Employer Tips For Wise Use Of Workers' Biometrics And Tech

By **Douglas Yang** (February 18, 2025)

Douglas Yang

This article provides guidance on biometrics and personal devices in the workplace. Prioritizing compliance for employee biometric data and bring-your-own-device, or BYOD, policies is important to safeguard sensitive information and maintain employee trust.

Biometrics, such as fingerprint and facial recognition, offer enhanced security but also raise privacy concerns and legal obligations.[1] Similarly, BYOD policies, which allow employees to use personal devices for work, can increase productivity and flexibility but also pose significant security risks.[2]

Employee Biometric Data

No single federal law regulates an employer's access to or use of employee biometric data, leaving the states to take the lead in regulating this developing space. Several states, including California, have enacted comprehensive data privacy laws that include biometrics as one category of protected data.[3]

By and large, however, few jurisdictions thus far have gone to the length of expressly limiting employer use of employee biometric data. Biometrics are commonly used for time clocks, as well as restricted access identification protocols.

The first law regulating the use of biometric data was Illinois' Biometric Information Privacy Act, or BIPA, which was enacted in 2008 and thereafter has led to various states adopting BIPA-like language — as well as a cottage industry of intense class action litigation brought against all manner of companies.

Under BIPA, a biometric identifier is a (1) retina or iris scan, (2) fingerprint, (3) voiceprint, or (4) scan of hand or face geometry.[4] The conversion of a biometric identifier into a usable form — i.e., to identify a person — constitutes biometric information that is regulated by BIPA.

BIPA imposes an affirmative consent requirement upon employers. Before a BIPA-regulated employer obtains biometric identifiers or biometric information from its employees, the employer must first:

- Notify each employee in writing of the specific reason for collecting, storing and using the information, and how long the biometric identifier or biometric information will be used or retained; then

- Receive each employee's signed written release, which in the context of employment is a release executed by an employee as a condition of employment.[5]

BIPA imposes various other recordkeeping and internal policy promulgation requirements.

Even in states where no biometric information law is currently on the books, the influence of BIPA has been widespread and profound, such that BIPA-like laws are to be expected going forward. California has not implemented a BIPA-like law, but the California Consumer Privacy Act does require covered employers to provide the appropriate notices to employees regarding the use of biometric information.

One area of confusion within California law concerns Labor Code Section 1051,[6] which prohibits employers from sharing or disclosing fingerprints or photographs with any third party when the employer requires its employees to submit them.

At first glance, the statute appears to functionally prohibit the use of any outside technology with fingerprint data or photographs, since such technology would inevitably involve the third-party vendor that maintains the technology and, therefore, would have access to the biometric data.

However, in a February 2014 opinion letter,[7] former California Attorney General Kamala Harris interpreted Section 1051 to permit an employer's agent — i.e., a vendor — to receive the biometric data, provided the agent is acting for the sole benefit of the employer and the file is only furnished to the employer.

As such, while current interpretations of Section 1051 may permit employers to use biometric technology, employers should ensure that they enter contracts with vendors to confirm that the collection and use of biometric data is restricted to the purpose for which the employer seeks to use that data.

Wearable Technologies

A related issue involves the use of wearable technologies in the workplace and their implications under federal equal employment opportunity laws.

Wearables are digital devices worn on the body that can track movements or location and collect biometric information. They include smart watches, smart rings, smart glasses, exoskeletons and other devices.

In December, the Equal Employment Opportunity Commission — which enforces federal laws prohibiting employers from discriminating on the basis of race, color, national origin, religion, disability, being 40 or older, genetic information, and sex, including pregnancy, sexual orientation and gender identity — issued a fact sheet providing guidance to employers on using wearable technologies in the workplace.[8]

In the fact sheet, the EEOC highlights potential equal employment opportunity compliance issues when employers direct employees to use wearable technology in order to obtain health-related information. For example, the Americans with Disabilities Act limits disability-related inquiries and medical examinations, as well as limiting the conditions where such inquiries are allowed, such as when they are job-related and consistent with business necessity. This means that if an employer mandates the use of wearables that collect health data, they must ensure that such requirements comply with ADA standards.

Additionally, the EEOC emphasizes the importance of confidentiality and the proper handling of medical information obtained through wearables.

Furthermore, the EEOC discusses the implications of using wearable technology data to make employment decisions. Employers must be cautious to avoid discrimination based on

information collected by these devices. For example, if wearables reveal information about an employee's health condition, employers must not use this information in a way that could be discriminatory under equal employment opportunity laws.

The EEOC fact sheet also highlights the potential "need to make an exception to a wearables policy as a reasonable accommodation" for certain employees. Under Title VII of the Civil Rights Act, the ADA and the Pregnant Workers Fairness Act, employers are required to provide reasonable accommodations to employees who have religious needs, are disabled, or are pregnant or have recently given birth.

The EEOC also addresses the accuracy and reliability of data collected by wearables. Employers must ensure that the data is accurate and used appropriately. Inaccurate data could lead to unfair treatment or discrimination, which would be a violation of equal employment opportunity laws.

Additionally, the storage and security of data collected by wearables is crucial. Employers must implement measures to protect the data from unauthorized access and ensure it is used only for legitimate business purposes.

Employee Use of Personal Devices for Work

The practice of permitting employees to bring their own devices is widespread, particularly since the advent of the COVID-19 pandemic and the significant increase in the number of employees who work remotely or on a hybrid schedule. BYOD practices can be beneficial because:

- Employees are often more comfortable and efficient using their own devices;
- Companies can reduce hardware and maintenance costs by leveraging employees' personal devices; and
- Employees can work from anywhere, enhancing flexibility and supporting remote work arrangements.

On the other hand, the use of BYOD can also have the following disadvantages.

Security Risks

Personal devices may lack robust security measures, making them vulnerable to malware, hacking and data breaches. Sensitive company data could be exposed if devices are lost or stolen.

Employees may inadvertently share confidential information through personal apps or cloud services.

Network Exposure

Personal devices connecting to the company network can introduce vulnerabilities, potentially allowing unauthorized access to company systems.

IT Support Challenges

Supporting a wide range of devices and operating systems can strain IT resources and complicate troubleshooting and maintenance.

Employers may struggle to comply with data protection regulations if they cannot control how data is stored and accessed on personal devices.

Reimbursement Requirements

Some jurisdictions, such as California, may require employers to reimburse employees if they must use their personal devices to fulfill mandatory work duties.[9]This may pose a significant administrative burden and headache that outweighs the benefits of a BYOD program.

Reduced Monitoring and Surveillance Capabilities

By and large, surveillance and monitoring of employees' personal devices is disfavored, even where the device is partially used for work purposes.

The courts consistently appear to view surveillance more favorably when it is performed on company-owned and operated devices. Employers should not consider the installation of a work application on an employee's device to be carte blanche to mount continuous surveillance of the employee.

Conclusion

Employers should ensure that biometric data is securely stored and handled in compliance with privacy regulations to protect employee information. Additionally, it's important to communicate transparently with employees, in writing, about how their biometric data will be used and safeguarded.

Relatedly, if an employer decides to adopt a BYOD program, it should memorialize the program in writing, preferably in an employee-facing policy. Such a policy should explain the requirements of the program, such as the security, usage or technical specifications imposed on the employee's personal device. It should also detail the program's limitations, such as requirements to keep personal devices updated and for nonexempt employees to not use their devices for work purposes outside their work hours.

A BYOD policy should also explain what employees can expect from participation in the program, such as the rate at which employees will be reimbursed for using their own device, whether employees' devices will be monitored by having work applications on them and how work data will be deleted upon separation of employment.

Douglas Yang is a partner at Sheppard Mullin Richter & Hampton LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] For more information on biometrics, see Biometrics Workplace Compliance and Best Practices for Employers.

[2] For more information on drafting such policies, see Bring-Your-Own-Device (BYOD) Policies: Key Drafting Tips.

[3] Cal. Civ. Code § 1798.140(c).

[4] 740 ILCS 14/10.

[5] 740 ILCS 14/10 and 14/15 (as amended effective Aug. 2, 2024).

[6] Cal. Lab. Code § 1051.

[7] https://oag.ca.gov/system/files/opinions/pdfs/12-1101_0.pdf.

[8] https://www.eeoc.gov/newsroom/eeoc-highlights-how-wearable-technologies-may-implicate-employment-discrimination-laws; https://www.eeoc.gov/sites/default/files/2024-12/Wearables_Fact_Sheet_V10_%28002%29_508FINAL.pdf.

[9] Cal. Lab. Code § 2802.