BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

BACKGROUND:

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 at a time)
- Obtain the person's written consent
  (e.g. user signs their name before sharing their fingerprint)

BIPA also establishes standards for how companies must handle Illinois consumers' biometric information. For example, the law requires all companies to protect biometric information collected from consumers in the same manner in which it protects other confidential or sensitive information. BIPA also prohibits any company from selling or otherwise profiting from a person's biometric information. The law continues to stand as the most protective in the nation, with the only one of its kind to offer protection with a private right of action. Widely regarded and praised as being "America's strongest biometric privacy law," BIPA continues to be considered model legislation for other states.

WHAT IS BIOMETRIC INFORMATION:

Biometric information means any information, regardless of how it is captured, converted, stored or shared, that is based on an individual's biometric identifier and can be used to identify that person. This includes:

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

What makes this information so unique is that it is arguably the most sensitive data about an individual, in part, because it can never be changed. While someone can get a new email address or phone number, they can never change their fingerprint.

WHY 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. Yet, more than a decade after BIPA's enactment, we constantly hear new examples in which companies have collected, shared, and misused the personal information of millions of people, without their knowledge or consent.

Take for instance the investigation into *Clearview AI*, a facial recognition company with a database of more than 3 billion facial images scraped from social sites. In addition to collecting this data, the company *shares* this data with federal and state law enforcement agencies, who use it to generate leads, target suspects and make arrests. Companies continue to create dangerous products that invade peoples' privacy and make them privy to an unnecessary police investigation.

ACLU Illinois

HOW DO WE PROTECT BIPA:

With new technological advancements implicating the biometric information of millions of people at a time, the strong protections of Illinois's law are more critical now than ever. BIPA is the one recourse Illinoisans have to control their own fingerprints, facial scans, and other crucial information about their bodies. That is exactly what the General Assembly had in mind when it enacted BIPA and what the Illinois Supreme Court held when it analyzed the law in *Rosenbach v. Six Flags*. The Court recognized that in addition to controlling their own biometric information, individuals must have the right to sue companies that unlawfully collect this information in order to hold them accountable. State decision makers must continue to protect BIPA without chipping away at any of the protections it offers.

BILLS THAT WEAKEN BIPA:

A number of bills introduced this session weaken the strength of BIPA. Specifically:

Bill #	Status	Weakens BIPA by ...
HB 5635 Keicher	Referred to Rules Committee	• Expanding the collection of biometric information by creating exceptions to the notice and consent requirement for security purposes and the use of biometric time clocks and locks. • Giving covered entities a "get out of jail free card," by allowing them to get away with violating BIPA, knowing that they can avoid any liability under the law by stopping their violations during the 30-day cure period. • Providing local or federal government agencies the ability to issue an order, warrant, or subpoena allowing entities to retain biometric information indefinitely. • Creating a 1-year statute of limitation.
HB 4686 Ozinga	Re-referred to Rules Committee	• Creating the "get out of jail free card" by establishing a 1-year statute of limitation and a 30-day cure period. • Allowing entities to bargain their way out of compliance with BIPA. • Increasing the amount of information collected about us by allowing entities to collect information derived from biometrics. • Severely weakening the private right of action.
HB 4102 Ford	Referred to Rules Committee	• Expanding the collection of biometric information by creating a "security purpose" exception to the notice and consent requirements. • Creating a "security purpose" exception to the 3-year period that entities can retain biometric information. • Increasing disclosures of biometric information through a "security purpose" exception to the prohibition on disclosures. • Limiting the ability to be anonymous online.
SB 3319 Murphy	Referred to Assignments	• Limiting the scope of entities that must comply with BIPA to those that employ more than 5 individuals despite it only taking one person to collect our biometric information without our permission.
HB 5836	Referred to Rules	• Creating a carveout from compliance for Internet dating services and undefined "providers" acting on their behalf if the collection, use, retention, and disclosure of biometrics can be justified for the vague and broad definition of "security purposes."

For more information contact Khadine Bennett: kbennett@aclu-il.org | 312.607.3355

ACLU Illinois

A No Position BIPA Amendment

In 2023, the Illinois Supreme Court reconsidered the issue of liability asking whether a claim accrued per violation or per person. In *Cothron v. White Castle*, the Supreme Court decided that a claim accrued for each violation. Under existing law, a violation occurs each time a White Castle employee scanned their fingerprint. In affirming the existing law, the Supreme Court acknowledged the White Castle's claim that it could cost as much as $17 billion in damages, and the opinion invited the General Assembly to clarify if it was the intention that damages accrue per violation or per person.

In response, there was a strong push from opposition to use the Supreme Court's decision to severely weaken BIPA including entire industry carveouts for data centers and trucking companies. After conversations and negotiations with interested parties including IRMA, the Chamber of Commerce, trial lawyers and us, legislation was introduced in 2023 as HB 3811 SA2. It was reintroduced this session as SB 2979 amending the enforcement provisions to provide recovery for damages to accrue per person rather than per violation. Critically, SB2979 retains the privacy preserving notice and consent requirements that entities must provide and receive before they can collect our biometric information.

In its current form, we have decided not to take a position on SB 2979 while stressing the vital and necessary role that a private right of action plays in enforcing laws that protect our right to privacy including control over when and if our biometric information can be collected and used. Weak enforcement provisions are a bad way to protect fundamental rights.

Bill #	Status	Amends BIPA by ...
SB 2979 Cunningham	Placed on Calendar for 3rd Reading	• Providing damages to accrue per person rather than per violation of BIPA.

WHAT NEEDS TO HAPPEN:

In order to ensure that the biometric information of Illinoisans remains protected, it is important for Illinois decision makers to:

- Commit to providing the data belonging to Illinois' residents with the utmost protection by prohibiting entities from sharing biometric information, unless they receive the informed written consent of consumers.
- Commit to protecting BIPA as the strongest biometric information privacy law in the nation by reaffirming the message sent by the Illinois General Assembly in 2008 and the Illinois Supreme Court in 2019.
- Commit to putting the privacy interests of Illinois' residents over the financial incentives of corporations.

For more information contact Khadine Bennett: kbennett@aclu-il.org | 312.607.3355

ACLU Illinois