THE UNIVERSITY OF SYDNEY

Governing Immersive Tech Rapid Analysis: Smart Glasses in New South Wales 2026

Data privacy

Smart glasses combine cameras, microphones and, increasingly, AI functions in devices designed to appear like ordinary glasses. The data they capture can include faces, voices, movements, interactions and locations of the wearer and those around them. This data can be used to distinguish, track and profile a person without establishing their name or legal identity, including by linking the same person across multiple recordings and datasets. For example, the I-XRAY project demonstrated how Meta smart glasses can be combined with existing facial-search and AI tools to match people captured by the glasses with information available online.

A single recording can also reveal sensitive information about a person—for example, that they were at a medical clinic, domestic violence service, protest or religious institution.

These issues concern how personal information captured through smart glasses is collected, identified, combined, analysed, used and disclosed. They are principally data privacy issues addressed through Commonwealth privacy law.

Recording privacy

Australia's statutory tort for serious invasions of privacy covers intentional or reckless intrusion such as watching, listening to or recording someone's private activities or affairs, if that person had a reasonable expectation of privacy. This makes sense for many privacy harms — being secretly recorded in your home, or having intimate images shared without your consent, for example. It does not, however, address the privacy problem created by smart glasses and other wearable devices that make it possible to covertly target and record people in public and semi-public spaces.

Research shows smart glasses are being used to record people in building foyers, shops, gyms, workplaces, on campuses, at beaches and parks, and on the street. These are places where there may be little or no expectation of privacy — places where people expect to be seen by others. But that doesn't mean people expect, or accept, that strangers can secretly record them and upload the footage to social media. That is a different type of intrusion that smart glasses are designed to facilitate.

A person at Bondi Beach, sitting in a café or travelling on a train expects to be seen by other people. That does not necessarily mean they expect another person to deliberately target and continuously record them, capturing their face, voice, movements and location, and potentially publish that recording online.

Wearable device providers, including Meta Platforms, have relied on indicator lights to signal when a device is recording. But an LED can be circumvented, difficult to see and, either way, notice is not consent.

Without proper regulation, smart glasses risk creating a society in which simply being in public means anyone can be recorded at any time, without their knowledge and with no control over how those recordings—or the information they capture—are used.

What NSW law already covers

The Surveillance Devices Act 2007 (NSW) regulates listening, optical, tracking and data-surveillance devices. It restricts the recording of private conversations using listening devices and the communication or publication of information obtained through unlawful surveillance. However, s 7(2)(c) provides an exception for the unintentional hearing of a private conversation by means of a listening device**.** Smart glasses, which can continuously or readily capture surrounding audio, may therefore challenge existing distinctions between intentional and unintentional listening and recording, as well as assumptions about when a conversation is private and when recording is consensual.

The Act's restrictions on optical surveillance are more limited. They principally apply where use of an optical surveillance device involves unauthorised entry onto premises or a vehicle, or interference with a vehicle or other object. The Act also expressly excludes an optical surveillance device from its definition of a "data surveillance device", which is defined as a device or program capable of recording or monitoring the input of information into, or output of information from, a computer.

The Crimes Act 1900 (NSW) provides additional protections against voyeurism and non-consensual intimate recording. The Workplace Surveillance Act 2005 (NSW) separately regulates surveillance of employees, including notification and visibility requirements for camera surveillance.

Together, these laws provide protections in specific circumstances, including private conversations, intimate imagery, voyeurism and workplace surveillance. They do not, however, establish a general prohibition on deliberately recording another person without their consent in a public or semi-public place, nor a general prohibition on publishing or distributing such a recording.

Question for NSW lawmakers

Do NSW's surveillance and criminal laws adequately protect people from being deliberately targeted and recorded by wearable devices in public and semi-public spaces?

About us

This is a Governing Immersive Tech report authored by Joanne E. Gray, Ben Egliston, Marcus Carter, Georgia Samuel, Milica Stilinovic and Wenqi Tan.

The Governing Immersive Tech Project is an Australian Research Council funded Discovery Project (DP250100343) developing frameworks for the public-interest governance of immersive and other emerging technologies. Our mission is to support proactive governance, not damage control.

Projectgit.com.au

Contact

j.gray@sydney.edu.au

sydney.edu.au

CRICOS 0026A

THE UNIVERSITY OF SYDNEY