EEOC Wearable Tech Guidance Highlights Monitoring Scrutiny

By **Zoe Argento, Bradford Kelley and Sean O'Brien** (January 29, 2025)

Zoe Argento

On Dec. 19, against a backdrop of various state laws regulating employee monitoring technologies, the U.S. Equal Employment Opportunity Commission published its **first fact sheet** on wearable technology under employment anti-discrimination laws.

Largely building on prior publications addressing artificial intelligence and technology in the workplace, the new fact sheet cautions against potential issues with federal EEO laws. Employers operating globally, however, may face stricter restrictions on such technology outside the United States.

Bradford Kelley

The EEOC's new fact sheet, "Wearables in the Workplace: Using Wearable Technologies Under Federal Employment Discrimination Laws,"[1] provides pointers to employers that utilize wearable technologies in their workforce. It also demonstrates growing concern from regulators and legislators about intrusive technologies in the workplace.

This concern has resulted in a **memorandum on surveillance** from the general counsel of the National Labor Relations Board; guidance on AI in the workplace from multiple federal agencies; and an array of state legislation on location tracking, biometric data and other forms of surveillance.[2]

Sean O'Brien

In this case, the EEOC cabined the fact sheet to wearables, such as smartwatches, glasses or helmets that monitor employees in the workplace; sensors that warn the wearer of a nearby hazard; and GPS devices that track location.

The EEOC did not explicitly define "wearable," instead referring to "digital devices embedded with sensors and worn on the body that may keep track of bodily movements, collect biometric information, and/or track location."

The fact sheet divided the risks arising from these devices into three categories: collecting information from wearables, using information from wearables and reasonable accommodations for wearables.

Regarding collecting information from wearables, the EEOC warned that any wearable that collects information about an employee's medical status, such as blood pressure monitors, may run afoul of the Americans with Disabilities Act. Further, the EEOC opined that such wearables could be classified as conducting medical examinations or making disability-related inquiries.

Under the ADA, medical examinations and disability-related inquiries are permitted only if they are related to the employee's specific job, and the exam or inquiry is consistent with a business necessity. Therefore, according to the EEOC's new fact sheet, employers could be liable for violating the ADA if they mandate all employees use a company-issued wearable that collects information, such as vital signs, without a business need.

Relatedly, if medical data is included in the information the wearable collects, employers should be careful to store that information separately from employees' personnel files. The following examples highlight a few considerations for employers.

First, employers considering utilizing wearables should spend time identifying the specific data and information they need to collect, and narrow the wearable to collect only that data and information.

Second, employers should be cognizant of where the data and information is stored, not only internally, but also where the wearable's vendor may store data. Doing so helps to ensure compliance with the ADA and local privacy laws.

The EEOC also warned of the risks of improperly using information from wearables. In particular, employers may violate EEO laws by taking adverse actions against employees based on information from wearables. These laws could include Title VII of the Civil Rights Act of 1964 or the Genetic Information Nondiscrimination Act.

For instance, an employer might use a wearable that collects inaccurate data about the productivity of employees with darker skin tones. In such a case, the employer may violate Title VII if it terminates these employees or takes other adverse actions against them based on the inaccurate data. This example underscores the importance of employers vetting the wearable technology's accuracy and validity testing, prior to implementing it in the workplace.

Importantly, the EEOC cautioned that even if the wearable technology complies with the ADA and other EEO laws, employers must still ensure they comply with the ADA insofar as certain employees may need accommodations for religion, pregnancy or disability.

Many of the points in the EEOC's fact sheet mirror concerns expressed in opinions and guidance from other regulators. For example, in October 2022, the NLRB's then-general counsel Jennifer Abruzzo released a memorandum[3] addressing various technologies, such as wearables, keyloggers, and software that takes screenshots, webcam photos or audio recordings.

While those technologies may be used to track and manage employees' productivity, Abruzzo noted that "employers could use these technologies to interfere with the exercise of Section 7 rights under the National Labor Relations Act by significantly impairing or negating employees' ability to engage in protected activity — and to keep that activity confidential from their employer."

Another concern arises when the wearable technology includes AI or similar software. In a joint

announcement[4] with the U.S. Department of Justice, the EEOC previously warned of "issues of technological equity, inclusion and accessibility" as AI is implemented in employment settings.

In 2021, the EEOC launched an AI initiative out of concern that AI tools may put certain employees at a disadvantage, including disabled employees. Indeed, the EEOC's first AI guidance document focused on disability discrimination.

Since then, the federal government has taken a whole of government approach to new technology, AI, and employment laws and regulations.[5] However, the EEOC has failed to issue any AI guidance in over a year and a half.

Outside the federal government, the last decade has seen a steady drumbeat of new state laws to regulate employee monitoring technologies.

Illinois and Texas have long had statutes that regulate the collection and handling of biometric information by private companies.[6] In the past year, Colorado enacted a statute requiring employee consent and other steps before employers can collect biometric information from employees.[7] Moreover, many states have passed laws requiring security safeguards and data breach notifications for biometric data.

On location tracking, Hawaii and New Jersey recently passed statutes requiring, respectively, consent and notice for certain types of workforce location tracking.[8] This new legislation adds to the statutes in approximately 20 states regulating the tracking of individuals' locations.[9] In even more targeted legislation, several states have prohibited employers from requiring employees to implant microchips.[10]

A separate trend takes aim at surveillance more broadly. For example, New York,[11] Connecticut and Delaware[12] now require written notice for many forms of workplace surveillance. Additionally, California has proposed regulations that would require detailed risk assessments, notice and data rights for certain types of employee monitoring.[13]

This new legislation layers over existing common law privacy protections; as well as statutory protections against eavesdropping, typically called wiretap laws; and video surveillance in private areas, such as restrooms.

Employers should bear in mind that wearables may collect information not only about the individual wearing the device, but also about others in the vicinity. For example, smart glasses that record what an employee sees and hears could violate wiretap laws and inadvertently capture images of other employees changing or in restrooms.

Finally, surveillance protections in other countries may be much stricter than in the United States. Most countries have comprehensive data protection laws that require notice for all forms of personal data collection, grant individuals the right to obtain the personal data collected about them, and impose detailed requirements related to data retention, security and cross-border data

transfers.

Moreover, in the European Union, as well as some other countries, intrusive continuous surveillance of employees typically violates data protection laws.

Depending on the technology and jurisdiction, employers may face a variety of risks and compliance hurdles in using wearables. To address these issues, employers should perform due diligence prior to integrating wearables into the workforce.

For instance, employers should first identify both the data they're seeking and legitimate business reasons for collecting that data. This process may help identify data that presents unnecessary risks to the business. In limiting the information collected, employers can reduce potential exposure to certain claims.

After identifying the data to be collected, employers should thoroughly vet the provider of the wearables, including how data is collected and where it is stored, the vendor's process for testing and validating the data's accuracy, the vendor's data security measures, and any disparate impact assessments the vendor conducted.

During this process, employers should review the applicable laws in jurisdictions where the data is collected and stored, in order to determine potential risks under relevant law and compliance obligations, such as notice, consent and formal risk assessments.

Then, the employer should conduct a risk-benefit analysis to determine whether the benefits of the technology outweigh the risks and compliance burdens of using it.

If the technology passes the test, the next step is rollout. Employers might consider doing a trial roll out first to work out hitches in the technology.

Regardless, employers should thoughtfully prepare communications to their workforce about the technology. These communications should comply with legal notice and consent requirements, and should also seek to address employees' concerns and questions.

In addition, employers should implement policies and procedures to ensure the wearables are used properly, and should provide training as needed.

With all this preparation, a company has a good chance of a smooth roll out and successful use of the technology. However, even successful programs require some monitoring.

In particular, employers should review manufacturer updates against applicable laws for changes in the collection, use and disclosure of the data, and changes in applicable laws.

Also, employers might consider periodic disparate impact assessments. By taking these steps,

employers can reduce the risk of harming employee morale, the risks identified in the EEOC's new fact sheet, and the risks under privacy and other laws.

Zoe M. Argento and Bradford J. Kelley are shareholders, and Sean P. O'Brien is an associate, at Littler Mendelson PC.

[1] https://www.eeoc.gov/newsroom/eeoc-highlights-how-wearable-technologies-may-implicate-employment-discrimination-laws.

[2] For more information on these developments, please see our articles: James A. Paretti, Jr. Christopher R. Henderson, and Michelle L. Devlin, NLRB General Counsel Calls for Board to Crack Down on Electronic Surveillance and Automated Management Practices, Littler Insight (Nov. 3, 2022); Bradford J. Kelley, Alice H. Wang, and Sean P. O'Brien, DOL Issues "AI & Inclusive Hiring Framework" Through Non-Governmental Organization, Littler ASAP (Sept. 25, 2024); Zoe Argento, Philip Gordon, Kwabena Appenteng, Alyssa Daniels, and Orly Henry, Implications for Employers of Colorado's New Biometrics Law, Littler Insight (June 27, 2024); Zoe Argento, Francis Kenny, and Spencer Soucy, New Jersey Joins the Trend of Increasing Privacy Protections for an Employee's Location, Littler Insight (Mar. 30, 2022).

[3] https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and.

[4] https://www.justice.gov/archives/opa/blog/anniversary-americans-disabilities-act-justice-department-and-equal-employment-opportunity.

[5] https://www.littler.com/publication-press/publication/dol-issues-artificial-intelligence-principles.

[6] See 740 Ill. Comp. Stat. 14/1 et seq.; Tex. Bus. & Comm. Code § 503.001.

[7] H.B. 24-1130, 74th Gen. Assemb., 2024 Reg. Sess. (Colo. 2024).

[8] Haw. Rev. Stat. § 378-102; N.J. Stat. Ann. § 34:6B-22.

[9] NCSL, Private Use of Location Tracking Devices: State Statutes, https://www.ncsl.org/technology-and-communication/private-use-of-location-tracking-devices-state-statutes (last visited Jan. 7, 2025).

[10] See Cal. Civ. Code § 52.7.

[11] N.Y. Civ. Rights Law § 52-C.

[12] See Conn. Gen. Stat. §31-48D; Del. Code § 19-7-705.

[13] For more on the proposed regulations, please see our article Zoe Argento, Denise Tran-Nguyen, Kwabena Appenteng, and Philip Gordon, Automated Decisionmaking Technology, Risk Assessments, Cybersecurity and More: Implications of the Proposed CCPA Regulations for Employers, Littler Insight (Dec. 9, 2024).