THE SAFE STEP

Your connection to protecting those who improve your community

YOUR RESPONSIBILITY TO KEEP BIOMETRIC INFORMATION SAFE

ILLINOIS' Biometric Information Privacy Act (BIPA) (740 ILCS 14/1)

The Problem

Society continues to witness significant advances in technology, enabling businesses to offer better products, services, efficiencies and security. We are collecting more personal and biometric information at a faster rate than ever before. Ever wonder why you see advertisements on your phone related to a recent conversation or search? The result is that privacy isn't so private anymore. While technological advancements intend to deliver a noble reward, collecting and using personal information significantly raises the risk profile for all entities regardless of size and industry class.

More and more businesses are using technology to collect biometric information to better understand and serve customers and employees. Biometric information presents a unique privacy exposure in that a biometric record is permanent and cannot be changed. For example, John Doe's fingerprint is immutable – a fingerprint can never be changed. However, John Doe's credit card number is easily changed when a new card is issued. Due to its permanency, biometric information is quite effective in identifying individuals based on physical characteristics, but this permanency raises the risk profile given biometric information cannot be changed if stolen or compromised.

ENTER BIPA - Illinois

Illinois passed the first biometric information privacy law in 2008, known as the Illinois Biometric Information Privacy Act (BIPA). Two additional states, Texas and Washington, subsequently passed privacy statutes directly related to the collection and use of biometric information. In Illinois, BIPA mandates specific processes be in place in order to collect and use biometric information. For example, BIPA Section 15 (b) (1) states biometric identifiers or information can be collected only if the private entity informs the subject in advance and in writing biometric information is being collected and stored. Generally speaking, biometric identifiers or biometric information can be defined under BIPA as fingerprints, facial recognition, voiceprint, retinal scan and hand scan. BIPA allows for a private right of action against an offending party that negligently violates any provision of the Act for a recovery of actual damages or liquidated $1,000 per each violation, which-ever is greater, and up to $5,000 or actual damages for a willful violation. This has led to many class action lawsuits alleging mere technical violations of the statute and requesting the liquidated damages set by statute without the need to prove any concrete harm has been sustained.

State Privacy Statutes

All 50 states have enacted some form of data breach laws governing the protection of personal information. What constitutes Personal Information and whether it includes biometric information is normally defined by each state's statute, so businesses need to understand each state's law to comply. Further, anticipate states may pass new laws or broaden current laws to include biometric information within the definition of personal information. Further, anticipate that even definitions of biometric information may vary from state to state. In addition, more states are considering and passing privacy laws, which include biometric information as part of the definition of personal information.

The Solution

Analyze the information you collect and make sure it is protected.

Suggested To DO

- Understand the IL privacy statute and how it applies to your business.
- Engage or consult with competent counsel or personnel to ensure compliance with BIPA.
- Provide all employees/customers with written notice that is compliant with BIPA regulatory requirements.
- Obtain signed releases/consent from all affected employees.
- Confirm that no biometric data is sold or disclosed to third parties for any reason other than permitted by BIPA regulatory requirements.
- Ensure that you, and/or any third parties with access to biometric data have adequate data security in place.
- Ensure that you have a security incident response plan that recognizes biometric data in data breach notification requirements.
- Train your employees on applicable policies and procedures.
- Consider mandatory arbitration agreements with class action waivers.

DON'T

- Ignore this alert.
- Increase the risk of loss by doing nothing.
- Fail to take action.

Illinois BIPA

Does BIPA apply to my business? Please visit the Illinois General Assembly website for more information: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 and consult with your legal counsel.

Great American Can Help!

Check out our all-new Risk Portal for information such as this and other resources that can help you manage your risks: https://gaig-shs.riskresourcesportal.org/