BIOMETRIC PRIVACY LAWS

What They Are & Why You Should Care

AHT INSURANCE
A BALDWIN RISK PARTNER

When it comes to data and privacy laws, the regulatory landscape is complex and in a state of continuous flux. As lawmakers and government officials attempt to catch up and keep up with a constantly evolving, multifaceted digital world, it's up to companies to stay informed regarding these regulatory changes so that they're able to remain compliant with the law and maintain standards that protect sensitive data from malicious actors.

Although it's not a new regulation, the Biometric Information Privacy Act (BIPA) enacted in the state of Illinois in 2008 has become a new pressing issue for organizations as enforcement of BIPA increases. **BIPA requires companies that do business in Illinois to comply with certain requirements pertaining to the collection, handling, and use of biometric identifiers and information by private entities.**

> The act prescribes a fine of $1,000 per inadvertent violation and $5,000 per intentional or reckless violation. Workers and consumers have up to five years to sue for violations of BIPA.

THESE REQUIREMENTS INCLUDE:

- **Advanced Consent** - Consent must be obtained from individuals if the company intends to collect or disclose personal biometric identifiers.
- **Timely Destruction** - If an employee leaves or is terminated, the employer must destroy their biometric identifiers in a timely manner.
- **Secure Storage** - Companies must securely store biometric identifiers.

WHAT ARE BIOMETRICS?

Biometrics are unique, intrinsic human characteristics that can be used to digitally identify a person to grant them access to devices, data, or systems. A common example is using your fingerprint or facial recognition to unlock your cellphone. Biometrics fall into two main categories: physical identifiers and behavioral identifiers.

PHYSICAL IDENTIFIERS INCLUDE:

- Fingerprints
- Facial patterns
- Iris/Retina
- DNA
- Veins

BEHAVIORAL IDENTIFIERS INCLUDE:

- Voice
- Typing cadence
- Signatures
- Gait

Following in the footsteps of Illinois, lawmakers in other states have introduced or enacted similar bills to regulate private entities' handling and processing of biometric information. This is likely an indicator that BIPA is just the start of an overarching trend that's changing the landscape of U.S. state privacy laws. At the federal level, a number of iterations of privacy bills have also been introduced, although none have passed.

LAWSUITS & LIABILITY

Beyond the regulatory enforcement, recently there has been an uptick in biometric privacy class action lawsuits filed against various companies, including McDonald's, Walmart, Amazon, White Castle, and more. And the price of settlements in these lawsuits is hefty, routinely reaching eight and nine-figure sums. Take for example the following cases:

- **TikTok** – A federal judge granted approval for a $92 million settlement between TikTok and class members. Claimants alleged that TikTok collected billions of biometric identifiers from users and disclosed it to third parties without user consent.

- **Facebook**– Facebook users sued Facebook over the social media giant's use of facial recognition technology in the photo-tagging tool, alleging that Facebook failed to comply with BIPA. A Federal judge approved a $650 million settlement for the 1.6 million involved class members.

- **BNSF** – In the first jury verdict on the issue, a federal jury awarded a $228 million verdict to plaintiffs in a class action lawsuit who filed against BNSF Railway Co. under BIPA.

An uptick of biometric privacy class action lawsuits means that this is a significant, emerging liability for businesses that use biometrics in any way. And insurance carriers are paying attention, with some carriers introducing exclusionary language in policies pertaining to biometric claims. As the regulatory and insurance spaces continue to evolve regarding biometric data, partnering with a team of experienced cyber liability experts can help your organization stay abreast of these changes, protect sensitive data, and remain compliant.

WHAT DO THESE DEVELOPMENTS MEAN FOR ORGANIZATIONS THAT CONDUCT BUSINESS IN THESE STATES?

Even if your company doesn't do business in states with biometric privacy laws, if you collect biometric identifiers from customers, employees, and other stakeholders, the wisest course of action is to be prepared and preemptively implement guidelines within your organization that adhere to best practices regarding the collection, handling, and storage of this data.

Biometric identifiers are particularly sensitive pieces of data because, unlike passwords or credit card numbers, it's not information that an affected individual can change in response to a breach – biometrics are intrinsic characteristics of people. If an organization is found to be at fault for the theft and unauthorized use of employees', customers', and/or other stakeholders' personal identifiers, it can lead to serious consequences in the form of monetary losses and reputational harm.

Learn more about what you can do to address biometric data risk. Connect with one of our Cyber experts to help protect your organization from this complex liability.