WERKSMANS
ATTORNEYS

DIGITAL MEDIA & ELECTRONIC COMMUNICATIONS

Are your employees' wearables creating a new governance blind spot?

31 August 2026 *9 min read*

by Tebogo Sibidla, Director

Over the past decade, organisations have invested heavily in securing workplace technology. Laptops, smartphones, cloud applications and enterprise networks are now subject to a range of security controls, including device management, multi-factor authentication and acceptable use policies. Wearable technology has, however, received far less attention. The latest generation of AI-enabled smart glasses, earbuds, watches and rings can receive confidential communications, analyse documents, authenticate users, record conversations and synchronise with cloud platforms. As these capabilities mature, organisations must decide whether wearables should still be viewed as personal accessories, or whether they have become another channel through which corporate information is accessed, processed and transmitted.

Wearables are no longer merely personal accessories

Wearables are electronic devices that can be worn on or attached to the human body. According to the IDC's Worldwide Wearable Device Tracker, global wearable-device shipments totaled 145.7 million units in Q1 2026, an increase of 4.3% year-on-year.

Wearables, once associated mainly with fitness tracking, have become embedded in daily personal and professional life. Unlike laptops and smartphones, they are not always perceived as part of an organisation's technology environment. Employees purchase them, wear them throughout the day, and design choices ensure they blend into ordinary clothing. Their familiarity masks their significance.

The change lies not only in what these devices do, but in how they operate. Earlier generations of wearables performed narrow, user-initiated tasks. Newer devices run continuously and with greater independence from the wearer. Interactions can occur through voice commands, gestures, visual prompts or automated sensing, without the wearer opening an application. A smartwatch connected to Outlook or Teams may provide almost immediate access to sensitive commercial information (emails, messages and calendar entries) without the employee touching a laptop. Smart glasses can capture photographs, video and audio, live stream, translate and interact with an AI assistant, all while resembling ordinary eyewear.

What matters most is the combination of capabilities these devices now contain. A device worn on the wrist or face may combine a camera, microphone, biometric sensors, location tracking, wireless connectivity, cloud synchronisation and AI-powered processing. It can collect information about the wearer, their colleagues, clients and the organisation, sometimes in the background, without any deliberate action by the wearer.

Many organisational controls still rely on familiar categories. Laptops are managed as workplace devices, smartphones fall under mobile-device controls, and cloud applications are assessed as third-party services. A watch, ring, pair of glasses or set of earbuds may not fit comfortably within any of these categories, even where their capabilities overlap with all three.

This creates a widening gap between how wearables are perceived and the role they actually play. Organisations should therefore consider whether their cybersecurity, information-governance and AI-governance frameworks adequately address the information these devices can access, capture, process, store and transmit.

Wearables may already be connected—even if the organisation has not approved them

Many organisational technology controls depend on visibility. Organisations know which laptops and smartphones they have issued, which personal devices have been authorised, and what security requirements apply. Procurement processes, minimum security standards, patch management requirements and device management controls are built around that visibility. Many organisations have detailed Bring Your Own Device (BYOD) policies governing personal smartphones, but those policies were drafted with smartphones in mind, not always-on, AI-enabled wearables that enter boardrooms and trading floors as unremarkable accessories.

A privately acquired wearable can bypass approval processes entirely. Employees may purchase and configure devices, install companion applications, connect to cloud services and synchronise with business applications, often without IT, information-security or legal involvement.

The connection does not necessarily have to be direct. A wearable may interact with corporate information through a paired smartphone, a companion application or a cloud-based account, without ever connecting to the corporate network independently. Its absence from the organisation's inventory of devices therefore does not mean that it lacks access to workplace information.

An organisation may have secured its conventional workplace devices while inadvertently overlooking an entire layer of personally owned unmanaged wearables capable of interacting with corporate systems.

Corporate information may be exposed without anyone pressing "send"

Modern wearables can display email previews, messaging notifications, calendar appointments, authentication requests and other business communications. Sensitive information can become visible in circumstances not contemplated when those communications were sent.

A smartwatch displaying the subject line of a confidential merger within the view of a nearby passenger on a flight, or an executive's smart glasses inadvertently recording a board meeting, illustrates the risks.

These risks do not depend on dishonesty or deliberate disclosure. They may arise from default device settings, automated functions, or a failure to appreciate how the device receives, displays and records information.

Wearables may expand the organisation's cybersecurity attack surface

Wearables present cybersecurity risks beyond inadvertent disclosure of confidential information. Many devices communicate with smartphones, laptops, companion applications and cloud platforms, creating multiple pathways for information to flow. Depending on the device and its configuration, these connections may use Bluetooth, Wi-Fi or other wireless protocols.

The risk is not that every wearable is inherently insecure, but that each introduces additional software, credentials, connections and third-party services into the organisation's environment. This expands the attack surface, the number of potential entry points through which systems or data could be compromised. Vulnerabilities may arise from outdated firmware, insecure device pairing, excessive application permissions, compromised cloud accounts or weaknesses in companion applications.

Physical connections create additional exposure. Where wearables or their accessories connect to laptops or desktops via USB for charging, synchronisation, firmware updates or data transfer, a compromised device could introduce malware or enable confidential information to be copied outside the organisation's usual security controls.

Following a cybersecurity incident, regulators, insurers and litigants may ask whether the organisation's security measures addressed all connected technologies capable of interacting with its systems.

AI-enabled wearables may fall outside existing AI governance controls

Several wearables now incorporate AI assistants that can summarise conversations, answer questions, draft messages and interact with business information through natural language. An employee might ask a wearable to summarise a confidential meeting or draft a response to a client.

The interaction feels different from opening a generative AI platform on a laptop and deliberately entering a prompt. A voice command during a meeting may seem like an ordinary interaction with a personal device, even though it could result in confidential or personal information being captured, transmitted and processed by an external AI service.

Organisations should ask whether confidential information is being processed by third-party AI providers; whether personal information is being transferred across borders; whether recordings, prompts or outputs are retained to train AI models; and whether their AI governance framework extends to wearables.

These issues are already surfacing in litigation. In the United States, AI-enabled smart glasses already the subject of lawsuits concerning data collection and processing practices. The allegations remain untested, but the dispute illustrates how the operation of AI-enabled wearables can create legal exposure extending beyond the individual wearer.

The technology may be new, but the legal duties are not

Legal obligations attach to the information processed, the conduct involved and the risks created—not the form of the device.

Where wearables collect or process personal information, the Protection of Personal Information Act, 2013 (POPIA) may apply. s19 requires responsible parties to implement appropriate, reasonable technical and organisational measures, identify reasonably foreseeable internal and external risks, and maintain appropriate safeguards. A device does not fall outside these requirements merely because it is personally owned.

The exposure, recording or external processing of business information through a wearable could breach employment confidentiality duties, NDAs, trade secret obligations or sector-specific requirements. Where communications with legal advisers are captured, organisations should consider the effect on legal professional privilege.

Directors remain bound by duties of care, skill and diligence reasonably expected of them. Although the Companies Act, 2008 does not prescribe controls for wearables, emerging technology risks may form part of the broader risk-governance matters warranting board oversight.

The organisation's response to wearables must, however, also respect employees' rights. Restrictions on personal devices, workplace monitoring and access to information collected by wearables should be proportionate, transparent and consistent with applicable privacy, employment and interception laws.

Governance should follow capability, not the label on the device

The appropriate response is not necessarily to ban wearables or draft a standalone wearables policy. Organisations should instead assess whether their existing cybersecurity, BYOD, acceptable use, confidentiality, AI-governance and incident-response frameworks address the capabilities of these devices and the circumstances in which they are used.

As part of that assessment, organisations should consider:

- Which wearables are being used in the workplace, and what are they capable of doing?
- May personal wearables interact, directly or indirectly, with corporate systems or display confidential communications?
- May camera- or microphone-enabled devices be used during confidential meetings or in sensitive areas?
- Do AI-governance and recording policies address functions such as live transcription, meeting summarisation, image analysis and contextual assistance?
- Do network-access and device-management controls adequately address wearable technology?
- Do recruitment and assessment protocols address candidates' use of AI-enabled wearables?
- If information were captured, disclosed or compromised through a wearable, could the organisation's incident-response processes identify, investigate and contain the incident?
- Is responsibility for wearable-related risks clearly allocated among IT, information security, legal, privacy and human-resources teams?

For many organisations, the answers may not be clear, not because they have chosen to accept the risks, but because their policies were written with laptops and smartphones in mind.

Any response should be proportionate to the device's capabilities and the environment in which it is used. Some organisations may need to prohibit particular functions or devices in sensitive areas, while others may manage risks through configuration requirements, access restrictions and policy updates. Medical and accessibility needs must be accommodated.

Closing the governance blind spot

Wearables can no longer be excluded from organisational governance by default. Organisations should consider whether their existing frameworks govern the technology employees actually use, rather than only technology formally issued or approved.

The governance blind spot arises not from the device itself, but from policies and controls that fail to evolve as device capabilities do. Addressing the issue now enables proportionate safeguards and clear employee guidance before an unmanaged device becomes relevant to a confidentiality or cybersecurity incident.

Tebogo Sibidla

Director

View Profile