





The Evolving Legal Landscape for Biometric Privacy

Laws and regulations governing biometric data usage and privacy are rapidly evolving across the United States. Groundbreaking legislation like Illinois' Biometric Information Privacy Act (BIPA) in 2008 established requirements for consent and private enforcement that have become a model for many other states. Recent high-profile BIPA lawsuits have further clarified acceptable versus prohibited uses of biometric data. No manual intervention, no SIEM needed. And we do all this before granting login access.



Several key themes have emerged from BIPA and similar efforts:

-  Mandatory opt-in consent for collection or use of biometric data
-  Private right of action for consumers regarding violations
-  Strict data minimization and retention limits
-  Ban on sale or profit from biometric data

In addition to Illinois, states such as Washington, Texas, New York, and others have passed biometric privacy laws. Comprehensive consumer privacy frameworks in California, Colorado, Utah, Connecticut, and Virginia have incorporated biometric consent requirements. This expanding patchwork of legislation aims to grant users control over their biometrics.

The case for on-device biometrics

With biometrics becoming ubiquitous for device unlock, authentication, and more, there are two primary approaches to biometric data storage:

-  **Centralized:** Biometric data stored on servers or cloud platforms. This method is vulnerable to large-scale compromise via breaches.
-  **On-device:** Biometric data stored locally on user devices only. This decentralized approach aligns with privacy best practices by avoiding centralized repositories.

Recent BIPA lawsuits have upheld on-device biometrics as compliant due to their enhanced privacy posture. The evolving legal landscape points toward on-device biometrics as the most viable path for balancing security, user experience and biometric privacy.

Beyond Identity's privacy-first approach

Beyond Identity's identity and access management platform is architected exclusively using on-device biometrics from major providers like Apple, Microsoft and Google. By leveraging biometrics stored locally on user devices, Beyond Identity avoids any centralized storage of biometric data.

This approach fully aligns with both the spirit and letter of current and emerging biometric privacy laws. BIPA and other efforts aim to put control in the hands

of consumers. Beyond Identity reinforces user control and privacy by binding biometric data to user devices.

Organizations that adopt Beyond Identity can deploy our solutions with confidence that our platform is at the leading edge of biometric privacy best practices. Our exclusive use of on-device biometrics means no additional effort is required to conform to biometric consent, data minimization, or other requirements.

Our commitment to security and privacy

Beyond Identity enables simpler, stronger authentication while protecting biometric privacy. Our platform offers the optimal balance of security, experience, and compliance with current and pending biometric privacy legislation. Security professionals

can trust in the robust systems we have in place, ensuring the highest standards of digital security for your organization. With Beyond Identity, your organization's digital assets are protected and user privacy is upheld.

Disclaimer

The information provided on this website does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available on this site are for general informational purposes only. Information on this website may not constitute the most up-to-date legal or other information.

BEYOND IDENTITY

Beyond Identity is revolutionizing digital access for organizations looking to improve protection against cyber attacks and deliver the highest levels of security for their workforces, customers and developers. Its suite of passwordless, phishing-resistant, and zero trust authentication solutions improves security and user experience. The platform delivers continuous risk-based authentication incorporating signals from the zero trust ecosystem to ensure only valid users and secure devices gain or maintain access to critical resources. Companies like Snowflake rely on Beyond Identity's highly available cloud-native platform to thwart attacks and advance their zero trust strategies. To learn more about Beyond Identity's FIDO-2 certified multi-factor authentication (MFA) solutions, visit beyondidentity.com and stay connected with us on [Twitter](#), [LinkedIn](#), and [YouTube](#).

Get a demo

beyondidentity.com

info@beyondidentity.com

BEYOND
IDENTITY