FindBiometrics Presents:

THE BIPA CHECKLIST

These Seven Questions Can Save You From a Biometrics Lawsuit

Illinois' Biometric Information Privacy Act (BIPA) is the strictest biometrics legislation in the world, and carries with it some incredibly heavy penalties. And while high-profile class action lawsuits under the legislation have seen the likes of social media giants Meta and TikTok paying out $90 million-plus settlements, the real effects hit much closer to home. Of the approximately 1,000 BIPA-related lawsuits, most deal with everyday workplace use cases like time tracking, employee verification, and even temperature scanning. What's more, the controversial act is serving as the model for other privacy regulations, including proposed US federal legislation.

With the threat of BIPA fines, it's easy to understand why some potential biometrics customers are thinking twice about the powerful identity technology. But in our rapidly digitizing world, biometrics remain the best technologies to anchor trusted identity, eliminate fraud, secure physical spaces, and enable frictionless customer experiences in retail, government services, banking, healthcare, and other integral markets. Positioned at the intersection of our converging physical and virtual worlds, biometrics have the potential to enhance workplace efficiency and security, while actually enhancing user privacy and building the highest possible levels of trust in our digitally transforming society.

So don't give up on biometrics. While BIPA has sharp teeth and the ability to punish the unprepared, starting on the road to compliance is as easy as asking yourself seven key questions about transparency, consent, and communication. If you are considering biometrics for your business—in or outside of Illinois—be sure to run through this checklist and make sure you're on the right side of the law.

1. Why Am I Collecting Biometrics?

BIPA compliance is built around transparency and informed consent. You must be able to articulate why you are using biometrics and communicate that to every user of your system. If you have a biometric punch clock, for instance, you are collecting biometric data to efficiently and securely track workforce attendance. Or if you have a biometric medical safe, you are collecting biometrics to authenticate authorized personnel when they are accessing restricted substances. Biometric data has many applications, but you need to be purposeful in your intent and use.

Being able to link a person's physical body to their biographical or contextual identity data (name, address, age, purchasing history, medical records, etc.) is not something that should be taken lightly. As much as we love to boost biometrics, sometimes their collection is simply not necessary. If you cannot articulate the specific reason for using biometrics, then save yourself the risk.

2. How Long Will I Need to Keep Biometric Data?

In addition to giving notice of your purpose for using biometrics, BIPA requires disclosure of how long any biometric data will be kept. You cannot retain biometric data for more than three years under BIPA, and the best practice is to only keep it as long as is necessary for your stated purpose. Some biometrics—like temperature scans or anonymous age checks—don't need to be stored at all, while other biometrics might be conditional on a user's continued employment and can be deleted when their contract is up. The first step to ensuring you follow best data retention practices is to clearly define said practices for you and your users, then follow them strictly.

3. Am I Willing to Ask Permission to Collect Each Biometric Scan?

BIPA's harsh penalties can largely be attributed to one specific aspect: each individual biometric scan—from enrollment through the user's last sensor interaction—can potentially be treated as its own infraction. This means that not only must you gain informed consent to enroll a user in your system, you must get them to re-consent before every subsequent use. Essentially: if a user agreed to be onboarded for your biometric time clock or medical safe, their continued consent cannot simply be assumed for every subsequent additional scan.

Given that BIPA currently carries a statute of limitations of five years, each individual scan retroactive for that entire time period can carry a $5,000 fine if it's a knowing infraction, and $1,000 for each negligent infraction. The math is staggering. Using the example of a time clock, an employee suing their employer under BIPA can potentially claim infractions for every attendance record interaction. If a full-time employee clocks in and out for lunch, a morning and afternoon break, and at the beginning and end of their shift, that means each work day carries a potential $40,000 fine. With such devastating consequences, it is crucial to ask permission for every biometric interaction.

4. How Am I Communicating to My Employees and Customers?

Transparency and consent requires clear and constant communication. The answers to the first three questions are not just for you: you need to communicate them to the people using your biometric technology at every touchpoint. What biometrics are you collecting, when are you collecting them, and why? How long will you store biometrics and for what purpose? For some uses of biometrics, like one-time background checks, that information can be conveyed by an employee or with an easy-to-understand opt-in form. For long-term use cases that require multiple biometric scans, a well placed sign can do the trick without adding friction to the process, keeping in mind that it is crucial to obtain written permission to collect and store biometrics from each user before their first scan.

5. Am I Being Fully Transparent in My Collection, Retention, and Use of Biometric Data?

You might be tired of reading the T-word by now, but it's important. BIPA compliance requires full transparency. If you don't have the avenue to inform a user how, why, and for how long you are collecting their biometrics, or if you worry that transparency might cause a user to withdraw consent, then you should revisit the first question on this list before proceeding. It bears repeating: biometrics are a powerful technology, and while BIPA may seem overly stringent, it is ideally in place to protect users from abuse, exploitation, and negligence, with transparency being key to achieving that goal.

6. What is My Data Hygiene Plan?

A well thought out plan can save you from a lawsuit. Thanks to BIPA's data retention aspects, it is incumbent on organizations using biometric technology to have a reliable records keeping system that includes an end-of-life plan for biometric data in line with their stated purpose for collection. The last thing you want is to get sued over forgetting to clean your records. Once you know why, how and for how long you need to keep a user's biometrics, make sure you set up a routine to purge any expired data.

7. Do I Have Any Questions About BIPA or Other Data Privacy Laws?

BIPA is only one of many data privacy laws dealing with identity and biometrics, and it is being used as a model for more regulations in the US and abroad. The best way to make sure you are using biometrics in a privacy-respecting, legal manner is to contact a legal expert. Don't just assume that a common everyday use case or your own good intentions can shield you from BIPA and the emerging legislation it's inspiring.

See it as a final test of transparency and consent to see if biometrics are right for you: if you are willing to seek legal advice on ensuring that you're using strong identity technologies legally and in good faith, then you're ready for the benefits of biometrics without being at risk of getting bitten by BIPA.

About FindBiometrics and Mobile ID World

FindBiometrics and Mobile ID World are your leading industry resources for all information on biometric identification and identity verification systems and solutions. We have the latest daily news from the global biometric and identity management business community, a comprehensive vendor list, informative articles, interviews with industry leaders, exclusive videos, links to biometric associations and a calendar for the most important and current industry events and conferences, including our lauded webinar series and virtual Identity Summit events. FindBiometrics is also a proud member and longtime supporter of the International Biometric and Identification Association (IBIA).

FindBiometrics and Mobile ID World are part of the ChannelPro Network, a division of EH Media LLC, a leading U.S. business-to-business media company and conference producer.

This resource is being provided as a starting point to understanding the best practices regarding biometric data collection and user privacy. It does not constitute actual legal advice. Before deploying any biometric technology it is wise to seek professional legal counsel regarding local, national, and international privacy laws.