Foster Garvey

Biometric Privacy in Washington Workplaces: Key Considerations for Employers

Legal Alert
October 17, 2025

Employers in Washington who use biometric timekeeping or security tools should take note of recent developments. While current state laws provide some exemptions for employment-related uses of biometric data, new litigation and emerging best practices highlight the need for careful attention to compliance, even when third-party vendors are involved.

Understanding Biometric Data

Biometric data refers to unique physical, biological or behavioral characteristics used to identify individuals, such as fingerprints, facial recognition, iris scans and voice patterns. These tools can help prevent time theft and simplify payroll or access control, but they also create privacy and security risks when biometric data is collected, stored or shared with third-party vendors.

Washington's Biometric Exemptions

Washington's 2017 Biometric Identifier Law and the My Health My Data Act (MHMDA) generally exempt biometric data collected for employment or security purposes. In these cases, the data may fall outside the laws' substantive compliance requirements such as notice and consent obligations or data subject rights, if implemented correctly.

While these carve-outs can reduce compliance burdens, they do not remove all legal risk. Employers may still face liability if a third-party vendor mishandles biometric data, or the employer's use of biometric information evolves to serve commercial rather than strictly employment-related purposes.

Contact

Claire F. Hawkins

Kenzie Kinsella

Related Services

IP & Technology

Labor, Employment & Immigration

Privacy, Cybersecurity & Data Protection

Multi-State Operations

Although most biometric systems are used at specific local sites, broader company-wide implementation may raise compliance issues. If employees or customers from other states interact with biometric systems, this could trigger additional requirements, including:

- Written notice and consent obligations
- Company data retention and destruction policies
- Limits on how biometric data can be used
- Enhanced data security parameters
- Documentation and recordkeeping standards
- Restrictions on specific uses of biometric information

Employers with multi-state operations should consult counsel in advance to confirm compliance with all applicable state laws before implementing biometric tools across jurisdictions.

Guidance from Federal and Other States Helps Shape Best Practices

Currently, there is no federal biometric privacy law, but the Federal Trade Commission Act (FTCA) authorizes the Federal Trade Commission (FTC) to pursue enforcement actions against unfair or deceptive practices, including misuse of biometric data.

In 2023, the FTC cautioned that deceptive or incomplete disclosures about the use of biometric data may violate the FTCA and could lead to enforcement actions.

Additionally, Illinois' Biometric Information Privacy Act (BIPA), widely considered the most stringent biometric privacy law in the United States, serves as a model for robust compliance obligations, even for employers operating outside Illinois.

What Employers Can Do

Audit Vendor Agreements

- Confirm that vendors are contractually prohibited from using biometric data for non-employment purposes or sharing it without the individual's prior informed written consent.
- Require vendors to maintain documentation showing that valid consent has been obtained.

- Limit vendor use of biometric data to specific, approved employment functions, such as timekeeping, access control, identity verification and safety compliance.

Review and Update Privacy Policies

- Ensure that privacy policies related to employment practices clearly and accurately disclose what biometric data is collected, how it is used, how long it is retained, how it is protected and when it may be shared with vendors.
- Avoid vague or incomplete language that could mislead employees or omit key details about biometric data practices.
- Align internal procedures and employee training materials with those disclosures to maintain accuracy and consistency.

Consider BIPA-Inspired Safeguards

Even if not legally required, adopting BIPA-style safeguards can significantly reduce risk, set clear expectations and demonstrate a proactive commitment to privacy and compliance. Employers should consider:

- Obtaining written consent from individuals before collecting biometric data
- Implementing defined retention schedules that specify how long data will be stored and when it will be destroyed
- Publishing a public-facing privacy policy that explains the company's biometric data practices

These measures can help reduce risk, set expectations and demonstrate a commitment to privacy and compliance.

Prioritize Clear Consent and Protection of Biometric Data

Ensure individuals, whether employees or consumers, are clearly informed about:

- What biometric data is being collected
- How that data will be used
- Whether it will be shared with others

Whenever possible, obtain and retain express, prior written consent.

To comply with privacy requirements and the Americans with Disabilities Act (ADA), biometric data, particularly if connected to health or disability information, should be:

- Stored separately from general personnel files
- Access-limited to individuals with a legitimate business need
- Properly encrypted
- Securely retained

Taking these steps not only supports compliance but also helps mitigate risk in the event of litigation or regulatory scrutiny.

Update Incident Response Plans to Address Biometric Data

Existing data breach response plans should be updated to explicitly address biometric data. If biometric data is compromised, the risks are heightened. Unlike passwords, biometric identifiers cannot be changed. This increases the potential for identity theft and fraud. A biometric data breach can expose an employer to:

- Regulatory penalties
- Private lawsuits under statutes such as BIPA
- Reputational damage

Incident response plans should include prompt mitigation steps, documentation procedures and compliance with all applicable breach notification timelines.

Looking Ahead

A pending class action under the My Health My Data Act (MHMDA) against Amazon may clarify how Washington courts interpret the scope of "consumer health data" and what qualifies as "harm" under the statute. In the meantime, employers should regularly evaluate their biometric systems and vendor relationships by securing indemnification and compliance warranties, reviewing privacy and security policies, monitoring data handling practices and requiring breach notification provisions. Conducting audits, assessing vendors' compliance records and working with privacy and employment counsel can further help identify and mitigate potential liability.

The information above involves complex legal considerations and is provided for general informational purposes only. It does not constitute legal advice. For guidance on specific legal matters, please contact your attorney.