ADVOCACY

umsu.unimelb.edu.au/advocacy
suashelp@union.unimelb.edu.au

Policy Consultation Feedback

Date: 2 April 2026

To: ciog-teamcomms@unimelb.edu.au.

Subject: Feedback on the proposed Surveillance Policy

Following investigation and findings by the Victorian Privacy and Data Protection Deputy Commissioner, the University asserts the draft policy is intended to increase transparency, formalise approval pathways for new or changed surveillance, and create a public register. While we acknowledge the principle that making surveillance activities transparent would be furthered by a specific policy, UMSU believes the proposed policy does not yet meet that object.

From a student-rights perspective, we are particularly concerned about privacy, freedom of expression, freedom of association, and the chilling effect surveillance can have in a university setting, especially during a period of intensified scrutiny of protest and dissent on campus. Accordingly, we are of the view that any surveillance framework requires especially strong safeguards, clear scope and limits, independent oversight, and rigorous accountability.

We acknowledge that the draft is a step forward in one respect: it recognises that surveillance engages privacy and human rights, requires approvals, and proposes a public register. That is a significant improvement on the opaque and apparently ad hoc custom and practice to date.[1] However, in its current form the proposed policy leaves major risks for student rights and does not provide a sufficient level of rigour, necessity, proportionality, transparency, remedy, and independence that would characterise a human rights protective policy.

The Office of the Victorian Information Commissioner's (OVIC) recent report into the University's use of Wi-Fi data also introduces three concepts that should shape the University's policy response - social licence, function creep, and informed choice. The Deputy Commissioner found that the University repurposed Wi-Fi tracking capability introduced for network management into disciplinary surveillance after the Mahmood's Hall protest, without substantial consideration of the privacy and human-rights implications and without sufficient consultation to obtain a social licence for that use. The report further found that students and staff were not given information clear enough to make an informed choice about using the Wi-Fi network in circumstances where location data might later be used against them. These concerns go directly to legitimacy, trust, and whether a university community can participate in campus life without hidden surveillance risks.[2]

[1] See Office of the Victorian Information Commissioner (OVIC), *Report: University of Melbourne – University Use of Surveillance* findings which indicate the decision to use Wi-Fi data was made in a matter of hours based on incorrect information provided to Uni General Counsel.
[2] Ibid.

Summary

While the proposed policy reflects some sound concepts, in its current form it is little more than an internal authorisation framework. In the current context, that is insufficient to rebuild the trust and confidence of the community of people using the campus. The University has suffered serious reputational damage over the findings of the Victorian Privacy and Data Protection Deputy Commissioner and urgently needs to rebuild the trust and confidence of the community. If the University is serious about protecting the university community's privacy, academic freedom, and democratic participation, it should adopt a policy that does not simply authorise surveillance but *actively restrains it*.

Moreover, increased transparency about the University's surveillance activities is likely to increase concern in those using the campus environment. In order to mitigate the sense of a perpetual 'Big Brother' milieu, any policy framework must put accountability front and centre and ensure a robust complaint pathway is accessible to those under surveillance.

Without substantial amendment, the policy risks legitimising a broad architecture for monitoring and repurposing student and staff data in ways that chill speech, association, and protest, while relying too heavily on internal discretion and too unconvincingly on independent accountability.

Overall position

UMSU is of the view that the policy should not be approved in its current form without substantial amendment.

Overall, the proposed framework is not only too broad in its permission structure, but lacks safeguards, rights, remedies, and accountability mechanisms needed to make any surveillance regime in a university setting legitimate, proportionate, and rights protective. The framework permits too much, defines too little, and leaves too many of the most important protections to internal discretion, other instruments, or silence.

Specifically, the proposed policy not only expressly authorises the most extreme forms of surveillance, it also builds a broad internal permission structure around surveillance and subsequent use of surveillance information, while leaving too much to internal discretion, too many activities outside the policy's scope, and too few enforceable safeguards for students and staff. That combination creates significant risk of mission creep, selective enforcement, and chilling effects on protest, organising, and dissent.

As OVIC put it, surveillance of individuals is antithetical to human rights and should only ever be undertaken in the most serious circumstances, with clear guidelines, well-managed authorising processes, and genuine understanding by affected individuals of the purpose and limits of the use. That should be the baseline standard for any university surveillance framework.

Key concerns

The exclusions are too broad

Section 2.2 carves out an extensive range of activities, including protection of the integrity, security, availability and service delivery of university computing and network facilities; foreign interference activities; breach-of-contract matters; "business continuity"; financial integrity activities; internal audit; and approved research projects. It also excludes incidental collection from teaching, assessments, meetings, attendance monitoring, wellbeing support, and academic integrity systems, unless later used to investigate suspected misconduct.

OVIC's findings are especially relevant to the proposed policy's broad exclusions. The report found that Wi-Fi tracking capability originally introduced for network management was later repurposed for disciplinary surveillance, and this is precisely the kind of function creep that broad operational exclusions can conceal.[3] In this context, any carve-out for IT, systems integrity, service delivery, or similar administrative purposes should be tightly confined to genuinely technical and non-identifiable uses unless and until a fresh approval threshold is met. In practice, we know that this already encompasses large-scale monitoring of networks, accounts, communications metadata, device use, and access patterns.[4] The website FAQ makes clear that "data surveillance" may include reviewing IT system or facilities access, emails, or websites visited where approvals are obtained, all of which is governed by the *Provision and Acceptable Use of IT Policy* (MPF1314) for which we have already provided extensive feedback. To the extent that the University intends those activities to remain partly outside the policy under the IT-security exclusion, the policy does not genuinely provide full governance over surveillance (or surveillance-like) activity.[5]

From a student-rights perspective, the wholesale carving out of these activities is one of the most serious defects in the draft. Digital systems are increasingly the primary source of surveillance risks in modern universities. This includes digital infrastructure such as learning platforms, IT access logs, network metadata, attendance analytics, assessment technologies, meeting recordings, and repurposing of ordinary administrative data.[6] Much of this, however, sits beyond the policy's scope until it is drawn upon for investigative purposes. This threshold is too remote, because privacy and other individual rights are affected as soon as data is collected, stored, analysed, accessed, or structured for later secondary use - well before any formal investigation begins

We have the same concern with respect to the foreign interference exclusion. In a university context the issue of foreign interference is highly sensitive given its potential intersections with protest, political belief, international student life, global academic collaboration, and activism.[7]

[3] OVIC, above n. 1.
[4] See UMSU Feedback on Provision and Acceptable Use of IT Policy - October 2025.
[5] See: *Privacy and Data Protection Act 2014* (Vic) sch 1 cls 1–4.
[6] See e.g. Office of the Victorian Information Commissioner, *Guiding Principles for Surveillance* (Principles 1–5.
[7] *Charter of Human Rights and Responsibilities Act* 2006 (Vic) ss 7, 13, 15, 16.

Recommendation 1

Section 2.2 should be substantially narrowed. Minimally, any targeted, identifiable, or inferential monitoring of students and staff should fall within the policy, including digital monitoring, access-log analysis, meeting/teaching recording reuse, attendance analytics, and monitoring framed as 'IT security', foreign interference, or business continuity where personal information is accessed or analysed in a way that affects individuals. Where the activities concern genuine IT system-health monitoring of anonymous telemetry these may legitimately remain outside the policy, but only if re-identification, matching, or personnel-level review is prohibited without a fresh approval.

Inadequate protection of freedom of expression, protest, and association

The policy provides that approvers must consider human rights, including privacy, freedom of expression, and freedom of association, and must ensure surveillance does not discriminate on protected attributes. While UMSU welcomes this principle, the operative protections are too weak for a university setting where lawful protest and political activity are both foreseeable and potentially sensitive.

Under Victoria's Human Rights Charter, privacy, freedom of expression, and peaceful assembly/association are protected rights, and limitations must be reasonable, necessary, justified, and proportionate. The Victorian Equal Opportunity and Human Rights Commission's public-sector guide to the Charter specifically flags restrictions on protest, disclosure requirements, limits on access to information, and regulation of public expression as triggers for Charter scrutiny.[8]

Importantly, the draft does not expressly prohibit surveillance for the purpose, or foreseeable effect, of monitoring lawful protest, political opinion, association, industrial activity, or advocacy. Nor does it impose any heightened threshold for surveillance in contexts where protest, assembly, organising, or controversial speech are likely. "Public order" and "compliance with University rules, policies or conditions of entry" are listed register purposes for optical surveillance, which is especially troubling in the current context, as these purposes appear designed to capture encampments, demonstrations, leafleting, banner drops, rallies, meetings, and other forms of legitimate student political expression.[9]

Even where the University may purport that the policy is not designed to suppress protest, the drafting of the proposed policy suggests otherwise. Typically, broad discretionary powers attract particular scrutiny in Australian legislative review because,[10] if insufficiently defined, they may be exercised arbitrarily or inconsistently; UMSU is of the view that the policy should be rights-protective which requires clear statutory limits and safeguards, not simple reliance on benign administration.

---

[8] *Ibid, ss* 15(2), 16(1), 28; Victorian Equal Opportunity and Human Rights Commission, *The Charter of Human Rights and Responsibilities: A Guide for Victorian Public Sector Workers*.

[9] See e.g Victorian Equal Opportunity and Human Rights Commission (VEOHRC), 'Right to Freedom of Expression'; VEOHRC, 'Right to Peaceful Assembly and Freedom of Association'; and ibid.

[10] See e.g. Senate Standing Committee for the Scrutiny of Bills, *Principle (ii): Insufficiently Defined Administrative Powers*; and Parliamentary Joint Committee on Human Rights, *Report 5 of 2025* regarding the insufficiency of purely discretionary or administrative safeguards, p 60 at 1.142.

Recommendation 2

The policy should contain an express clause that surveillance must not be used to monitor, deter, profile, or identify participants in lawful protest, assembly, association, political activity, industrial activity, or expressive activity, except where there is a documented, evidence-based and imminent safety risk or suspected serious unlawful conduct, and where less intrusive means are not reasonably available. Any approval concerning protest or political activity should require a heightened approval threshold, written reasons, and post-use reporting.

"Legitimate University purpose" - too vague enabling function creep

While proportionality and human rights considerations must be contemplated, otherwise new surveillance activities and new uses/disclosures need only a "legitimate University purpose" to be approved. UMSU is of the view that this is an insufficient standard, as almost anything could be reframed as a legitimate purpose in a large institution.

OVIC's guidance provides that surveillance should be connected to a legitimate aim that directly corresponds to the organisation's functions, limited to what is demonstrably necessary, and generally not used where direct collection from the individual is reasonable and practicable. The proposed policy does not expressly require necessity, nor does it require consideration of less intrusive alternatives before surveillance is approved. "Reasonably proportionate" alone is not enough if the baseline purpose is cast too broadly.[11]

The proposed policy largely defers storage and retention issues to the *Retention and Disposal Authority* rather than specifying clear category-based rules within the surveillance framework itself. That is not sufficient given the sensitivity and breadth of the information contemplated in the register. Each surveillance activity should identify what is collected, what is strictly necessary, how long it is kept, when it must be deleted, whether it may be archived, and whether de-identification is required once the operational need ends. The framework should expressly prohibit indefinite retention or "just in case" retention of surveillance material.

UMSU is of the view that vague retention settings are one of the main ways that surveillance systems become normalised over time, particularly once information collected for one purpose becomes available for later trawling, matching, or repurposing.

Recommendation 3

Replace "legitimate University purpose" with a stricter necessity test requiring a specific, lawful, evidence-based, and clearly defined purpose that is necessary for a university function and cannot reasonably be achieved by less intrusive means. Require a written alternatives analysis before approval.

[11] See: Office of the Victorian Information Commissioner, *Privacy Impact Assessment*, OVIC, above n 6, Principles 2–4; *Privacy and Data Protection Act 2014* (Vic) sch 1 cl 1.1;.

The register evidences the intended breadth of secondary use

The proposed register permits wide use and disclosure of optical recordings, including for public order, property protection, health and safety, research integrity, biosecurity, academic misconduct, special consideration, staff misconduct, student general misconduct, and broader investigations of policy breaches. The approved users include multiple internal teams beyond security, such as Workplace Relations, Human Resources, Enterprise Technology, Health and Safety, Student and Scholarly Services, Physical Security, and Research Ethics/Integrity areas.[12]

Table 2 is particularly concerning because it allows "incidentally collected" information from online meetings, teaching, assessments, interviews, public lectures, and audio recordings of those activities to be used for misconduct processes and other investigations. Personally identifiable building access data can also be used for compliance management and investigations. The guidelines also contemplate matching video with access data and network-facilities data to determine a person's location or verify identity for misconduct investigations.

This exceeds what might ordinarily be understood as site security. It creates a system in which routine educational and administrative records can be repurposed for disciplinary investigation across a range of domains.[13] In a climate of restriction of protests, this raises a significant risk that ordinary campus participation, attendance at events, entry to buildings, presence at meetings, or participation in classes and public lectures could be turned into investigative material.

In the context of OVIC's findings regarding the University's use of Wi-Fi data to discipline protesters, the report indicates that not only was the later use of Wi-Fi location data intrusive; the University could not establish that using that data to identify individuals for misconduct proceedings was the primary purpose of collection, nor could it establish that this was a permitted secondary purpose under IPP 2.1. Accordingly, the policy should do more than require internal approval for later uses. It should expressly prohibit secondary use of surveillance-related data unless the University can identify a specific lawful basis, demonstrate necessity, and show that the use falls within a clearly defined and publicly disclosed category.

Recommendation 4

Significantly restrict authorised secondary uses. Replace broad "investigations" language with specific, defined grounds and require category-specific thresholds. Do not permit reuse of teaching, assessment, meeting, or lecture recordings for disciplinary purposes unless there is a serious matter, a documented necessity assessment, and approval by an independent body or officer not involved in operational security or discipline.

[12] *Privacy and Data Protection Act 2014* (Vic) sch 1 cl 2.1; Office of the Victorian Information Commissioner, 'Information Privacy Principle 2: Use and Disclosure'.
[13] OVIC, above n. 1

Cross-system Matching

One of the most intrusive features of the proposed framework is not simply the existence of separate forms of optical, audio, access, tracking, and computing/network surveillance, but the extent to which these systems can be combined to determine identity, location, conduct, or association. Once data from different systems is matched, relatively mundane operational records become a much more powerful profiling infrastructure.[14] This is especially relevant given the broader concerns already raised in relation to function creep and broad reuse powers in other policy settings.

Recommendation 5

The proposed policy should prohibit cross-dataset matching, inferential profiling, or identity verification unless there is a clearly defined serious-matter threshold, written necessity reasons, and approval subject to genuinely independent oversight.

There is no independent oversight

Approvals for new activities are entirely internal. New surveillance activities require any two senior staff, one from the Vice-Chancellor's Advisory Group. New uses/disclosures outside the register require endorsement by internal executives and approval by senior internal officers. The Chief Information Officer also maintains the register.

UMSU is of the view that this does not represent independent oversight. Rather it is internal executive oversight by the same institution that benefits from the surveillance. In matters that may be contentious - particularly those involving protest, industrial issues or reputational pressure - an internal-only approval process is unlikely to inspire confidence. Something which should be of the utmost concern to the University at a time when trust in the University's decision-making processes, governance frameworks and social licence as a tertiary institution continues to be in question by both its student population and the broader community.

While the OVIC report does not prescribe a single model of independent oversight, its findings strongly support policy that goes beyond internal executive approval alone, particularly in high-risk cases involving protest, disciplinary use, location data, or cross-system matching.[15]

OVIC's surveillance guidance emphasises safeguards, review, complaints, and remedy, and encourages consultation and privacy impact analysis early in design. The draft lacks an independent reviewer, independent appeals pathway, mandatory publication of de-identified approval reasons, or regular external audit.[16]

[14] OVIC, above n 6, under 'Definition of surveillance' and Principles 3–5; *Privacy and Data Protection Act 2014* (Vic) sch 1 cls 1, 2, 4.
[15] OVIC, above n. 1.
[16] OVIC, above n 6, Principles 5 and 7; see also *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 38.

Recommendation 6

Establish independent oversight, such as a Surveillance Review Panel including student, privacy, staff, and human-rights expertise, with elected student representation. Minimally, require external legal/privacy review for any surveillance proposal affecting protest, political activity, industrial activity, mass monitoring, analytics, or identity-matching.

Too Many Cooks

UMSU has significant concerns regarding the proposed policy's approach to access controls and internal misuse safeguards. We are of the view that strong technical and governance controls become essential once surveillance information can be accessed across security, IT, HR, student services, health and safety, and integrity or investigative functions. Least-privilege access, comprehensive logging of all access and disclosure, regular audits, and clear sanctions for misuse should be mandatory.

Similarly, staff with access to surveillance information should be subject to role-specific training in privacy, human rights, procedural fairness, and the particular risks associated with secondary use of incidentally collected material. Without those controls, the formal approval architecture of the policy is manifestly insufficient.

Standing approvals are a major loophole

Section 5.4 allows an approver to give a standing approval for uses or disclosures of surveillance information outside the register. In UMSU's view, this is a significant red flag. We consider that standing approvals are antithetical to the warranted level of tightly confined, case-specific scrutiny. Standing approvals facilitate the quiet normalisation of exceptional cases.[17]

UMSU believes that this is precisely how mission creep begins. First there is an exception, then a class of exceptions, then a routine pathway that is opaque and not meaningfully visible in public reporting. The risk is amplified because under 5.5(b) of the proposed policy, surveillance activities approved for testing or feasibility purposes are not entered on the *Register of Approved Surveillance Activities* unless and until they are fully implemented.

Recommendation 7

Remove the ability to grant standing approvals for secondary uses and disclosures outside the register. Require all non-routine uses/disclosures to be time-limited, case-specific, documented, and reported publicly in de-identified form.

Transparency still missing

The policy still leaves major transparency gaps despite a stated objective of the proposed policy to "ensure transparency in the University's surveillance activities". We acknowledge that the proposed public register is a positive step, however it does not require publication of privacy impact assessments, approval reasons, statistics on requests and approvals, rejection rates, incidents of non-compliance, or the volume of surveillance information disclosed for disciplinary or investigative purposes.[18]

[17] See OVIC, above n 6, at Principles 1, 5.
[18] Ibid at 5.2–5.5.

Although the proposed policy website stresses transparency and a public register, transparency is not secured merely by recording a category of activity. Appropriate transparency in UMSU's view would involve student access to information about what data is collected, where, for how long, who accesses it, how often it is used for disciplinary matters, whether analytics or matching are used, and what rights they have to challenge misuse.

The draft policy requires a Privacy Impact Assessment (PIA) where one is required by the *Privacy Policy* and allocates responsibility for conducting that assessment to the Director, Information Governance Services. Notwithstanding that PIAs are acknowledged to be an important safeguard in the approval process, the proposed policy does not require completed PIAs to be published or otherwise made available for scrutiny.[19] The result is that privacy risks will be assessed internally without any external visibility as to what risks were identified, how necessity and proportionality were evaluated, or what mitigations were adopted.

The proposed policy additionally requires the requestor to keep a record of the approver's decision under the approval provisions at 5.2 and 5.4, expressly permitting standing approvals. Yet it does not require any public reporting on how often approvals are granted or refused, how often standing approvals are used, or how frequently surveillance is relied on in particular operational contexts.

Finally, while the proposed policy provides that surveillance information will be stored and retained in accordance with the *University's Retention and Disposal Authority*. It also requires requests for new surveillance activities to explain how surveillance information will be managed. But the proposed policy does not disclose what retention periods apply to particular classes of surveillance, nor does it require those periods to be stated in the register. This leaves retention rules opaque to affected persons and makes it difficult to evaluate whether retention practices are appropriately tailored to the nature and purpose of the surveillance activity.

Recommendation 8

For maximum transparency, the proposed policy should require publication, at least annually, of:

1. *the full register in searchable form;*
2. *subject to 5.2(b)(ii) and 6.3 of the proposed policy - all completed PIAs, with redactions only where strictly necessary;*
3. *aggregate statistics on approvals, refusals (5.5(a)(i)), standing requests (5.4(d)), disciplinary uses (Register, Table 1 and Table 2), law-enforcement disclosures subject to 2.2(b), and data matching subject to 2.2(f);*
4. *retention periods for each surveillance class.*

Notice and consent protections are underdeveloped

Under 5.1(a)(vi), cl 5.2(b)(iv), the proposed policy provides that requests should explain how affected individuals will be notified and that collection notices and procedures should be in place. UMSU considers this insufficient, because in practice "notice" may amount to little more than generic notifications or obscure web pages that affected individuals are unlikely to see before their data is repurposed.

[19] OVIC, above n 11.

OVIC's recent investigation report found that the relevant University materials were poorly presented, used misleading headings and titles, and made the purpose of collection and use unclear.[20] It also found that the delivery method for the Wi-Fi notice - an on-screen pop-up - was not an effective mechanism for explaining complex terms and conditions. Consequently, the policy should require not only notice, but notice that is prominent, intelligible, context-specific, and designed for actual understanding rather than formal compliance.

Additionally, Victorian privacy guidelines emphasise clear notice, purpose limitation, and privacy impact assessment, including attention to whether a secondary use is a use that individuals would reasonably expect.[21] In the university context, OVIC's investigation into the University of Melbourne underscores the point that people should not discover *only after the fact* that data collected for operational purposes has been repurposed for misconduct investigation.

Recommendation 9

The proposed policy should require specific, accessible, plain-language notices at point of collection and prior to secondary use wherever feasible. Where immediate prior notice would prejudice a serious investigation, the policy could still require delayed notice unless legally proscribed, and explicit notice should be required when data from one context may be matched with other data sources.

Insufficient data minimisation, access, and deletion rules

The OVIC report also makes clear that surveillance harms extend beyond the eventual target of an inquiry. The Deputy Commissioner observed that the University could have pursued its objectives with fewer privacy impacts, not only on the individuals ultimately investigated, but also on others who were incidentally caught up in the University's inquiries. That finding supports stricter minimisation, anti-trawling, and deletion requirements. A university policy should not assume that collateral intrusion is acceptable merely because only some individuals are later pursued.

The proposed policy provides that surveillance information will be stored and retained in accordance with the *University's Retention and Disposal Authority*. UMSU is of the view that this remains too high-level. A rights-protective surveillance policy should contain narrower defaults - minimal retention, strict role-based access, access logging, audit trails, mandatory deletion where no incident is identified, and prohibitions on speculative browsing of footage or logs.
This would bring the proposed policy into better alignment with OVIC's privacy guidance (see footnote 3) which emphasises security, role-based access, auditability, and reasonable steps to prevent misuse and unauthorised disclosure.

The proposed policy at 5.6 provides only that surveillance information will be stored and retained in accordance with the University's Retention and Disposal Authority, while the proposed register separately identifies various categories of surveillance information - including recordings, audio recordings, GPS/location data, video analytics data, online meeting recordings, public lecture

[20] OVIC, above n 1.

[21] Office of the Victorian Information Commissioner, Collection Notices; Information Privacy Principle 2 – Pocket Guide; Privacy Impact Assessment Guide; Guiding Principles for Surveillance; Investigation into the Use of Surveillance by the University of Melbourne.

recordings, and building/facilities access data. Accordingly, while the proposed policy recognises different types of data, retention of that data is dealt with only by a cross-reference to another instrument.

Additionally, the proposed policy contemplates access control and operational procedures, but it does not expressly require access logs, routine review of who actually accessed information, or periodic audits of compliance.

Finally, although the proposed policy regulates uses and disclosures of surveillance information and the register contemplates downloaded transcripts, internal sharing, and data matching, it does not prohibit downloading, copying, or sharing except where strictly necessary and authorised.

Recommendation 10

The proposed policy should specify default retention limits by data type, require access logs and periodic audits, and prohibit downloading, copying, or sharing surveillance information except where strictly necessary and authorised.

Heightened Risks for Vulnerable Cohorts

As we have previously noted in our feedback on the University Privacy Management Policy (MPF1104), tracking, access, location, and identity-linked information can expose attendance, movement, and association in ways that create acute risks for people experiencing gender-based violence including stalking, family violence, harassment, discrimination, or other safety concerns. In the university context, this also extends to attendance at counselling, health, union, activist, queer, faith, and other sensitive spaces or activities. These harms are particularly associated with location-linked and other sensitive information. In the context of the Action Plan Addressing Gender-based Violence in Higher Education and the University's obligations under the National Higher Education Code to Prevent and Respond to Gender-based Violence, this is an especially egregious approach.

Students who rely on campus facilities for extensive periods of time because it provides refuge from unsafe home environments are more likely to experience harms associated from surveillance. This includes a loss of privacy around personal circumstances and a chilling effect on help-seeking behaviour or staying on campus for safety. This might also produce a constant sense of being watched which is especially harmful for students who experience control, trauma or unstable authority figures at home. Such students are especially susceptible to increased psychological stress and hypervigilance when under constant surveillance.

Case-study – Noah Rodriguez[22]

Noah is a first-year student studying a Bachelor of Arts at the University of Melbourne. He is a first-in-family student and is proud of his achievement. He attends the campus daily and uses facilities extensively as he does not have internet at home (and instead relies on his mobile phone for hot spotting). He finds it difficult to prepare for classes and complete assignments at home. One of his parents has recently passed away and his remaining parent is suffering from substance abuse disorders which weighs heavily on Noah.

Noah was unaware of the Mahmoud's Hall protests and requested advice from a security guard before entering the Arts West building. He was advised that he was welcome to use the facilities before his class and he proceeded to one of desks so he could complete a media assignment before class. He kept his noise-cancelling headphones on and proceeded to work on his assignment for the next few hours where he then proceeded to his class tutorial.

Weeks later he was issued a general misconduct allegation notice. He was shocked to receive this because he had not been part of the protests. A document setting out his location and Wi-Fi use was used by the misconduct discipline committee to place Noah at the location and time of the protests. Noah was upfront about his family situation and his reason for being at Arts West during the time in question. He also explained how unclear he found the instructions by the University and that he had sought advice from a security guard about accessing the building on the day.

Despite this, the Committee found Noah to have committed general misconduct. Noah felt betrayed by the University and since then he has decreased his time on campus. His trust in university staff has been badly damaged, affecting his experiences and success as a student.

Noah's example demonstrates how increased surveillance and location tracking can have a direct effect on academic engagement for vulnerable students.

Recommendation 11

The proposed policy must require heightened safeguards where surveillance could expose vulnerable people or reveal attendance, association, or movement in sensitive contexts.

No meaningful complaints, appeal, or remedy pathway is built into the policy

OVIC's surveillance guidance expressly includes complaints and remedy as a core principle. The draft does not appear to create a dedicated pathway for students or staff to:

- find out whether their information was used,
- challenge improper use,
- seek correction of records,
- seek deletion where use was unjustified, or
- obtain an independent review.

[22] This case-study is based on a real matter. However, the student has been de-identified to protect their privacy and a pseudonym has been used instead.

The proposed framework is also notably underdeveloped on the rights of people who are actually subjected to surveillance or secondary use of surveillance information. While the policy is detailed on internal authorisation and record-keeping, it is much lighter on whether an affected student, staff member, or other person has any meaningful right to know when surveillance information has been used against them, to seek access to that information, challenge misuse, or obtain review of a decision based on it. A surveillance framework which lacks clear complaint pathways, independent review, and procedural fairness where surveillance information is used in disciplinary, academic, employment, or other adverse processes is manifestly incomplete.

Recommendation 12

The proposed policy should include:

1. *a process for affected individuals to request access to records of surveillance decisions affecting them, subject only to narrow lawful limits.*
2. *correction rights where appropriate.*
3. *right to seek review where surveillance information has been relied upon in a way that adversely affects a person.*
4. *a dedicated complaints and review section with internal review plus referral rights to OVIC and other appropriate bodies.*

There should also be a presumption of post-use notification where surveillance information is used in an adverse process, unless delayed for compelling legal or safety reasons.

Summary of Recommended Changes

UMSU is of the view that minimally the following amendments should be made:

1. **Narrow the exclusions in section 2.2.** Bring within the policy any identifiable monitoring, analytics, matching, or access to logs/recordings that may affect an individual, including when framed as IT security, foreign interference, business continuity, attendance monitoring, academic integrity, or wellbeing.

2. **Add an express prohibition on protest and political surveillance.** State that surveillance must not be used to monitor lawful protest, organising, political belief, association, union activity, or expressive activity, except in narrowly defined, evidence-based, serious-risk scenarios.

3. **Replace "legitimate University purpose" with a necessity test.** Require a specific lawful objective, evidence of necessity, consideration of less intrusive alternatives, and documented reasons.

4. **Delete standing approvals under section 5.4(d).** All non-routine uses/disclosures outside the register should be case-specific and time-limited.

5. **Require independent oversight.** Create an independent approvals/review panel with student representation and privacy/human-rights expertise.

6. **Strengthen transparency.** Publish PIAs, annual statistics, approval summaries, audit outcomes, and retention periods.

7. **Tighten the register.** Remove broad catch-all investigation purposes and restrict reuse of teaching, meeting, lecture, and assessment recordings.

8. **Add protections for sensitive contexts.** Any surveillance affecting protest, student discipline, industrial matters, vulnerable cohorts, or political activity should trigger enhanced scrutiny.

9. **Mandate notice and post-use notice.** Require clear notice at collection and, where feasible, notice before or after secondary use.

10. **Specify default retention limits.** The proposed policy should specify default retention limits by data type, require access logs and periodic audits, and prohibit downloading, copying, or sharing surveillance information except where strictly necessary and authorised.

11. **Add protections for vulnerable student cohorts.** The proposed policy must require heightened safeguards where surveillance could expose vulnerable people or reveal attendance, association, or movement in sensitive contexts.

12. **Add complaint and remedy rights.** Include challenge, correction, deletion, review, and escalation pathways.