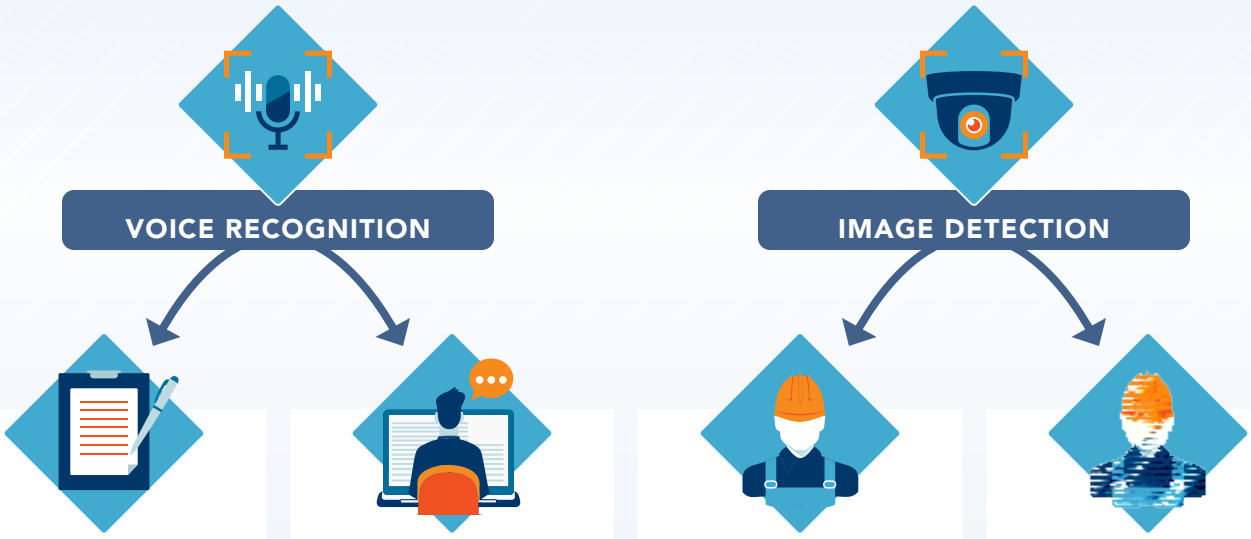
BSA Recommendations for Biometric Privacy Legislation

In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA). BIPA regulates businesses' ability to collect, disclose, retain, and destroy "biometric identifiers," which include retina or iris scans, fingerprints, voiceprints, or hand and facial geometry scans. BIPA enforces these provisions through a broad private right of action.

Protecting the privacy of biometric information is important, but technology has changed significantly in the years since BIPA's enactment. As a result, states that adopt BIPA-style legislation can unintentionally impede beneficial uses of biometric-related technologies. BSA recommends that state lawmakers considering BIPA-style legislation examine how BIPA has been applied in practice, and better focus any legislation to achieve their goals.

Many Types of Technology Use Biometrics

Consumers and businesses today rely on technologies that use biometric information for a range of beneficial reasons, including to improve workplace safety. For example, voice recognition technologies and image detection technology can serve a variety of useful purposes.



Workplace Tool

Used for routine purposes, such as the transcription of meeting records

Assistive Technology

Provides speech-to-text capabilities for people with disabilities

Safety Purposes

Used to detect if construction workers are wearing hardhats or other protective equipment

Facial Redaction/ Blurring

Used to redact/blur faces in videos or images to protect individuals' privacy

Practical Effects of BIPA

BIPA has affected beneficial uses of biometric-related technologies because of its broad definitions of "private entities" and "biometric identifiers." In practice, this results in:

» **Broad application—even to businesses that are not consumer-facing.** BIPA requires private entities to provide individuals with notice regarding the collection and storage of biometric identifiers/information and obtain written consent. Because private entities are defined broadly, these notice and consent obligations can be read to apply even to businesses that lack a direct relationship with a consumer, so may be unable to seek her consent.

» **Broad definition of biometric identifiers—even when they are not used to identify a person.** BIPA focuses on "biometric identifiers" and the statute can be read to impose obligations on all companies that obtain such information even when those identifiers are not used to identify an individual.

BSA Recommendations

Lawmakers considering BIPA-style legislation should address at least four key issues:

1. **Any obligations should focus on companies that decide how and why to use consumers' biometric identifiers, rather than all companies that obtain or possess those identifiers.**
2. **Any obligations should focus on biometric identifiers that are used to identify a specific individual.**
3. **Legislation should be exclusively enforced through the state's attorney general.**
4. **Lawmakers should promote comprehensive privacy bills, rather than more specific biometric privacy legislation.**

1 Any obligations should focus on companies that decide how and why to use consumers' biometric identifiers, rather than all companies that obtain or possess those identifiers.

THE ISSUE: BIPA appears to apply to a wide range of businesses, which it defines as "private entities," regardless of whether the business has a direct relationship to a consumer or controls whether, how, and why a consumer's biometric data is processed. This is particularly concerning for companies that act as service providers, which process biometric information on behalf of business customers. For example, cloud storage providers store business customer information but would have to individually analyze each piece of data to know if it includes biometric data. Applying BIPA to all "private entities" also means consumers may receive consent requests not only from the consumer-facing companies they interact with, but also from dozens of those companies' service providers with whom they have no relationship.

SOLUTION: Any requirements should focus on companies that decide how and why to collect consumers' biometric information—to ensure those companies comply with notice and consent obligations, without requiring duplicative consent requests from downstream companies. To do this, the definition of "private entity" should be narrowed to entities that "determine the purposes and means" of collecting biometric identifiers. This would align the definition with the longstanding definition of a "controller" under comprehensive privacy laws.

2 Any obligations should focus on biometric identifiers that are used to identify a specific individual.

THE ISSUE: BIPA's broad definition of "biometric identifier" can be read to apply even when information is not used to identify a specific person. Because the statute does not define "face geometry," it is unclear if this language could extend to technology that detects the presence or absence of a face, without revealing the identity of an individual. This can result in extremely broad application of the law, limiting potential beneficial uses of biometric-related technologies.

SOLUTION: Any legislation should define "biometric identifier" and "biometric information" as information used to identify a specific individual.

3 Legislation should be exclusively enforced through the state's attorney general.

THE ISSUE: Threats of liability under BIPA's private right of action have had a negative impact on businesses' ability to provide consumers with beneficial uses of technologies that use biometrics. BIPA has led some companies to geographically restrict the products and services they offer to consumers.

SOLUTION: State Attorneys General (AGs) should be provided with exclusive authority to enforce biometric privacy legislation. AG offices have a long history of enforcing consumer protection laws, and all comprehensive state privacy laws empower state AGs to enforce privacy obligations, including protections on consumers' biometric information.

4 Lawmakers should promote comprehensive privacy bills, rather than more specific biometric privacy legislation.

THE ISSUE: Biometric privacy protections are a subset of broader privacy concerns, which should be addressed comprehensively. Creating rules through both BIPA-style laws and separate comprehensive privacy laws creates uncertainty for businesses, impacting their use of technologies that use biometrics for practical and beneficial purposes.

SOLUTION: States should pass comprehensive state privacy laws that include protections on sensitive biometric information.

What Does This Mean for Policymakers?

As deployment of technologies that use biometrics grows, state lawmakers should focus on protecting consumers' biometric information in ways that support beneficial uses of biometrics.