Smart Glasses: A study outlining implications for public sector organisations

THE UNIVERSITY OF SYDNEY

Centre for AI, Trust and Governance

Table of Contents

Research Question

Using the University of Sydney as a case study, what are the implications for public sector organisations in responding to the use of smart glasses and other AI-enabled wearable recording devices on campus? In particular, how should legal, policy, and ethical frameworks be applied to manage issues of privacy, consent, academic integrity, and safety?

Authors:

Jacky Zeng
Professor Kimberlee Weatherall
Professor Kalervo Gulson

We would like to acknowledge the contributions of Deborah Hook, Anita Kelly, Alexia Trani, and Tze Jie Yong to this paper.

10 February 2026

Recommended Citation
Zeng, J., Weatherall, K., & Gulson, K. (2026). *Smart Glasses: A study outlining implications for public sector organisations.* The University of Sydney.
https://doi.org/10.25910/qffx-cj68

On Social Media
Please use the report url: **https://hdl.handle.net/2123/34844** plus **sydney.edu.au/arts/ai-trust-governance**

Executive Summary

Smart Glasses are a technology which has seen rapid development in recent years – evolving from niche gadgets to functional technology. Leading products today enable the user to capture – and subsequently distribute – audio, video, geolocation etc., in a hands-free and discreet manner. In the context of the University of Sydney (the University), the use of Smart Glasses by people on campus grounds (mostly, students and visitors) raises or exacerbates concerns related to safety, privacy, copyright and academic integrity.

This can trigger legal issues. Recording may implicate privacy-related laws: surveillance devices and privacy legislation can require consent (from all parties) for recording. As a rule, however, consent is only required where there is a reasonable expectation of privacy. The use of Smart Glasses in classrooms can trigger copyright regulations – which prohibit the use of lecture materials beyond personal use. Most obviously, use in examinations would contravene the University's policy on academic integrity. Smart Glasses may also amplify downstream malicious activity such as stalking and doxxing, as well as cyberbullying and harassment, for which there are strict prohibitions in both the law and University policies.

On the other hand, any responses need to take into account accessibility enhancements that Smart Glasses can offer for people with disabilities.

As we discuss below, there are some gaps and ambiguities between existing safeguards and potential harms. A combination of explicit policy and/or education may help promote safety and respect on University campuses.

Our **six recommendations** are**:**

- **Recommendation 1:** The University should consider its stance on the use of Smart Glasses in semi-public areas on campus e.g. Eastern Ave in consultation with stakeholders (students, staff and management) and groups already engaged with the University's policies on bullying, harassment, and campus safety (Section 4.1).
- **Recommendation 2:** The University should consider its stance on the use of facial recognition technology (FRT) in Smart Glasses (Section 4.1).
- **Recommendation 3:** The University should consider what 'adequate consent' means in the Smart Glasses context (Section 4.2). Consideration should be given as to whether specific guidance or communications are required.
- **Recommendation 4:** The University should consider what may constitute 'private circumstances' on University campuses (Section 4.2). Consideration should be given as to whether specific guidance or communications are required.
- **Recommendation 5:** The University should give due consideration to the practical and organisational factors including (but not limited to): avenues for redress, clear internal processes and procedures, training and awareness, and consequences for offenders. (Section 4.3)
- **Recommendation 6:** The University needs to consider the possibility of Smart Glasses being used by some students for accessibility purposes, and how equity issues interact with the key policy questions noted above.

Introduction

Smart Glasses are a technology which has seen rapid development in recent years: evolving from niche gadgets to functional technology. Leading products today are discreet, wearable devices that offer a range of visual, auditory, and AI-assisted features to capture, communicate, and process information. A key draw for users is the seamless access to digital technology: most Smart Glasses enable users to record video, receive directions and listen to music in a hands-free manner without the need to pull out a phone. Smart Glasses have also shown promise as assistive technology, primarily for individuals with visual impairments who can benefit from the Smart Glasses' ability to convert visual features to audio.[1] Popular models can generally be purchased for less than $1,000, making the technology an accessible consumer product.

While similar to smart phones in function, Smart Glasses are distinct due to their covert appearance. They look like normal glasses. This means that individuals may be able to record interactions and access information without other people being aware, and in scenarios which are outside everyday expectations. In the context of a University like the University of Sydney, the use of Smart Glasses raises various concerns related to safety, privacy, copyright and academic integrity.

University campuses are private property, but in practice operate like open spaces which students, staff, visitors, tourists, and members of the general public are usually welcome. It is important for the University to navigate these blurred boundaries consciously and ensure that its campuses remain a place where students and staff feel safe and academic excellence is upheld.

This whitepaper takes the University of Sydney as a case study, but the issues explored are likely to be broadly applicable to other semi-public areas where there are blurred boundaries between private and public property, and where many individuals may pass through or congregate. Examples may include other educational institutions but also stadiums, shopping malls, some government buildings, and public transport.

Scope

This whitepaper examines the implications for the University in responding to the use of smart glasses on campus. In particular, the scope of the paper focuses on **the use of Smart Glasses by 'people' on University campus grounds (mostly, students and visitors)**.

We (1) explore the function of Smart Glasses (2) discuss key risks relevant to the University (3) consider the application of existing legal and policy frameworks; and (4) identify key gaps and uncertainties where the University should consider action.

The implications of University staff using Smart Glasses during their core teaching and research functions are out of scope. Use in those contexts is a complicated issue in its own right, raising distinct concerns related to workplace surveillance, research confidentiality and enterprise privacy and security.

---

[1] Victoria Song, **'The strongest argument for smart glasses is accessibility'**, *The Verge* (Web Page, 20 September 2025).

1. About the technology

We define Smart Glasses as: *a wearable device which is designed to resemble eyewear that is capable of capturing, processing and outputting data.*

Smart Glasses are wearable devices which may utilise speakers, microphones, cameras and head-up displays (HUD) to enable users to access and interact with information while seeing the world around them through the lens. Smart Glasses are intentionally designed to look like everyday eyewear. In this sense, they are distinct from other augmented reality products (e.g. Apple Vision Pro) which offer similar visual functionalities but are much more obvious.

'Smart glasses' can also refer to glasses with only inbuilt speakers or sunglasses where the users can manually adjust the tint.[2] Such devices are not relevant to the discussion below to the extent that they only output information.

1.1 Core Features

The core features available in flagship Smart Glasses include:[3]

- Display of texts and notifications in HUD;
- Hands-free photo and video capture. Many products will signal active recording using a LED indicator, however, there are cheap accessories which may bypass this mechanism;[4]
- Receiving navigation directions;
- Listening to audio such as music and podcasts;
- Taking phone calls and video calls;
- Livestreaming video to Facebook or Instagram;
- Accessibility support via integration with Be My Eyes enables blind or low-vision users to connect with sighted volunteers for guidance in daily tasks; and
- Interacting with AI-enabled features such as translation, captions, local search, Live AI and AI assistants.

[2] See e.g. **Ampere Dusk Smart Glasses**.
[3] These features have been based on the **Meta Ray-Ban Display glasses** (limited release in the US, i.e. not in the Australian market yet). Not all Smart Glasses in the market will have all of these functionalities. E.g., **products from Even Realities** do not have a camera and are unable to take photos or record video. Similarly, not all devices will have easy access to AI assistants.
[4] See e.g. **products available on Amazon**.

A list of Smart Glasses on the market is noted below:

Product	***Camera***	***Display***	***Audio***	***AI-assistance***
Meta Ray-Ban Display **(announced but not released in Australia)**[5]	Y	Y	Y	Y
Oakley Meta Vanguard	Y	N	Y	Y
Oakley Meta HSTN	Y	N	Y	Y
Meta Ray-Ban Glasses (Gen 1 and 2)	Y	N	Y	Y
Even Realities G1 and G2	N	Y	Y	Y
Viture Luma Pro	Y	Y	Y	-
XReal One Pro	Y	Y	Y	-
XReal One	Y	Y	Y	-
XReal Air 2 Pro	Y	Y	Y	-

1.2 Data flow

Smart Glasses are not standalone devices, but rather extensions of the user's smartphone.[6] This connectivity is key for the majority of features Smart Glasses offer, where the phone is the core processing engine and the glasses act as an additional input and output device.

Overall, Smart Glasses enable the user to capture a broad range of information: audio, video, geolocation etc. which is transferred and stored to the user's personal phone. Some of this information may be collected by the companies who provide platform and data processing services.

Smart Glasses by Ray-Ban Meta, for example, function by connecting to the Meta AI app on the user's phone. Pictures and videos captured by the glasses are temporarily stored on device, transferred to the app cache, and then automatically synced to the Meta AI app for viewing and editing. Certain features such as translation need to be initiated from the Meta AI app. Other features, such as using the glasses to send a photo, may require user content to be uploaded to Meta cloud servers where it is temporarily stored.[7]

Ray-Ban Meta Smart Glasses are also subject to Meta's Supplemental Meta Platforms Technologies Privacy Policy and Privacy Policy which indicate that Meta collects and stores a wide range of information collected from the glasses and wrist devices and the Meta AI companion app.[8]

---

[5] As at 6 Jan 2026.
[6] '**How it works: the tech behind AI glasses'**, *Even Realities* (Web Page, November 2025).
[7] **'Learn more about cloud media on AI glasses'**, *Meta Help Centre* (Web Page); '**How media storage works with AI glasses and the Meta AI mobile app'**, *Meta Help Centre* (Web Page).
[8] **'Control what information you share with Meta on your AI glasses and wrist devices'**, *Meta Help Centre* (Web Page).

2. Key risks

This section explores the various risks which may arise from the use of Smart Glasses on University campus grounds including risks related to safety, privacy, copyright and academic integrity.

2.1 Privacy, harassment, and cyberbullying

Smart Glasses could be used on campus to covertly film interactions with students, staff, or visitors without their knowledge or consent.

This alone is sufficient to raise privacy and surveillance concerns for the individuals being recorded, especially if the nature of interactions or location of recording are of a private or sensitive nature (e.g. in confidential meetings or bathrooms). The discreet appearance of the device, and the fact that individuals may not be aware of filming raise questions as to when it is possible to infer consent to any filming: in this sense Smart Glasses are different to mobile phones, where the act of filming is generally more obvious, even at a distance.

Recordings may be posted to online platforms leading to potential breaches of confidentiality, public harassment, and cyberbullying of subjects. For example, an American content creator using Smart Glasses has faced backlash for secretly filming interactions where he attempted to 'pick up' women in streets and shops and on beaches in Sydney. The videos were later uploaded to Instagram and TikTok. Victims were subject to "horrific comments" on social media, with some feeling that the conduct was "violating and disgusting".[9]

2.2 Facial Recognition Technology

A particularly sensitive use of Smart Glasses involves the use of facial recognition technology (FRT) – where images or videos can be used to identify and profile individuals. The discreet nature of Smart Glasses lowers the barrier for people who might want to misuse FRT to identify strangers on campus. It also makes such actions harder to detect and protect against.

Further, Smart Glasses may also be integrated with FRT to covertly identify individuals in real-time. Two Harvard students demonstrated a system pairing Ray-Ban Meta Smart Glasses with a publicly available facial recognition computer program to identify individuals from public databases real time, revealing names, addresses, phone numbers, and relatives.[10]

The malicious use of this technology could enable serious downstream threats such as stalking and doxxing. More generally, capabilities like these threaten students' and staffs' feelings of safety on campus.

---

[9] Chantelle Al-Khouri, **'US content creator secretly filmed Sydney women with covert sunglasses camera lens'**, *ABC News* (Web Page, 25 March 2025).
[10] Lindsey Choo, **'How 2 Students Used The Meta Ray-Bans To Access Personal Information'**, *Forbes* (Web Page, 4 October 2024). According to media reports, the students involved left university to pursue plans for Smart Glasses that would record and transcribe conversations of the user.

2.3 Secondary data use

Smart Glasses rely on external systems to process and provide most of their features. This means that the data collected by Smart Glasses is processed by companies who may separately collect and store this information for other purposes. For example, data captured by Ray-Ban Meta glasses including audio, video, location data, meta data, may be used by Meta to 'personalise' (i.e. profile) the user and used to train Meta AI models.[11]

While the *wearer* of Smart Glasses may have 'consented' to these terms (albeit perhaps without reading them), the individuals being recorded most likely have not. This raises concerns regarding the unauthorised use of sensitive (biometric) data, as well downstream risks of exposure when such information is stored and has been used to train publicly available AI models.

There may also be inadvertent data surveillance where Smart Glasses are unintentionally triggered by a 'wake word' or other means. For the Ray-Ban Meta glasses, these interactions (including metadata including hardware details, audio length, and text transcripts) are processed by Meta's systems. Misactivations, labelled as "false wakes" are retained for up to 90 days before deletion.[12] This creates a risk of continuous, passive surveillance in campus environments.

2.4 Academic integrity

Smart Glasses could be worn by students to cheat in exams. In one case, an 18-year-old student used camera-equipped Smart Glasses to photograph test questions during Waseda University entrance exams, sending them to his phone and sourcing answers from others online.[13]

Similarly, Smart Glasses could be used to record a fellow student's notes without their knowledge or consent.

2.5 Copyright and intellectual property

Smart Glasses may be worn by students to record lectures and other material which may be subject to intellectual property and copyright restrictions: without the controls that apply to officially sanctioned and managed recordings.

[11] Meta, ***Supplemental Meta Platforms Technologies Privacy Policy*** (November 2025).
[12] Meta, ***AI Glasses Voice Privacy Notice*** (22 July 2025).
[13] Arata Mitsui, **'Teenager tells police he cheated on exam with smart glasses'** (Web Page, 15 May 2024).

3. Application of key laws and University of Sydney policies

The section discusses the application of key laws and University policies on the use of Smart Glasses on campus. The goal here is to clarify how existing frameworks may address the key risks noted above and assess whether further action is needed.

Overall, existing laws and policies apply where:

- Smart Glasses are used in private circumstances (including private conversations and acts) (Section 3.1);
- material captured is subject to copyright, intellectual property or breach of confidence (Section 3.2); and
- there is serious misuse such as: stalking and doxxing (Section 3.3), and cheating, bullying and harassment (Section 3.4).

We do not expect existing laws and policy to cover all possible risks posed by emerging technology such as Smart Glasses. Rather, they serve as good starting points for understanding the circumstances where Smart Glass use may be harmful, and what relevant mitigations may be appropriate. Potential gaps are explored in Section 4.

3.1 Private circumstances

There are number of laws which may apply to the use of Smart Glass in **private circumstances.** We focus here on laws and policies applicable at the University of Sydney as an example; details may vary state to state, university to university.

Surveillance Devices Act 2007 (NSW)

Under the *Surveillance Devices Act 2007 (NSW)* a person cannot record a **private conversation** unless all parties to the conversation consent.

The Act regulates the use, installation and maintenance of *surveillance devices* – which captures Smart Glasses as devices capable of recording audio and/or visual of a conversation.[14]

A conversation is taken to be private if the circumstances may "*reasonably be taken to indicate that any of those persons desires the words to be listened to only by themselves, or by some other person who has the consent, express or implied, of all of those persons to do so, but does not include a conversation made in any circumstances in which the parties to it ought reasonably to expect that it might be overheard by someone else.*"[15]

[14] Noting here carve out here for devices used by people with visual or audio impairment. See e.g. s 4 definition of 'listening device'.
[15] See s 4 for definition of 'private conversation'.

Policy learning: *For conversations which can be considered private, the recording party (i.e., the wearer of the Smart Glasses) is required to get consent from all parties.*

For example: a conversation between a teacher and student in the teacher's office will likely be considered private.[16] Consent from all parties is needed to record.

The main limitation is that private conservations are only a fraction of interactions which could be recorded on campus. For example, a casual conversation between students on Eastern Avenue (an open space at the University of Sydney) is likely not private and not subject to s7 of the *Surveillance Devices Act 2007 (NSW).*[17] Further, the Act regulates the recording of private *conversations,* which means there must be spoken words (s 4). There may be interactions out of scope which are not conversations, but are still private in nature, carrying similar risks of privacy and harassment.

Tort for the serious invasion of privacy

An individual (plaintiff) may have a cause of action against another person or organisation (defendant) who has invaded their privacy by doing one or more of the following, in **instances where the plaintiff would have had a reasonable expectation of privacy in all the circumstances**: [18]

- intruding upon the individual's seclusion – for example, by physically intruding into their private space;
- misusing information that relates to the plaintiff.

A plaintiff will also be required to demonstrate a number of other factors, including that the public interest in protecting their privacy outweighs any countervailing public interest. The statutory tort was introduced in recent reforms to the Privacy Act and commenced on 10 June 2025.

It is likely that the act of recording could constitute a serious invasion of privacy if other requirements are met. The scope of the tort likely extends beyond private conversations (captured in the *Surveillance Devices Act 2007 (NSW)*) to include other interactions of a private nature*:* for example, recording a student through the window of their dormitory.

Policy learning: *where individuals have a reasonable expectation of privacy, the default position is that you are not allowed to record or misuse (e.g. stream or upload) information related to the person – this may constitute an invasion.*

Again, as with the *Surveillance Devices Act,* there are limitations on the scope of the tort. Interactions recorded in semi-public spaces will not be captured. The statutory tort is also very new and untested. Actual remedies and recourse via litigation may be expensive, slow and burdensome.

---

[16] The location and nature of the conversation are relevant factors. E.g. a doctor's consult in a private room was considered a private conversation; despite the fact it could be overheard from the reception. *Toth v Director of Public Prosecutions (NSW)* [2014] NSWCA 133.
[17] The sole fact that a conversation took place in a busy location where it may be overheard does not mean that it won't be private. A conversation may be private even though it occurs in a public place e.g. restaurant. *Kanjian v Kanjian (No 3)* [2021] NSWSC 839 [477].
[18] Privacy Act 1988 (Cth), Sch 2.

Private acts

Malicious use of Smart Glasses in private circumstances may also trigger criminal offences related to filming private acts without their consent. Under section 91K of the *Crimes Act 1900* (NSW), it is an offence to film private acts including activities such as undressing, using the toilet, showering, or engaging in sexual activities, without consent.

Discussion:
This captures more malicious uses of the technology. The definition of private acts is narrower than the private circumstances mentioned in the tort above. Acts must be one of the specified activities and there must be circumstances such that a reasonable person would reasonably expect to be afforded privacy.[19]

The nature of criminal offences means that enforcement relies on prosecution by the State, which can be a barrier for victims.

Policy learning: *Similar to the tort for serious invasion of privacy, this standard could be used to inform circumstances on campus where Smart Glasses are prohibited/ need to be switched off, so that there is no possibility of recording. For example, Smart Glasses should be switched off before entering bathrooms or change rooms.*

Consent

Whether a party has consented to the recording is key factor in the scenarios above. Here, the Office of the Australian Information Commissioner (OAIC) provides useful guidance.[20]

Consent can be express or implied – i.e. where consent may reasonably be inferred in the circumstances from the conduct of the parties.

The four key elements of consent are:

- the individual is adequately informed before giving consent;
- the individual gives consent voluntarily;
- the consent is current and specific; and
- the individual has the capacity to understand and communicate their consent.

This discussion is relevant to our discussion below in section 4.2.

3.2 Copyright and Intellectual Property

Section 113P of the *Copyright Act 1968 (Cth)* prohibits the unauthorised recording and distribution of lectures or teaching materials. While educational exceptions exist under ss28 and 201A for institutional use of third-party content (e.g. text, images, music, film), these do not extend to student recordings.

Students may rely on the fair dealing exception for research or study under ss40 and 103C, but only where recordings are made for their own research or study. This exception does not apply where:

---

[19] The *Crimes Act 1900 (NSW)*, s91I.
[20] The Office of the Information Commissioner, **'Chapter B: Key Concepts'** (Web Page), definition of 'Consent'.

- the lecturer has explicitly prohibited recordings, rendering surreptitious recording unfair; or
- the material is subsequently distributed, shared, or monetised, including via livestreaming or uploading to third-party platforms (meaning the purpose is no longer the student's own research or study).

University copyright notices reinforce these obligations, warning against reproduction or communication of teaching materials without permission. IP generated by lecturers (e.g. lecture content) is governed by the University's IP policy, and students are bound by the Academic Integrity Policy, which prohibits unauthorised recording and distribution, including uploading materials into generative AI tools.

Copyright issues arise in particular circumstances, namely, in class – where there are lectures or teaching material or in settings where there are confidential research, meetings, or documents. The law here is clear and the University has established pathways and policy. Unlike interactions that happen in general public spaces, in class, students commonly have and visibly use devices. In this context, Smart Glasses may not raise significant additional risks, given it is possible for a student to covertly record a class on their phone, laptop or tablet.

A related concern is breach of confidence, particularly where Smart Glasses are used to record confidential research, meetings, or documents. Dissemination of such material may constitute a breach of general law duties of confidence.

3.3 Stalking and doxxing

Smart Glasses may empower bad actors to engage in stalking – the monitoring or tracking of a person's activities, or residence[21] – and doxxing – the publication of someone's personal information which is aimed to be menacing or harassing towards that individual.[22] These can constitute criminal offences.

While the use of Smart Glasses alone is unlikely constitute a stalking or doxxing offence, the technology provides an increased capacity for individuals to capture personal information – including sensitive biometric information – of others, and identify strangers without their knowledge.

This has the potential to increase the circumstances where stalking and doxxing is possible, generally making it easier for potential bad actors to engage in such misconduct. For example, while the facial recognition example discussed earlier can be replicated with smartphones, the fact that a person can access these functionalities in a hand-frees manner with 'normal' looking glasses that doesn't raise suspicions from others will likely increase its adoption.

Policy learning: *Use of Smart Glasses may result in more complaints and instances of stalking and doxxing.*

[21] The *Crimes (Domestic and Personal Violence) Act 2007*, s13.
[22] Section 474.17C of the *Criminal Code Act 1995*, as introduced by the *Privacy and Other Legislation Amendment Act 2024 (No.128 – 2024)* – **Sch 3**.

3.4 Relevant University Policies

Formal law may apply in limited circumstances: certain recordings or invasions of privacy; more extreme malicious behaviour. But behaviour on university campuses is also governed by University policies. The University of Sydney has a range of policies relevant to use of Smart Glasses.

Academic Integrity Policy

The specific use of Smart Glasses in exams or other assessment will most certainly constitute cheating[23] and a breach of the University's Academic Integrity Policy.[24]

Policy learning: *The University can, through its internal policies make expressly clear that Smart Glasses are prohibited, or prohibited in certain circumstances (such as during any form of assessment).*

For example, The University of Adelaide explicitly prohibits the use of Smart Glasses, Smart watches, and mobile phones during examinations. Any possession of these devices in the exam room is treated as unauthorised material and constitutes a breach of the Academic Integrity Policy, triggering formal misconduct procedures.

Teachers and exam supervisors should be aware of what Smart Glasses may look like to adequately enforce the Academic Integrity Policy.

Cyberbullying and harassment

The University's **Bullying, Harassment and Discrimination Prevention Policy 2015** deals with inappropriate behaviour on campus such as discrimination, harassment, workplace bullying, sexual misconduct and sexual harassment. Intimidating or harassing behaviour is also prohibited under USyd's **Campus Access Policy 2024** (cl 2.4 (1)(g)). We note that some such behaviour may also fall within the remit of the eSafety Commissioner under the *Online Safety Act 2021*.

To the extent that Smart Glasses use involves or leads to inappropriate conduct, these policies present an established pathway for students or staff to seek redress, and for harms to be mitigated.[25]

For example, a student who repeatedly uses Smart Glasses to film and post embarrassing videos of another student on social media without their consent may be engaging in harassment and cyberbullying. There are various ways for the victim to report this behaviour to relevant University entities.[26] This has potential to cover a broad scope of actions by the Smart Glasses wearer – i.e. not just private interactions.

However, there are limitations, similar to our comments above regarding stalking and doxxing. Harassment and bullying are downstream and contextual behaviours and cannot be solely relied on to govern Smart Glasses misuse. The University could see an influx of complaints and conflicts if the technology becomes increasingly common.

---

[23] https://www.sydney.edu.au/students/academic-integrity/breaches.html.
[24] https://www.sydney.edu.au/policies/showdoc.aspx?recnum=PDOC2012/254&RendNum=0.
[25] See e.g. **Bullying, Harassment and Discrimination Resolution Procedures.**
[26] See **'Bully, Harassment and Discrimination'**, *The University of* Sydney (Web Page).

Campus Access Policy

USyd's Campus Access Policy 2024 sets out the expected standard of behaviour on university campus for anyone who enters University land. Potentially relevant sections include:

- Section 2.1(1)(a) contains a broad commitment to uphold respect for people, privacy and property.
- Section 2.4 (1)(g) which prohibits intimidating or harassing behaviour, such as continuing to engage with a user after they make clear that the contact is unwanted.

Special locations

Specific locations may have their own restrictions on filming, streaming or publishing content. For example. The *Chau Chak Wing Museum Collections Guidelines* (Version 6, February 2023) s 4.7.4: note that any commercial recording within the museum must be requested.

3.5 Do privacy laws apply?

Australia has privacy laws on both the state and federal level, neither of which are likely to apply to activities within the scope of this paper. The laws which are potentially relevant to the University are:

- the *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act) which regulates the handling of personal information for NSW public sector agencies; and
- the *Privacy Act 1988 (Cth)* which regulates the handling of personal information for federal agencies and businesses (other than small businesses).

Both Acts provide a set of flexible and technology-neutral principles which govern how data about individuals is collected, used and retained. The obligations in both Acts are largely equivalent, and they differ mainly in the scope of entities captured.

The University of Sydney is a NSW statutory body which is subject to the PPIP Act. This means that should the University permit the use of Smart Glasses by its employees – e.g. admin or teaching staff – it will need to consider whether such use is consistent with the privacy principles contained in the PPIP Act and what mitigations will need to be in place address potential privacy risks. A Privacy Impact Assessment is a tool which can help with this process. However, as noted above, this scenario is beyond the scope of this paper, which instead focuses on the use of Smart Glasses by visitors or students on campus grounds. In the latter case, the PPIP Act does not apply as its scope is focused on public sector agencies and not individuals.

Similarly, the majority of obligations under the *Privacy Act 1988 (Cth)* are only applicable to **APP entities** defined with the intention of capturing businesses. Small businesses with an annual turnover $3 million are expressly carved out of the Act. The federal Act is also unlikely to apply to individuals in the scenarios considered by this paper.[27]

[27] Note here that there may be exceptions where privacy laws may apply to individuals e.g. when handling health information – but these are defined quite strictly.

4. Key Gaps/Uncertainties

Consider the following scenario:

Scenario
Two University of Sydney students (Molly and Jill) are walking along Eastern Ave, a large pedestrian space on Campus, after class when they are approached by a fellow student, Sam, who starts a conversation. The trio attend the same class, although Sam has never spoken to Jill or Molly. As conversation starters, Sam mentions Molly's local church and Jill's high school; he follows this up with some flirtatious remarks. During the course of the conversation, Molly notices that a red LED light is blinking from Sam's glasses.

Molly asks Sam if he is recording via his Smart Glasses, and expressly objects to being recorded. She requests that Sam delete the recording of the conversation. Sam responds that they are on a public walkway, and he has a right to record. The conversation ends shortly after and Sam walks away. Molly is anxious at what Sam may do with the footage.

Later, Molly is disgusted to discover that her interaction with Sam has been posted on Instagram as part of a video titled '*Chatting up single Christian girls on campus'*. In addition to the recording, the video shows the process of Sam 'game-planning' for the interaction by utilising FRT on photos of Molly and Jill he covertly took via his Smart Glasses earlier in the class. This helped Sam identify the personal information he used in the conversation.

However, Sam has misidentified Jill (a devout Buddhist) as Christian. This has led to Jill receiving significant amounts of negative comments and spam from her local community online.

4.1 Public spaces and FRT

The above scenario highlights gaps – or at least uncertainties – in the existing law and rules when: (1) Smart Glasses are used to film individuals in semi-public spaces; and (2) there is use of FRT.

Despite obvious harm to Molly and Jill, there are not many laws or rules which clearly apply to Sam's actions:

- Eastern Ave is an open space where there are low reasonable expectations of privacy. It is uncertain whether conversations held on Eastern Ave are likely to be considered sufficiently private to be subject to the rules related to surveillance and invasion of privacy noted in Section 3.1.
- It is unclear whether Sam's one-off actions would be characterised as stalking or carry the intent required for doxxing. These are criminal offences which have a high evidentiary burden.
- Similarly, it is unclear whether posting the interaction online constitutes bullying or harassment. For example, the earlier example of the TikTok creator posting his 'pick-up' interaction with women was reported by victims for harassment to no avail. Many of the videos remain online today. [28]
- The use of FRT is another example where existing laws are lacking in their application to emerging technology. Commentators have long called out the sensitivity of facial data and risk to human rights posed by the misuse of FRT.[29] In Australia, the main applicable legislation to the uses of FRT is the *Privacy Act 1988 (Cth).* However, as discussed, the Act is unlikely to apply to individuals, and even if applied, leaves many uses of FRT unregulated.[30]

When it comes to the use of Smart Glasses in semi-public areas, or in relation with FRT, the University has **an opportunity to progress rules and set norms and expectations that address emerging harms.** Campus grounds are private property which provides an enforceable mechanism for the University to set conditions of entry which are beyond the baseline of existing law.

However, consideration of such measures will need to take into account instances where further restrictions may inhibit free speech. The University needs to consider whether mitigations may be used as mechanisms to censor or suppress videos e.g. of a protest or instances where there is broader public interest.

[28] Above n 7.
[29] See e.g. Nick Davis, Lauren Perry, Ed Santow, '**Facial Recognition Technology: Towards a model law, Human Technology Institute'** (2022), The University of Technology Sydney.
[30] Ibid, p 35.

Recommendation 1
The Univeresity should consider its stance on the use of Smart Glasses in semi-public areas on campus e.g. Eastern Ave in consultation with stakeholders (students, staff and management) and groups already engaged with the University's policies on bullying, harassment, and campus safety.

A strong argument can be made that consent from all parties should be required even in public spaces (see also **Recommendation 3** on consent). While not directly applicable, the *Privacy Act 1988* provides some backing for this position. Recording of individuals will certainly capture biometric information – a subset of sensitive information. The handling of sensitive information requires consent from the individuals (subject to exceptions). This needs to be balanced with issues regarding free speech.

Recommendation 2
The University should consider its stance on the use of FRT in Smart Glasses.

- A general prohibition could be considered. This is because there is unlikely a legitimate reason for individuals to use FRT in the Smart Glasses context. This contrasts with the serious risks to privacy for University students and staff who may be subject to real-time identification and profiling.
- A broader assessment of FRT in the University is needed to assess risks beyond the Smart Glasses context.

4.2 Clarity on existing laws

What is consent?

Consider these questions which arise from the above scenario:

Scenario questions

- If instead, Molly noticed the flashing LED but **remained silent,** is that sufficient for Sam to infer consent?
- How does that change if Sam uses stickers to block the LED so that he can record without people seeing the LED?
- If instead, Sam wanted to record a clearly private conversation which requires consent, what information should he provide?

The discreet design of Smart Glasses makes it harder for individuals to detect when they are being filmed, potentially challenging what adequate consent means. Confronting a person about their recording is socially awkward. In a scenario like this one, it could be natural for some people, for personal and/or cultural reasons, to

avoid discomfort or even out of fear of a bigger, stronger individual, to seek to avoid conflict and/or confrontation by not challenging use.

Recommendation 3
The University should consider what 'consent' means in the Smart Glasses context. Consideration should be given as to whether specific guidance or communications are required. Key factors to consider include:

- **Taking acquiescing as implied consent:** the OAIC notes that it should not be assumed that an individual has given consent on the basis alone that they did not object to a proposal to handle personal information in a particular way.
- **Adequate information:** individuals should be clearly informed about how their personal information will be handled. This should generally include the purpose of collection, and the individual's rights to access and correct information.
- **Express consent:** generally, when handling sensitive information (including biometric information), express consent should be sought.

When is there a reasonable expectation of privacy?

Establishing that there is a reasonable expectation of privacy in the circumstances is the key factor in the application of laws discussed in Section 3.1. However, the concept is tackled by different legal regimes and the circumstances which are captured may vary. Notably:

- The *Surveillance Devices Act* – relates to private conversations between two or more parties;
- The tort for serious invasion of privacy – relates to an intrusion where someone would have had a reasonable expectation of privacy in all circumstances; and
- Private acts – relates to acts of an intimate or sexual nature.

Scenario questions
What if, instead, Sam, Molly and Jill discussed how Jill has been struggling with the recent death of her father – a deeply sensitive and vulnerable topic. Does that constitute a private conservation under the *Surveillance Devices Act*?

Recommendation 4
The University should consider what may constitute private circumstances on campuses relevant to Smart Glasses. Consideration should be given as to whether specific guidance or communications are required.

For example:

- **Private conversation:** a conversation between a teacher and student in the former's office – *consent is required*;
- **Tort:** filming someone in their dormitory or car – *prohibited;* and
- **Private acts:** undressing, using the toilet, showering, or engaging in sexual activities – *prohibited*.

These factors could also inform locations where Smart Glasses need to be switched off – e.g. bathrooms, changerooms, colleges, faculty rooms etc.

4.3 Practical, non-legal factors

There are a number of practical and organisational factors which may arise from the legal considerations above. Assuming that the University comes to a clear policy position on Smart Glasses, what other measures are needed in ensuring that policies are implemented and that students and staff feel safe on campus?

Some key considerations include ensuring:

- **There are avenues to seek redress** when policy has been breached. E.g. can academics, students, or others legitimately ask a person to turn devices off? What are the paths of escalation if a person refuses? How accessible are these pathways for the average student? Can an individual request that content be taken down from social media?
- **There are clear internal processes and procedures**: How do these emerging risks integrate into existing procedures? Which unit should have oversight (e.g. campus security vs student affairs)? How ready are staff to address questions?
- **Training and awareness for both students and staff** – including complaints handling staff – to ensure that they are adequately versed with the various Smart Glasses related risks – and exam supervisors – to ensure that exams or other assessments can be monitored for attempted cheating.
- **Clarity on consequences for offenders** – what penalties/ consequences may offenders face?

Recommendation 5
Give due consideration to the practical and organisational factors including (but not limited to): avenues to redress, clear internal processes and procedures, training and awareness, and consequence of offence.

4.4 Disability exception

Scenario questions
If instead, when Molly asks Sam about the Smart Glasses recording, Sam mentions that he is visually impaired and relies on the glasses for its accessibility features. The LED indicates that accessibility features are operational. What can/should be done?

A possible wrinkle in all the discussion above is the legitimate use of Smart Glasses for people with disabilities. For some, Smart Glasses can provide cutting edge accessibility features such as live transcription of lectures – for the people with auditory impairments – and real-time navigation for people with vision impairments.

The University will need to carefully balance the mitigation of Smart Glasses risks with inclusive design. Notably, similar measures can be observed in the law. For example, the use of listening devices for disability purposes is expressly carved out of the *Surveillance Devices Act*.[31] Yet, this exception was certainly not drafted with Smart Glasses in mind – a key difference being the multitude of features available on Smart Glasses, as compared to a more conventional narrow purpose accessibility device. Smart Glasses can in theory shift between providing accessibility features and conducting FRT at the direction of the user, unknown to other individuals. Striking the right balance in this discussion is still an area that is underexplored.

Recommendation 6
The University needs to consider the possibility of Smart Glasses being used to improve accessibility and how that interacts with the key policy questions noted above.

Being a technology which is relatively new, it may be worth exploring the utility of Smart Glasses as accessibility devices: are they legitimate game changers that provide new accessibility functionalities? Are there privacy-enhancing alternatives available?

Further, should the University implement exceptions for Smart Glasses, it is worthwhile to consider who may access the exception (e.g. the threshold of visual impairment) and where the onus should land in evidencing the disability, and how beneficiaries of the exception can avoid conflict.

[31] See s 4 for definition of 'listening device'.

Glossary

Term	Definition
FRT	Facial Recognition Technology – involves the matching of an individual's face against a database of biometric information for the purpose of facial identification.
HUD	Head up display – a transparent display which presents information without requiring the user to look away.
Smart Glasses	A wearable device which is designed to resemble eyewear that is capable of capturing, processing and outputting data. See section 1 for a list of products.

Contact

Centre for AI, Trust and Governance

aitg.centre@sydney.edu.au

sydney.edu.au

CRICOS 00026A