# OSHA Inspectors to Use AI-Driven Smart Glasses to Inspect Workplaces: What Employers Should Do to Protect Privacy Rights

Insights
12.10.24

A high-tech company just announced that it will expand its deployment of smart glasses equipped with cameras, sensors, and internet connectivity to even more federal safety inspectors in 2025 so they have ability for real-time documentation, augmented reality features, and instant communication with outside personnel. Although details of OSHA's intended use of the Vuzix M400™ smart glasses are limited, the December 2 announcement raised eyebrows in the employer community. After all, the continuous use of cameras and recording features raises significant questions about whether their use might violate constitutional protections and even OSHA's own policies concerning the use of recording devices during inspections and interviews. What do you need to know about this development and what steps can you take now to protect your organization and your employees?

**What are Smart Glasses?**

Smart glasses are wearable devices equipped with cameras that can record video and audio, take photos, and stream live footage. Often, when connected to the internet, smart glasses can also provide the wearer with real-time access to "augmented reality" (AR), which is technology that overlays digital information such as images, videos, sounds, or other data. Like a scene out of Spielberg's "Minority Report," inspectors using the glasses would have real-time access to regulations, SDSs, and even remote consultations with other OSHA personnel or experts that only they could see.

Indeed, the Vuzix M400s boast an "ultrabright OLED display system" with the capability to share "perspective in superior detail" with a "4K video streaming auto-focus camera," "noise cancelling microphones," "wide field view," and "voice inputs," all the while keeping it hands-free. Last week's announcement also indicated the glasses would be equipped with subscription-based Zoom licenses to boost operational efficiency during field inspections and service activities. According to Vuzix, the M400 is compatible with almost any PPE and bears an Ingress Protection Rating of 67 (IP67), indicating it is dust proof and water-resistant, on par with most modern cell phones.

**6 Concerns Over Use of Smart Glasses During OSHA Inspections**

Traditional OSHA inspections often involve inspectors conducting walkthroughs of worksites with their actions typically known and identifiable to workers. We often advise employers to "take the same photos, videos, and sampling as OSHA during the walkaround." But with smart glasses, inspectors may be able to **discreetly record and stream footage** without employers or employees realizing they are being monitored or what has been recorded.

This kind of **covert documenting and surveillance** could be seen as an unreasonable search or infringement on privacy rights, especially considering that everything OSHA sees during an inspection is fair game. OSHA inspeactors can cite you for what they see; in the near future, they could potentially cite you for what smart glasses see.

Another concern is the **storage and use of the footage** collected by smart glasses. The video, photos, and other data captured by the glasses are often stored in the cloud or on remote servers, potentially making them accessible to unauthorized parties. In industries where sensitive business practices, trade secrets, or proprietary information are involved, this data could be vulnerable to breaches.

Employers and workers alike **would not have control** over how their images or videos are used, who can access them, or whether they are kept private and/or confidential. Note that documents you produce to OSHA contain markings relating to their confidentiality, trade secret, and proprietary nature and should be held by the agency as such. OSHA should place them in a secure section of the file, and not produce them in accordance with any future FOIA requests, information requests, etc., without consulting the undersigned counsel. It is uncertain how the use of smart glasses to capture information would interfere with these important safeguards.

Furthermore, using smart glasses equipped with cameras and live-streaming capabilities would allow inspectors to capture footage of employees **without their knowledge or consent**, raising serious privacy issues. This is especially true when inspectors use the glasses to record video and audio during routine inspections or employee interviews/interactions. These recordings could inadvertently capture sensitive personal data, including conversations, non-work-related activities, or even supposed confidential interactions.

Finally, many states require **two-party consent** for conversations to be recorded. A failure to get all parties' consent to recording a private conversation could constitute a felony in some states. In places where consent must be obtained from both the person sending and receiving the communication, this requirement applies to recordings or active interception of both wire (telephone) and oral (spoken) communications. The use of smart glasses without the consent of the person being recorded may be a potential felony violation in many states.

**What Should Employers Do?**

OSHA has not yet provided any insight or guidelines for how it will deploy or use this new technology. Without proper oversight, businesses and the American workforce have no information for when or

Without proper oversight, businesses and the American workforce have no information for when or how their activities could be captured. This lack of transparency increases the risk of potential abuses, such as the overuse of surveillance, broadening of the scope of an inspection, or the collection of personal data or information.

Until we have more detail from the agency, we recommend employers take the following steps to minimize liability and ensure your rights – and the rights of your workers – are protected:

**Make sure your policies on OSHA inspections contemplate the use of smart glasses before they are implemented for use.** These policies should consider when, where, and how the glasses could be used, and at the very least, ensure that you and your employees have a full understanding about the surveillance capabilities of the device. Obtaining consent before using smart glasses should be necessary before such use.

**If an OSHA inspector requests or simply shows up at an inspection wearing smart glasses, immediately consult with your safety attorney to determine whether and how to restrict the use of recording features.**

- You might be able require inspectors to rely on other traditional methods, such as notes or photographs.
- You should take necessary steps to protect the data captured by smart glasses, ensuring that video footage and images are stored securely, with limited access, and for a set period, to prevent misuse of such data. Additionally, you should be able to restrict the use of data for limited in-scope compliance purposes and not for other unrelated purposes.

**Ensure any information that could be confidential (such as trade secrets or other proprietary data) is protected and held by OSHA as such, regardless of how it is collected.** OSHA should ensure any such information gathered by smart glasses is secured and not produced in accordance with any Freedom of Information Act (FOIA) requests or other information requests without first consulting the employers and employer's counsel.

**Conclusion**

As we expect OSHA's use of smart glasses in workplace inspections to become more widespread, it is crucial for employers to take steps now to protect not only the worksite from unreasonable searches, but also to protect workers' privacy rights. You should understand your rights during an OSHA inspection and contact the author of this insight, any member of the Workplace Safety Practice Group, or your Fisher Phillips attorney for guidance if an inspector shows up wearing smart glasses. And make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information on OSHA issues.

***Related People***

**Patrick W. Dennison**
Partner
412.822.6627
Email

## *Service Focus*

AI, Data, and Analytics

Workplace Safety and Catastrophe Management

## *Trending*

AI Governance Hub