL 2445541 (N.D. Ill. May 31, 2018)(granting motion to remand and discussing lack of injury-in-fact analysis).

Take control: What every attorney should do to keep hackers at bay

CONTINUED FROM PAGE 1

consequential to the reputation and future of the firm. Of note for attorneys, The American Bar Association and Missouri Bar Association[1] have recently added competency requirements for lawyers, including the "risks associated with relevant technology." Larger firms can and should consult security experts and form their own information security and privacy team, while smaller firms can outsource some of their security needs.

All the time, energy, and money spent by a firm to secure client data may be pointless if the individuals within the organization do not follow some basic steps. The problem remains that regardless of firm size, today's plethora of devices mean that hackers have many more potential access points to confidential data. Hence, responsibility to secure data must often rest with attorneys themselves. The necessity of using anti-virus and anti-malware protection as well as keeping your software up-to-date is a given. However, every attorney should take a number of additional basic measures to protect their data—and their business—from bad actors. Following are three steps that you should be taking to secure your personal devices and accounts.

1. Use long, unique passwords.

This idea has been around a long time and you have heard it before. It was good advice then and it is good advice now. Use long, unique passwords for your accounts. There is no easier way to open your door to hackers than making a password similar to "Password123!" or using the same password across multiple accounts. Some research shows that using longer, simple passwords, such as "checkhorsecarbatteriessunday" are more secure than shorter, complex passwords, such as "P@ssw0rd1". The important thing is that you use unique passwords across your accounts and devices.

Added Protection: Use a password manager

You likely have more than 10 online accounts, so how are you supposed to remember all of those passwords? Password managers such as LastPass or Dashlane store your login information across your devices and generate (then auto-save) long, random, unique passwords for each new account that you create. Then, you can securely autofill your login information and say goodbye to the "forgot password" button.

2. Use two-factor authentication.

Stolen identity can be a problem and a hacker may pose as you to gain access to your devices and accounts. As a result, you want a method to verify your identity before your device or account will accept the password. There are three categories of credentials that can be used to verify your identity: something you know (like a password or PIN), something you have (like your cell phone), or something you are (like your fingerprint). Two-factor authentication—sometimes referred to as multi-factor authentication—uses two or more of these categories to verify you before granting access. Typically, this is done through sending a text message with a short numerical code to your mobile phone, which you then type into the device to log in. This massively reduces the likelihood that your account can be hacked, and using it can even alert you to attempted attacks, i.e. if you receive a text message when you haven't attempted to log in.

Added Protection: Use a dedicated two-factor authentication device

While using two-factor authentication with your mobile phone is a big upgrade, mobile phones ultimately remain a device that can be hacked as well. Security firms make small, dedicated "security key" devices which can be attached to your keychain. When you log in, you "plug" the key into your device to complete your login. There are many security keys available on the market, but a popular make is the YubiKey. For the latest security, get a key meeting the FIDO U2F standard.

3. Send important documents securely.

In today's fast-paced world, the use of email to communicate and send documents allows us to be efficient and productive. For instance, it helps us make those last minute deadlines! Yet, email is also infamously unsecure. Sidestep this problem, particularly when sending documents outside of your firm's network, and use an encrypted file sharing service such as Citrix ShareFile that requires the recipient to have credentials to access documents. Pro tip: in most office programs, you can even password-protect individual documents. Just make sure that the sharing system provides end-to-end encryption.

Added Protection: Use an encrypted messenger

Like email, using our cell phones to send messages has become necessary for us to maximize our time and communication. It is also another way that a hacker may gain access to confidential information. Foil a potential hacker and send secure, encrypted messages on your phone using an encrypted messaging service. Apps such as Signal provide secure text messaging and even encrypted voice- and video-calls. They also have options for data to self-destruct a certain amount of time after the recipient has read your message—all without PIN codes or special login credentials.

These three easy, low cost steps are readily accessible to every attorney. For little to no cost, you can quickly implement these security measures, keep client information confidential, and avoid potentially large damages should a hacker attempt to access private client information on your devices. Following these steps will allow you to take control and keep hackers out of your devices and accounts. ■

Ruth E. Schneider, attorney at RCJ Law, LLC and executive director of RISE Law Institute, INC.

1. https://www.logicforce.com/reports/detail/cyber-security-q1.
2. http://fortune.com/2017/06/29/dla-piper-cyber-attack/.
3. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.
4. http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_house_action_compilation_redline_105a-f.authcheckdam.pdf.
5. https://www.courts.mo.gov/courts/ClerkHandbooksP2RulesOnly.nsf/c0c6ffa99df4993f86256ba50057dcb8/20fd60132de3411886256ca6005211b4.