
BAKER BOTTS
PARTNER TO THE INNOVATORS

Biometric Data Privacy & Litigation: Emerging Risks and Compliance Strategies

Matthew Baker

Practice Chair – Privacy & Cybersecurity

Jenna Comizio

Vice President, Compliance & Legal Affairs

Cara Ciuffani

General Counsel

Biometric Data - Defined

Biometric data includes physiological or behavioral characteristics used to identify individuals (e.g., fingerprints, facial recognition, retina scans, voiceprints).

Definitions vary slightly under different statutes, but the focus remains on uniqueness to an individual.

Why Biometric Data is Distinct

- **Immutability**: Unlike other personal data, biometric traits cannot be changed if compromised.
- **Sensitivity**: Highly personal nature heightens potential harm from misuse and, therefore, expectations of privacy.
- **Growing Use**: Rapid adoption of technology in workplace, public spaces, and consumer applications.
- **Risk Profile**: Breaches can expose individuals to lifelong risks; loss can be permanent.

Example Use Cases Across Industries

Industry	Function
Employment	Timekeeping systems; workplace access control
FinTech	Identity verification for account access (e.g., voiceprints, face ID)
Healthcare	Patient authentication and medical record security
Retail	In-store security (e.g., facial recognition); Consumer product authentication

Legal Landscape and Key U.S. Statutes

Law/Ordinance	Scope	Private Right of Action	Enforcement Authority	Notable Provisions
Illinois Biometric Information Privacy Act (BIPA)	Applies to private entities collecting biometric identifiers (e.g., fingerprints, facial scans) within Illinois.	Yes	Civil	Strict consent and data handling requirements; significant statutory damages
Texas Capture or Use of Biometric Identifier Act (CUBI)	Applies to entities collecting biometric identifiers for commercial purposes in Texas.	No	Attorney General	Consent and timely data destruction
Washington House Bill 1493 (HB 1493)	Regulates the collection and use of biometric identifiers for commercial purposes in Washington State.	No	Attorney General	Consent with exceptions for security purposes; data protection obligations
California CCPA/CPRA	Applies to businesses collecting personal information of California residents, including biometric data categorized as "sensitive personal information."	No (for compliance) Yes (for a breach)	California Privacy Protection Agency & Attorney General Civil	Consumer rights to limit use of sensitive personal information
New York City Biometric Privacy Ordinance	Applies to commercial establishments in NYC that collect biometric identifier information from customers.	Yes	Civil	Mandatory signage; prohibition on sale of biometric data

Litigation Trends

Class Actions

- Over 1,500 BIPA class action filings since 2019.
- Common targets: big tech, employers, retailers, app developers.
- Settlements ranging from modest sums to over $1B.

Key Cases

- *In re Facebook Biometric Information Privacy Litigation* (2021) - $650M BIPA settlement over photo tagging system.
- *Cothron v. White Castle* (2023) – IL Supreme Court rules that a separate BIPA claim for damages accrues each time a private entity scans or transmits an individual's biometric identifier or information.
    - Now, under SB 2979 (2024), a private entity collecting the same biometric identifier from an individual using the same method is considered to have committed a single BIPA violation.
- *Texas v. Meta Platforms* (2022) - $1.4B CUBI settlement for repeatedly running facial recognition without consent on millions of Texans through the "tag suggestions" feature.

Common Claims

- Failure to obtain informed consent
    - Retroactive or bundled consents often deemed insufficient.
- Failure to maintain reasonable security
    - Data storage and encryption practices under scrutiny.
- Unauthorized sharing or indefinite retention
    - Retention schedules often missing.

Other Liability Considerations

- **Third-Party Data Systems**: Companies can liable for tech they *buy*. Risk isn't only from in-house systems but also vendor-provided solutions.
- **Jurisdictional Reach**: Even a single store or employee in a biometric-regulating state creates multi-state compliance obligations for the whole organization.

Officer & Director Personal Liability

- Courts are increasingly allowing suits against corporate officers who “authorized or participated” in violations related to cyber incidents, and this trend could extend into biometrics.
- Biometric claims may trigger coverage under directors and officers (D&O) insurance policies, though this differs for public and private companies, and policy exclusions. related to PII disclosure are increasing.
- Cyber insurance policies may cover regulatory fines and penalties.
- Ensure proper management and adherence to protocols when overseeing biometric programs to minimize risk.

Compliance & Risk Mitigation

Notice and Consent

- Provide clear, separate, written notice before collection.
- Obtain affirmative consent, not passive or bundled with other agreements.
- Make disclosures specific about purpose, retention, and sharing.
- Essentially, no surprises – the person should understand exactly what they are consenting to.
- Store copies of these consents (and timestamp them) because they are your legal defense if a dispute arises.

Data Minimization & Retention Policies

- Only collect biometric data that is strictly necessary for the purposes.
- Publish written retention schedules.
- Automatically and securely dispose of biometric data at the earliest point allowable by law.
- In practice, set a conservative retention period – *e.g.*, if an employee leaves, delete their biometrics promptly; if a customer stops using the service, purge their data. Include this schedule in your policy and stick to it.

Security Measures & Privacy by Design

- Encrypt biometric data both in transit and at rest.
- Implement strict role-based access controls and multi-factor authentication.
- Conduct regular vulnerability assessments and penetration tests.
- Ensure that any new product or system involving biometrics goes through a Privacy Impact Assessment.

Vendor Management

- Conduct due diligence on vendors processing biometric data.
- Include specific contractual terms on data use limitations, breach notification, and audit rights.
- Ensure downstream processors (i.e., subprocessors) also comply with applicable law.

- Regularly train employees handling biometric data on legal obligations and internal procedures.
- Frontline staff should understand how to obtain valid consent and safeguard data.
- They should know to seek legal/privacy approval before launching any new biometric project.
- Regularly refresh training and update it when laws change.
- Educate management about the serious financial risks of non-compliance so they support these efforts.

Litigation & Incident Response Readiness

- Maintain compliance documentation (e.g., signed consents, retention logs) and follow those policies.
- Design programs with an eye toward early dismissal defenses (e.g., clear consent flows).
- Recognize the stakes of a biometric data breach in incident response planning, prioritizing immediate containment, notification to affected individuals, and prompt regulatory reporting.

Emerging Areas to Watch

AI & Biometrics

Algorithmic bias, surveillance concerns, new forms of biometric analysis (e.g., gait recognition).

Legislative Trends

Discussions around new state privacy laws incorporating biometric-specific requirements, or new biometric requirement.

Reforms to BIPA & Other Biometric Statutes

Potential adjustments to statutory damages or class action scope.

FTC Enforcement

The FTC has signaled it will scrutinize misuse of biometrics under its consumer protection mandate.

Practical Strategies for Privacy Teams

Map Biometric Data Uses

Identify all instances where your company is collecting or using biometric information.

Assess Legal Obligations by Jurisdiction

If dealing with a patchwork, apply the strictest applicable law

Implement Strong Procurement Practices

Ensure your **contracts have robust privacy and security clauses**.

Establish Protocols & Checkpoints

Create an internal process so that **any new project or technology involving biometrics is reviewed by legal/privacy counsel** before implementation.

Training & Awareness for Key Teams

Conduct training sessions for HR, Security, IT, and product development teams focusing on biometric data rules

Prepare for DSARs

Plan how for regulatory requests and appropriate responses.

Insurance and Liability Planning

Given the class action trend, **having insurance for defense costs and settlements** could be financially prudent

Stay Updated on Legal Developments

Biometric privacy law is a fast-evolving field. In-house counsel and privacy officers should **stay current** through updates from law firms, industry groups (IAPP, etc.), and news of court decisions

AUSTIN
BRUSSELS
DALLAS
DUBAI
HOUSTON
LONDON
NEW YORK
PALO ALTO
RIYADH
SAN FRANCISCO
SINGAPORE
WASHINGTON

bakerbotts.com