Riding the BIPA wave

Three steps for employers to navigate risks posed by the Biometric Information Privacy Act[1]

A series of recent decisions by Illinois courts have brought varying degrees of clarity to litigation risk posed by the Biometric Information Privacy Act ("BIPA" or the "Act")[2]. The most recent came from the Illinois Supreme Court on January 25, 2019 when it commented on the definition of the word "aggrieved." To understand the implications of this decision and why the Illinois courts have great influence on this matter, a brief history of the Act is required.

BIPA – A brief history and description

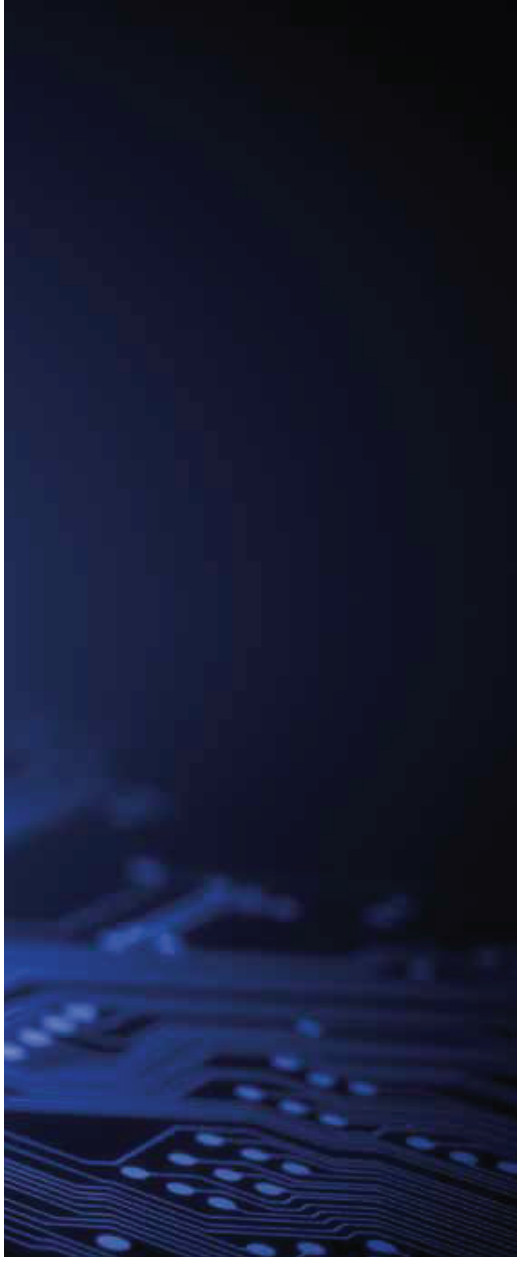
Illinois became the first state to regulate the collection, use and storage of an individual's "biometric information" by private entities with the enactment of its pioneering Biometric Information Privacy Act in 2008. "Biometric information" is defined in the Act to include retina or iris scans, fingerprints, voiceprints and facial recognition.

BIPA contains five key elements:

1) BIPA requires informed consent prior to collection;
2) BIPA prohibits a private company from selling or otherwise profiting from biometric data it collects or stores;
3) BIPA permits only a limited right to disclose biometric data;
4) BIPA requires a business to protect biometric data in the same manner it would other sensitive and confidential information in its possession; and
5) BIPA creates a private right of action for individuals harmed by violations of BIPA.

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

Since 2008, Texas and Washington have followed suit with similar statutes, albeit with marked variations. To date, these variations have insulated those statutes from the



> "This Illinois Supreme Court ruling has likely paved the way for a revival of BIPA litigation, including class action litigation"

onslaught of litigation that has ensued in the past few years under BIPA.

Despite its enactment in 2008, it was not until 2015 that there was an uptick in the number of BIPA (class-action) lawsuits. A number of these suits were brought by employees challenging employers' collection and use of biometric data for time-management purposes. However, defendants have challenged these lawsuits based on the failure to allege an actual injury (as opposed to a mere technical violation of the statute).

Recent decisions vary on need to prove actual injury

While courts have been split on this issue of demonstrating actual injury, there was some short-lived clarity in 2017 when the Illinois Appellate Court determined that BIPA requires "an actual injury, adverse effect, or harm..."[3] However, on May 30, 2018, the Illinois Supreme Court granted leave to appeal this 2017 decision, and recently swung the pendulum in the opposite direction with its January 25, 2019 decision.[4]

The Court noted that in the absence of a specific legislative definition of the word "aggrieved," the Court may rely on the definitions of aggrieved in collegiate and legal dictionaries. Relying on the commonly accepted meaning of the term "aggrieved," the Court held that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[5]

This Illinois Supreme Court ruling has likely paved the way for a revival of BIPA litigation, including class action litigation.

Steps for employers to address BIPA risks

Here are three actions employers should consider to assist with protecting themselves against the threat of litigation and exposure:

a) **Assess current risk.** Review current practices and policies regarding the collection, storage and destruction of biometric data subject to BIPA, particularly as it relates to Illinois-based employees. In addition, corporations should also evaluate exchanges of BIPA-covered biometric information between third parties. In both instances, generally, companies should use a three-year lookback period.

b) **Obtain informed consent and written policies.** If the assessment reveals risk, companies should develop a form of consent that provides: (i) information about the biometric information being collected, (ii) the purpose and the duration for which the biometric information will be collected and (iii) a written release which is executed by the impacted individual(s).

In addition, generally, BIPA requires that private entities develop written policies regarding the collection, storage and destruction of biometric information over a three-year period; generally, these policies must be made available to the public.

c) **Mitigate exposure.** In the event an employer is faced with a BIPA lawsuit, it is important to know what insurance coverage may be available, if any. In particular, companies should be familiar with the language in their Cyber Liability, Employment Practices Liability, Errors and Omissions and Commercial General Liability Policies. Corporations—in conjunction with (internal/external) counsel—should assess entity-specific risk(s) and determine appropriate coverage levels.

As legislatures, regulators and courts increasingly focus on company practices regarding the collection and use of information, including biometric information, it is important for employers to work with their insurance brokers and carriers to address the evolving risks.

Endnotes

[1] The subject matter and opinions expressed herein are the opinions of the individual author and may not reflect the opinions of QBE. The contents herein are for informational purposes only and not for the purpose of providing legal, regulatory, or compliance advice. The reader should contact his or her own attorney or compliance professional to obtain advice with respect to any particular issue or problem.

[2] 740 Ill. Comp. Stat. 14/1 (2017).

[3] *Rosenbach v. Six Flags Entertainment Corp.*, No. 2-17-0317, 2017 WL 6523910 (Ill. App. Ct. Dec. 21, 2017).

[4] *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186

[5] *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶ 40

Moire Morón, Esq.
Assistant Vice President,
Claims Practice Leader,
QBE North America