

BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

WHAT IS BIPA?

The Illinois legislature unanimously passed the Biometric Information Privacy Act (“BIPA”) in 2008, an initiative led by the ACLU of Illinois. The law ensures that individuals are in control of their own biometric data and prohibits private companies from collecting it unless they:

- ✓ Inform the person in writing of what data is being collected or stored
(e.g. fingerprint is stored when using TouchID to log into bank account app on phone)
- ✓ Inform the person in writing of the specific purpose and length of time the for which the data will be collected, stored and used
(e.g. fingerprint is stored for ease of logging into app and only for a duration of six months)
- ✓ Obtain the person’s written consent
(e.g. user signs their name before sharing their fingerprint)

WHAT DOES BIPA DO?

BIPA establishes standards for how companies must handle Illinois consumers’ biometric information. In addition to its notice and consent requirement, the law prohibits any company from selling or otherwise profiting from consumers’ biometric information. BIPA continues to stand as the most protective biometric privacy law in the nation, with the only one of its kind to offer consumers protection by allowing them to take a company who violates the law to court.

Types of biometric information

- Retina or iris scans
- Fingerprints
- Voiceprints
- Hand scans
- Facial geometry
- DNA
- Other unique biological information

WHY DO WE NEED BIPA?

A person’s biometric information belongs to them, and only them. This information should never be left to corporate interests who want to collect data and use it for commercial purposes. BIPA is currently the one legislation that makes it unlawful for private companies to use facial recognition technology to identify and track people without their consent. This technology has proven to be both inaccurate and harmful, making it prone to discriminatory effects, especially on women and people of color. Yet, more than a decade after BIPA’s enactment, we constantly hear new examples about companies seeking to collect, share, and misuse personal information of millions of people, without their knowledge or consent. At this critical moment, it is important for state decision makers to continue protecting BIPA under mounting attacks.

Unlike a phone number, email address, or other password, biometric information can never be changed! That is why we continue to rely upon BIPA to protect our most sensitive information.

HOW IS BIPA UNDER ATTACK?

Even though BIPA is widely regarded as being “America’s strongest biometric privacy law,” it is facing a number of threats today. It is imperative that Illinois lawmakers continue protecting BIPA without chipping away at its many protections. Here’s why:

THREAT:	RISK:	BILLS
Eliminating the private right of action	<ul style="list-style-type: none"> • Losing effective enforcement and any accountability for private entities collecting and sharing biometric information of individuals. • Left unregulated and without reasonable limitations, biometric technologies give corporations and law enforcement the power to track people’s movements and activities in both public and private spaces, while simultaneously creating the risk of exposing people to identity theft without a remedy. 	HB 559, 560, 1764, 3112, 3304, 3414 SB 56, 300, 1607, 2039
Creating a right to cure	<ul style="list-style-type: none"> • Consumers lose protections and businesses gain a get out of jail free card. • A right to cure allows businesses to violate BIPA, knowing that they can avoid any liability under the law by shutting down their violations during a 30-day “cure” period. 	HB 559 SB 56, 300
Carving out an exception for employers	<ul style="list-style-type: none"> • Limiting the extent an employee is able to hold their employer liable for reckless or negligent violation of BIPA. • Leaving the biometric information of employees vulnerable to unlawful and invasive collection by employers. Without robust protections under BIPA, this sort of exception creates a power imbalance that allows employers to create an environment where they are immune from liability and fails to protect employees. 	HB 559, 560, 1764, 3112, 3304, 3414 SB 300, 602, 1607, 2039
Redefining the scope of injury	<ul style="list-style-type: none"> • Overburdening the plaintiff with the requirement to prove an additional injury and going against the very heart of BIPA. • Failing to recognize the loss of control of one’s biometric injury as an injury. 	HB 3112
Reducing recovery for unlawful behavior	<ul style="list-style-type: none"> • Severely diminishing the value of biometric information. Companies will not be held sufficiently responsible for their unlawful behavior and easily be able to pay off the small dollar amounts for violations. • Such limitations fail to acknowledge the harm done by a company’s intentional and reckless behavior and do not provide adequate protections for biometric information. 	HB 559, 560, 1764, 3112, 3304, 3414 SB 300, 602, 1607, 2039
Limiting the definition of biometric information	<ul style="list-style-type: none"> • A large set of data is left vulnerable to misuse by private entities if the definition of biometric information is narrowed. • Carving out an exception for templates created by biometric identifiers fails to acknowledge the harm done by collecting this information and would be counterintuitive to BIPA. 	HB 559, 560 SB 300, 602
Gutting BIPA entirely	<ul style="list-style-type: none"> • Losing all protections for the biometric information and leaving this incredibly sensitive information vulnerable to misuse. • Repealing BIPA would be a massive step backwards for Illinois; a state that has long been the leader in recognizing the privacy rights Illinois residents hold in biometric information. 	HB 3304 SB 2039