jackson lewis.

Illinois Biometric Information Privacy Act FAQs

Fingerprints, voice prints, and vein patterns in a person's palm are just three examples of the kinds of biometrics maintained about individuals. Of course, these technologies, aimed at increasing security and, to a lesser degree, convenience, raise concerns about and risks to data privacy and cybersecurity. However effective, convenient, and efficient these technologies may be, companies need to think through carefully their adoption and implementation, particularly in the workplace. Currently, one of the toughest laws in the U.S. concerning the protection of biometric data is the Illinois Biometric Information Privacy Act (BIPA), enacted in 2008. The following FAQs summarize the requirements under BIPA.

1. What is biometrics?

Biometrics is the measurement and statistical analysis of an individual's physical and behavioral characteristics. The technology associated with biometrics has many uses but frequently is used to verify personal identity. Examples of physiological characteristics include: DNA, fingerprints, face, hand, retina or ear features, and odor. Examples of behavioral characteristics include gestures, voice, typing rhythm, and gait.

2. How is biometrics used in business?

The use of biometrics in the business world has become widespread, and the types of usage are constantly evolving. With new technological developments and the technology itself becoming more readily available, industries of all sizes and kinds are discovering the benefits of biometrics. Common uses include:

- ***Time Management*** – Businesses across all industries have found that biometric time clocks – devices that facilitate clocking in and out with a fingerprint or other biometric, rather than an I.D. card or pin code – are cost effective, help eliminate time theft, and ensure more accurate compliance with attendance policies.
- ***Security Access*** – One of the original and most common forms of biometric use, typically through fingerprint readers, hand geometry scanners, and facial recognition, businesses use this technology to secure laptops, keyboard/mice, USB and portable storage devices, as well as for general physical

security (access to buildings and spaces within). Iris and retina scanners are more expensive, and generally justify use only in locations that require a high security clearance.

- ***Safety*** – As regulations and internal policies are added to increase employee safety, biometrics allows employers to complete a profile for each employee – a "one-stop shop" for keeping up-to-date with training, certification, use of company information, and for issuing credentials.
- ***Health Plans*** – Biometrics assists health plans in establishing effective wellness programs. Biometric screening of an enrolled population allows data to be aggregated, providing a complete risk profile for each individual. Some plans also measure biometric data of individuals to assess their health risks and provide incentives for changing behaviors that could lower those risks.

3. Does collecting biometric information subject my organization to violation of Illinois law requirements?

The Biometric Information Privacy Act, 740 ILCS 14 *et seq.* (BIPA), enacted in 2008, was one of the first state law to address business's collection of biometric data. The BIPA's comprehensive set of rules for companies collecting biometric data of state residents has five key features:

- Requires informed consent prior to collection
- Permits a limited right to disclosure
- Mandates protection obligations and retention guidelines
- Prohibits profiting from biometric data
- Creates a private right of action for individuals harmed by BIPA violations
- Provides statutory damages up to $1,000 for each negligent violation, and up to $5,000 for each intentional or reckless violation

The BIPA largely went unnoticed until 2015, when a series of five class action lawsuits of similar nature were brought against businesses alleging unlawful collection and use of the biometric data of Illinois residents. (*See – Pezen v. Facebook Inc.*, 1:15-cv-03484 (N.D. Ill. Apr. 21, 2015); *Licata v. Facebook Inc.*, 1:15-cv-04022 (N.D. Ill. May 5, 2015); *Patel v. Facebook Inc.*, 1:15-cv- 04265 (N.D. Ill. May 14, 2015); and *Gullen v. Facebook Inc.*, 1:15-cv-07861 (N.D. Ill. Aug. 31, 2015); *Norgberg v. Shutterfly, Inc.*, 1:15-cv-05351 (N.D. Ill. June 17, 2015)). These cases sparked a flood of similar customer-based class actions, as well as employee-based class actions claiming BIPA violations in connection with the deployment by employers of time-management biometric tools. For example, between July 2017 and November 2017 alone, more than 30 employment class actions based on BIPA were filed in Illinois state court.

One key issue in this line of both customer- and employee-based class actions has been whether an individual must allege actual injury or adverse effect, beyond a violation of his/her rights under BIPA, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages, attorneys' fees and costs, and injunctive relief under the Act. In January 2019, the Illinois Supreme Court handed down a significant decision in *Rosenbach v. Six Flags*, No. 123186 (Ill. 2019), holding that actual harm is not a requirement to establish standing to sue under BIPA.

The decision in *Rosenbach* is likely to increase the already significant number of suits, including putative class actions, filed under BIPA as it sets a low bar on plaintiffs' eligibility to sue. Now, any time an organization violates even a technical or procedural aspect of BIPA, even if no specific injury or adverse effect results, the individual whose biometric data was collected will have standing under the Act.

4. Do I have to safeguard biometric information?

Whether biometric technology is used in tracking employees' time-management, authenticating a transaction, creating a profile for a wellness program, or employing facial recognition for marketing purposes, biometric datasets often comprise sensitive personal identifiable information that must be protected. In the case of fingerprints, a biometric dataset can even be used to falsely incriminate the subject in a physical crime.

Under the BIPA, a business is obligated to protect and store biometric data at least to the same degree it protects other confidential or sensitive information.

5. What best practices should the company use if it maintains biometric information?

Confirm whether your company is really capturing biometric data as defined under Illinois law. Under the BIPA, "biometric information" is any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual, such as a fingerprint.

As the Illinois Supreme Court explained in *Rosenbach v. Six Flags,* No. 123186, (Ill. 2019):

> *[c]ompliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced.*

Given the Illinois Supreme Court's holding in *Rosenbach*, your organization should take immediate steps to comply with the statute.

Only collect the biometric information you need. This is a general collection principle for any type of personal information, not just biometric information. Biometric information of customers, clients, or employees should be collected and maintained for a lawful purpose directly related to your organization's functions and activities for which it was collected in the first place. The collection of biometric data should be necessary and not excessive for achieving this purpose. Due to the sensitivity of biometric data, if this lawful purpose can be achieved by collecting other data or less sensitive biometric data, then only that data should be collected.

Retention of biometric information should be for no longer than is needed. Similar to the consideration of the above "only collect the biometric information you need" principle, a good rule of thumb is: avoid keeping personal information for longer than is needed. The BIPA codifies this rule. Under the BIPA, biometric identifiers and biometric information must be permanently destroyed 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 entity collecting it, whichever occurs first. Remember to consider all areas where this information may be stored – third-party vendors, backup files, devices, and so on.

Establish a plan for accessing, storing, and safeguarding biometric information. Before collecting biometric data, companies generally must provide notice and obtain written consent from the individual. However, BIPA requires a "written release," which means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment. As with other personal data, if it is accessible to or stored by a third-party service provider, the company should obtain written assurances from that service provider concerning such things as minimum safeguards, record retention, and breach response.

Implement appropriate safeguards. This should include administrative, technical, and physical safeguards, such as:

- ***Administrative examples***: Assess risks and vulnerabilities, employee training, establish limits on who is authorized to access, collect, process, disclose, save, and destroy the data.
- ***Technical examples***: Store biometric information locally (on a mobile device or smart card), providing individuals with greater control over their biometric information and minimizing the likelihood of mass

data loss or a data breach, use biometric templates that summarize relevant information, as opposed to raw data, to minimize data stored, encrypt data, and develop a backup strategy.

- ***Physical examples***: Adopt a facility access plan, lock doors to data center storage rooms, and maintain an inventory of devices.

Moreover, given the holding in *Rosenbach*, if a BIPA compliance plan is already in place, your organization should review its time-management, point-of-purchase, physical-security, or other systems that obtain, use, or disclose biometric information against the requirements under the BIPA. In the event you find technical or procedural gaps in compliance (such as not providing written notice, obtaining a release from the subject of the biometric information, obtaining consent to provide biometric information to a third party, or maintaining a policy and guidelines for the retention and destruction of biometric information), you need to quickly remedy those gaps.

Prepare to handle a breach of biometric information. Illinois law requires notification of a breach of "personal information," including biometric information. Accordingly, companies should include biometric data as part of their written incident response plans. Of course, BIPA's definition of biometric information is not necessarily the same as under Illinois' breach notification law. The breach notification law protects:

> Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

6. Do I need a consent from an employee in order to collect, use, or disclose biometric information?

In Illinois, under BIPA, before the company may "collect, capture, purchase, receive through trade, or otherwise obtain" a biometric identifier or biometric information, it must:

i. Inform the individual or the individuals legally authorized representative in writing (I) that a biometric identifier or biometric information is being collected or stored and (II) of the specific purpose and length of term for which such identifier or information is being collected, stored, and used; and
ii. Receive a written release executed by such individual or representative.

In general, a "written release" means an informed written consent. However, in the context of employment, this means a release executed by an employee as a condition of employment. We can provide a sample form for this purpose, if needed, which would need to be customized based on your practices, including record retention.

7. Is a scan of a fingerprint or fingertip or some other geometric image or composite considered biometric information?

Under the BIPA, biometric information means any information, regardless of how it is captured, converted, stored, or shared based on an individual's biometric identifier used to identify an individual, such as a fingerprint. Subject to a number of exceptions, a biometric identifier means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

8. What kind of liability can I have for violating the rules on collecting or using biometric information?

The BIPA permits individuals to sue for violations and, if successful, they can recover liquidated damages of $1,000 or actual damages per violation, whichever is greater, along with attorneys' fees and expert witness fees. The liquidated damages amount increases to $5,000 if the violation is intentional or reckless. To date, no Illinois court has interpreted the meaning of "per violation," but the majority of BIPA suits have been brought as class actions seeking statutory damages on behalf of *each* individual affected.

9. What if I am not storing biometric information but a third-party is collecting or storing it on my behalf?

As with other personal data, if biometric data is accessible to or stored by third-party service providers, the company should obtain written assurances from its vendors concerning such things as minimum safeguards, record retention, and breach response.

For more information, please contact:

Joseph J. Lazzarotti, Esq., CIPP
Principal | Morristown, NJ
973-451-6363
Joseph.Lazzarotti@jacksonlewis.com

Nadine C. Abrahams
Principal | Chicago IL
312-803-2512
Nadine.Abrahams@jacksonlewis.com