UMSU ADVOCACY

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

Memo

Date: Monday 13 October 2025

To: Policy Office, Information Regulation
Information Governance Services
Legal and Risk, COO Portfolio
BusServ-teamcomms@unimelb.edu.au

Subject Feedback regarding the University's proposed amendments to the *Provision and Acceptable Use of IT Policy* (MPF1314)

The UMSU Advocacy Service welcomes the opportunity to provide feedback on the proposed changes to the *Provision and Acceptable Use of IT Policy* (MPF1314) given its impact on students' safety, freedom of association, and right to lawful protest on campus.

The Mahmoud's Hall Protests and OVIC's Investigation

A failure of informed consent

We raise significant concerns regarding the proposed changes, which appear primarily intended to legitimise IT surveillance practices targeting students and staff that were previously either unlawful or of dubious legality.

In view of the 2024 Student Experience Survey,⍰ where the University of Melbourne scored the lowest ratings for Overall Educational Experience by undergraduate students compared to other Australian universities (and fourth lowest for postgraduates), there is a clear indication that trust in the University's decision-making processes, governance frameworks and social licence as a tertiary institution is in question by both its student population and the broader community.

We recognise that the poor results in the QILT survey is not solely related to the University's recent use of IT surveillance technologies. However, we believe that the University's previous covert IT surveillance has contributed to the collective student sentiment that the University is profoundly mistrustful of its students and staff and it creates a bad faith environment where it appears uninterested in the student experience.

Our feedback in this consultation paper is provided in the hope we can assist the University rebuild trust with the student population and renew its social license as a responsible steward of critical digital assets.

To that end, it is important to examine the historical context that has shaped the present landscape, enabling a clearer understanding of the systemic issues at play. This includes UMSU's advice regarding the responsible use of Wi-Fi technologies in 2016, the findings of the Office of the Victorian Information Commissioner (OVIC) this year, and the University's refusal to review it management of the misconduct hearings arising from the Mahmoud's Hall protests considering OVIC's findings.

When the University introduced Wi-Fi tracking, it assured privacy groups that its intention was to track general movement on site to improve retention rates and the student on-campus experience. The head of services at the time, Paul Duldig, provided assurances that individual students would not and could not be identified[1]. In response, the UMSU president, Tyson Holloway-Clarkey, noted privacy concerns explaining that the University's adoption of this technology raised concerns about its compliance with privacy laws, and likely function creep[2].

Fast forward to 2024, and during the Mahmoud's Hall protests, the University used Wi-Fi surveillance technology to selectively identify students for misconduct allegations, raising concerns about fairness, transparency and appropriate use of data.

This matter was referred to OVIC for investigation. On the 10 August 2025, OVIC published its investigation into the use of surveillance by the University of Melbourne[3]. In the report, OVIC noted:

> *The University engaged in function creep by using surveillance of users of on-campus Wi-Fi in disciplinary proceedings it began after a protest. The University introduced the Wi-Fi tracking capability some years ago, for the purpose of network management, with a reassurance that it would not be used to surveil individuals.* ***The University subsequently used the capability for disciplinary purposes, because it was already in place, without substantially considering the human rights or privacy impacts of doing so.*** *In failing to consult with stakeholders about the policy change, the University failed to obtain a social licence for the use of this technology.*[4]

The Deputy Commissioner also found that individuals whose Wi-Fi location data was used to determine their physical position on campus were "subjected to a form of surveillance" and that the students are "likely to have experienced a significant breach of trust"[5].

We note that the proposed amendments clearly set out that the primary and secondary use of its Wi-Fi technologies is to identify and detect network users, and that this information may be used in misconduct allegations unrelated to use of the IT infrastructure. The concerns raised by privacy advocacy groups and UMSU in 2016 have now been fully realised. The introduction of these provisions demonstrates a level of organisational overreach which is likely to further erode student trust in the University. Below, we set out how this approach to on-campus surveillance is likely to impact the student population.

[1] Australian Broadcasting Commission, 'University of Melbourne defends wi-fi tracking of students as planning move amid privacy concerns' <https://www.abc.net.au/news/2016-08-12/university-of-melbourne-tracking-students-through-wifi/7723468>.

[2] Ibid.

[3] Office of the Victorian Information Commissioner, *Investigation into the use of surveillance by the University of Melbourne* (Final Report, 10 August 2025).

[4] Ibid, 3.

[5] Ibid, p 32.

General Principles and Issues

The fraying of social trust and the social license

There are significant human rights concerns associated with both Wi-Fi and CCTV surveillance technologies.

Some key issues include:

Privacy Rights

Modern surveillance technologies pose growing threats to privacy, with digital monitoring systems becoming formidable tools for control and potentially oppression.[6] The UN Declaration of Human Rights Article 12 protects individuals from arbitrary interference with privacy, family, home, or correspondence,[7] but surveillance systems often operate in domestic statutory grey areas. Given the current erosion of governance frameworks and the documented history of non-compliance with privacy legislation, there is limited confidence of the University's capacity to navigate these domestic statutory grey areas with the necessary contextual awareness and institutional maturity.

CCTV Surveillance Issues

Lack of Legal Safeguards: In Australia, there are currently no general, legally enforceable rules to limit privacy invasions and protect against abuse of CCTV systems.[8] This creates serious accountability gaps for large institutions such as the University of Melbourne with few if any external checks and balances on its activities. For example, proposed section 4.14 states that the Executive Director, Business Services and Chief Information Officer will be able to authorise access to personal information. It is suggested that this provision is introduced to identify that an authorising environment exists for approving access. However, no parameters or criteria exist to limit or check the authority to allow this access to extraordinarily sensitive personal information. Without this transparency of how this authority may be exercised, the long-term legitimacy of this policy is likely to be compromised and the successful adoption of technology initiatives is likely to suffer.

Discriminatory Targeting/profiling: Video camera operators frequently bring existing prejudices and biases to their work, leading to discriminatory surveillance practices. Apart from the potential for racial profiling, studies in the UK have found that predominantly male camera operators used systems voyeuristically to spy on women, with one in ten women targeted for entirely voyeuristic reasons.[9] Given these concerns, it remains unclear how the University will reconcile its obligations under the standards of the National Code to Prevent and Respond to Gender-based Violence with surveillance practices that lack transparency and demonstrate overreach.

[6] See: OHCHR, 'Spyware and surveillance: Threats to privacy and human rights growing, UN report warns' <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>; UN Human Rights Council, 'The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights', UN Doc A/HRC/51/17 (4 August 2022).

[7] Daniel J. Power, Ciarra Heavin and Yvonne O'Connor, 'Balancing privacy rights and surveillance analytics: a decision process guide' (2021) 4(2) *Journal of Business Analytics*.

[8] See e.g. in US What's Wrong with Public Video Surveillance? | American Civil Liberties Union

[9] Ibid.

WiFi & IT Surveillance Concerns

Mass Monitoring: New technologies enable systematic monitoring of what people say online and widespread digital surveillance of public spaces, with automated data collection sweeping away previous practical limitations on surveillance scope.[10] This is likely to impact a student's campus experience, eroding their privacy and damage trust between the University and the student population.

Location Tracking: Wi-Fi tracking identifies and tracks mobile devices based on Wi-Fi signals they generate, determining movement patterns without people's knowledge or valid legal reasons.[11] Simply telling people it will happen is different to actually alerting them when it is occurring. Wi-Fi log data can reveal sensitive location information and potentially create risks for those already experiencing gender-based violence.

Impact on Vulnerable Groups

Surveillance tools purportedly deployed for combating misconduct can be used for illegitimate, political or ideological reasons, including clamping down on activism, opposition to university stances, and the activities of other human rights defenders.[12] Students are generally reliant on University IT and consequently face greater surveillance risks than those with private networks. Students may opt to move away from university provided IT, introducing a range of other undesirable consequences for the university community.

Institutional Accountability

Surveillance technology companies have human rights responsibilities under UN Guiding Principles to avoid causing or contributing to adverse human rights impacts through their business.[13] However, enforcement remains inconsistent/non-existent, and many institutions lack transparency about how they address surveillance risks. The current proposed changes to *the Provision and Acceptable Use of IT Policy* (MPF1314) exacerbate rather than ameliorate these risks.

The fundamental concern is that pervasive surveillance undermines democratic freedoms, chills free expression, and creates power imbalances that can be exploited for political repression, discrimination, and control—all while operating with insufficient legal oversight or accountability mechanisms.

Response to Proposed Policy Provision Changes

Lack of visibility, potential overreach and legal and ethical ambiguity

Policy Reference 1 (d): This section creates the authority for university staff to use computer and network facilities to detect and investigate actual or reasonably suspected unlawful behaviour or breach of policy. However, this section fails to provide any limitations on this authority, nor does it define 'reasonably suspected'. As OVIC states in its investigation into the University:

> *Surveillance of individuals should only ever be undertaken in the most serious of circumstances, where clear guidelines are available, authorising processes are well-managed, and individuals*

[10] Above n. 8.
[11] Data protection digest 3 - 17 May 2024: Wi-Fi tracking, exam monitoring, data theft and extortion - TechGDPR
[12] Above n. 8.
[13] UNHCR, Guiding Principles on Business and Human Rights.

> *understand the purpose and limitations of the use of the information.*[14]

This provision should include clear limitations on the authority to enhance transparency of operations.

Policy Reference 4.10 and 4.11: These provisions set out the terms for the usage, monitoring and investigation of data as well as expressly stating that data gathered may be used to investigate misconduct matters. In their investigation, OVIC goes into details exploring the line between the invasion of privacy and the need to investigate unlawful activity which may include breaches of privacy. However, when referring to the Mahmoud's Hall protests, OVIC refers to the proportionality test stating that even when an organisation is investigating breaches in policy for legitimate purposes, "it cannot do so at all costs to individuals' privacy"[15].

These sections fail to reference the proportionality test, which is a critical omission if the University intends to demonstrate its credibility as a responsible custodian of sensitive data.

Policy Reference 5.20: This section places an obligation on the service user to ensure that any Wi-Fi networks used are secure to improve the University's cybersecurity best practice. However, given that many of these proposed provisions are likely to compromise personal privacy, many students may elect not to use the University's Wi-Fi network due to distrust with how their personal information may be used. This could result in exposure to a range of new cyber threats to the University. As such, a review of the policy that includes robust personal privacy safeguards is more likely to increase the use of the University's networks and in turn ensure cybersecurity best practice.

Conclusion

Although we have highlighted the more problematic areas of the proposed policy inclusions, we take the position that the broader principle at stake must be addressed: the deployment of such measures by a large public institution is fundamentally undesirable and should be rejected outright.

At a time when public trust in universities is at a historic low, and the institution's social licence is dangerously close to being cancelled, we believe the proposed changes risk further eroding confidence and represent a major misstep in the context of the University's Statutory Objects which require the University to

> *serve the Victorian, Australian and international communities and the public interest by: ...*
> *promoting critical and free enquiry, informed intellectual discourse and public debate*
> *within the University and in the wider society.*[16]

Accordingly, we strongly recommend that the proposed reforms be abandoned and redrawn.

Michelle Almiron
Project & Research Lead
UMSU Advocacy Service
m.almiron@union.unimelb.edu.au

[14] OVIC, above n.3, p3.
[15] OVIC, above n. 3 p 27.
[16] *University of Melbourne Act 2009* (Vic), Section 5.