Published on *The National Law Review* https://natlawreview.com

The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020

Article By:

Natalie A. Prescott

As more and more states seek to expand biometric privacy protection, plaintiffs begin to explore new claims under these legislative schemes. Companies, therefore, must proactively monitor their compliance with emerging privacy laws.

The plaintiffs' class action bar has shifted its focus to biometric privacy class actions. To minimize their risk, businesses must implement heightened awareness of the current and anticipated laws, be aware of the technical requirements, be vigilant with respect to compliance, and be aggressive in defending against litigation.

The number of biometric privacy class actions continues to skyrocket, with the decade-old Illinois Biometric Information Privacy Act (BIPA) continuing to pose the greatest threat to companies. While BIPA remains the only biometrics legislation that provides for a private right of action, five other states (Texas, Washington, California, New York, and Arkansas) have now passed their own biometric statutes or expanded existing laws to include biometric identifiers. These five states, however, either do not address the private right of action or expressly allow enforcement by the state attorneys general.

Illinois Remains the Leader in the Biometric Privacy Arena

The **Illinois Biometric Information Privacy Act (BIPA)** is the first and the oldest biometric regulation in the United States. Enacted in 2008, it regulates the collection and storage of biometric information. Biometric information includes a wide variety of identifiers such as retina scans, iris scans, fingerprints, palm prints, voice recognition, facial-geometry recognition, DNA recognition, gait recognition, and even scent recognition.

Although biometric laws broadly apply to all industries and regulate private entities and individuals, compliance issues most frequently arise in the HR and employment context. Many U.S. employers have recently begun to utilize the employees' biometric information to monitor when their workers clock in and out, or to restrict access to secure areas, to provide system login and regulate online access to sensitive data, and even to monitor productivity tracking and ergonomic tracking. While convenient, highly accurate, and efficient, use of biometric technology at work brings about a slew of legal and regulatory-compliance issues.

Let's for example, take BIPA—an undisputed leader in the field of biometric privacy class actions. Under BIPA, private entities that utilize biometric information must have a written policy, schedule, and guidelines its collection, retention, and destruction. BIPA also requires advance disclosure and a written release from the subject or employee whose information is going to be collected. It also severely restricts the entity's right to disseminate biometric information. And, most importantly, unlike many other privacy laws, BIPA provides for a private right of action. Indeed, the seminal 2019 decision from the Illinois Supreme Court, Rosenbach v. Six Flags Entertainment expressly held that a person does not need to suffer actual or concrete harm in order to have a standing to sue under BIPA—the mere violation of the Act is enough.

Penalties for Violating Biometric Privacy Laws Remain Steep

BIPA has a strong bite: It imposes a $1,000 penalty for each negligent violation, or a $5,000 penalty for each willful or reckless violation. It also provides for injunctive relief and actual damages, of actual damages exceed the prescribed penalties. Additionally, BIPA allows for the recovery of attorney fees and litigation expenses—a great incentive for the plaintiffs' attorneys to take BIPA cases on contingency. Given the steep penalties and the private right of action, the potential exposure for companies sued for BIPA violations can quickly skyrocket.

Over 200 BIPA lawsuits reportedly have been filed in 2018-2019 alone. Most of these cases are class actions, and most target employers that utilize biometric technology at work. These lawsuits are on the rise and expensive and difficult to defend against. In California, Facebook continues to defend a putative class action lawsuit alleging that the company violated BIPA when it unlawfully used its facial recognition software on photos that users upload to the site. Facebook recently lost its appeal in the 9th Circuit on the certification issue. Facebook is reportedly facing billions in damages.

Other States Finally Follow Suit

Texas:

Unlike Illinois, other states do not yet have comprehensive biometric regulations. In 2009, Texas passed its own biometric privacy act, Tex. Bus. & Com. Code §503.001. It provides that a "person may not capture a biometric identifier" without a prior consent, may not sell biometric date without consent or unless allowed by law, must use reasonable care in storing it, and "shall destroy the biometric identifier within a reasonable time." Although it imposes a steep civil penalty of "$25,000 for each violation," there is no private right of action, unlike with BIPA. Rather, the state attorney general has the enforcement rights.

Washington:

Washington enacted biometric privacy legislation more recently, in 2017. This law, Wash. Rev. Code Ann. §19.375.020, prohibits any company or individual from entering biometric data "in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose." Like Texas, it does not provide for a private right of action but authorizes enforcement by the attorney general.

California:

California's now-widely known California Consumer Privacy Act (CCPA), which will go into effect in 2020, also regulates biometric data by including it in the definition of personal information. CCPA

defines biometric data very broadly to include “physiological, biological or behavioral characteristics, including … DNA[,] that can be used … to establish individual identity,” including “imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.”

New York:

New York amended its existing data-breach notification laws with its 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act, going into effect in early 2020. The SHIELD Act broadens the definition of private information to include biometric information. It defines biometric information to include fingerprints, voiceprints, retina or iris images, or other unique physical characteristics. Interestingly, it also includes other forms of unique digital representation of biometric data used for authentication purposes. Earlier, New York had also passed a limited biometric legislation, N.Y. Lab. Law §201-a, which applies specifically in the employment context. It prohibits fingerprinting “as a condition of securing employment or of continuing employment.” It does not expressly provide for a private right of action.

Arkansas:

Several months ago, Arkansas became the latest state to pass biometric-data legislation. Specifically, Arkansas amended its breach-response laws, Arkansas Code §4-110-103(7), by revising the definition of covered personal information to now also include biometric data. It defined biometric data to include an individual’s “Fingerprints; Faceprint; A retinal or iris scan; Hand geometry; Voiceprint analysis; Deoxyribonucleic acid (DNA); or Any other unique biological characteristics.”

Other States:

In recent years, many other states have introduced biometric legislation. Although these laws have not yet been enacted, there is a notable trend towards state regulation of biometric data.

Takeaways

To protect your company against allegations and lawsuits involving biometric laws, implement the following steps:

- Consider whether use of biometric technology is necessary and appropriate for your business.
- If relying on biometric technology, provide advance notice to the individuals and obtain consent.
- Ensure that the notice adequately discloses why you collect, how you use, how you store, and how you disclose biometric data.
- Include notice of biometric policies in “terms and conditions” and in the privacy policy.
- Obtain written informed consent from each individual, when appropriate.

- Allow individuals to opt out of biometric information collection.
- Stay abreast of the latest legal developments in this area and work with your outside counsel on implementing and updating relevant policies and procedures.

Conclusion

Privacy advocates are demanding stronger biometric privacy protection across the country, while businesses and the tech industry view biometric laws as an unnecessary deterrent at the time of innovation and the increasing need to rely on biometric data to authenticate customers and employees. As more and more states pass comprehensive privacy laws, companies that collect and use biometric data or plan to do so need to pay close attention to creating policies and procedures, implementing appropriate security measures, and being aware of the notice and consent requirements various laws impose.

National Law Review, Volumess X, Number 15