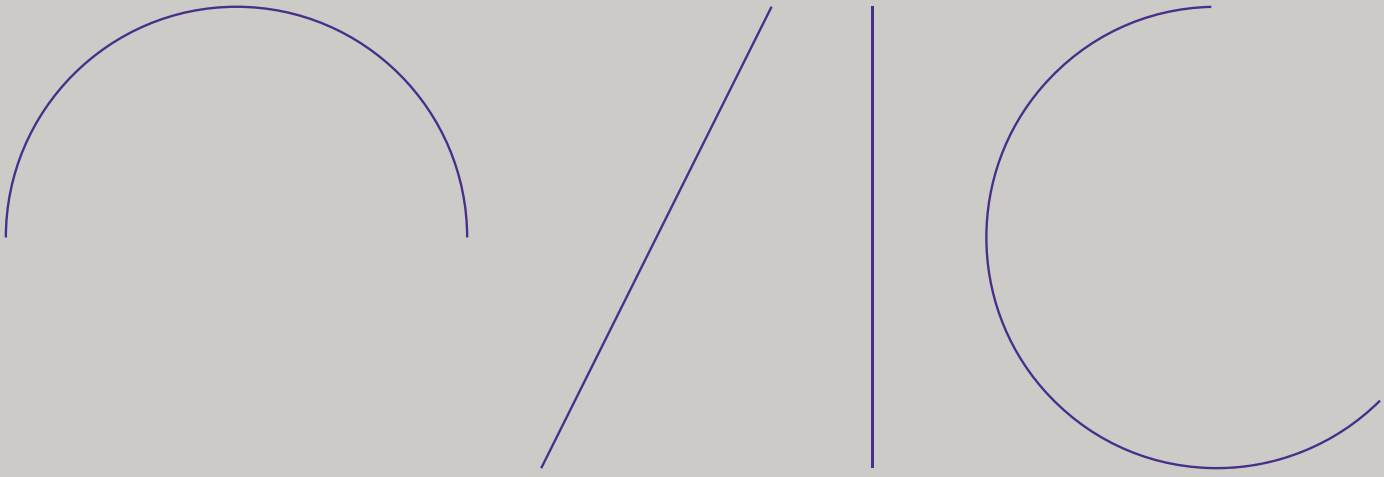
OVIC
Office of the Victorian Information Commissioner

Investigation into the use of surveillance by the University of Melbourne

Under s8C(2)(e) of the *Privacy and Data Protection Act 2014*



Disclaimer

The information in this document is general in nature and does not constitute legal advice.

Copyright

Foreword

This investigation focuses on the importance of good governance and effective communication, in the context of events that took place during and after a protest at the University of Melbourne in May 2024.

Social licence and function creep are two important concepts in interpretation of the relationship between human rights and technology. When governments or other official bodies implement technology, society expects them to respect human rights, including the right to privacy. This is usually achieved through the preparation of a Privacy Impact Assessment, and through communication with affected stakeholders about the purpose of the technology and the ways in which its use will be governed.

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.

Effective communication is an essential ingredient in good privacy practices. For people to understand how their information may be used by an organisation, that organisation should communicate clearly and simply, in a manner that facilitates understanding. The investigation found that the information contained in the University's Wi-Fi Terms of Use, Provision and Acceptable Use of IT Policy, Property Policy, Student Privacy Statement, and Staff Privacy Statement was poorly presented, contained misleading headings and titles, and contained information that made the purpose of collection and use unclear.

The delivery method for the Notices related to Wi-Fi use - an on-screen pop-up - was also not an effective mechanism for explaining complex terms and conditions.

Additionally, the governance and authorising processes the University used to authorise access to staff email accounts fell below the standard the Deputy Commissioner expects. This access occurred after the urgency of protest had passed, and could have been dealt with more carefully.

These factors contributed to a breach of the Information Privacy Principles (**IPPs**). Because the collection and use of the data involved the surveillance of students and staff, and surveillance by its nature is antithetical to human rights, the breach was serious.

Notwithstanding the breach, there were circumstances in which the University could have achieved the outcomes it sought, with fewer impacts upon the privacy of the individuals concerned and individuals who were incidentally caught up in the University's inquiries. 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 understand the purpose and limitations of the use of the information. The University has undertaken to amend its Collection Notices, and its governance of the management of information collected, to remedy these defects.

Because many of the remedial steps have already been taken, and the remaining ones will be completed soon, the Deputy Commissioner did not issue a compliance notice.

Rachel Dixon

Privacy and Data Protection Deputy Commissioner

19 August 2025

Table of Contents

Foreword 3

Executive Summary 6

1. Background 10

2. The Deputy Commissioner's investigation 10

3. The sit-in protest and the University's misconduct investigations 11

Sit-in protest at the Arts West Building 11

What form of misconduct did the University investigate? 12

How did the University identify protesters who participated in the sit-in? 13

The University's decision to use Wi-Fi location data 13

The University's decision to conduct discovery of staff email accounts 14

Outcome of the misconduct investigations and proceedings 14

4. Did the University contravene the IPPs in relation to student and staff Wi-Fi location data? 15

IPP 1.3 – Did the University take reasonable steps to make students and staff aware of the purposes for which their Wi-Fi location data was collected? 15

IPP 2.1 – Was the University's use of Wi-fi location data for the primary purpose of collection? 20

IPP 2.1(a) – Was the use of Wi-fi location data for a secondary purpose that an individual would reasonably expect? 22

IPP 2.1(e) – Was the use of Wi-fi location data a necessary part of an investigation into unlawful activity? 24

5. Whether to issue a compliance notice 29

How did the contraventions occur? 29

Does the University have sufficient controls in place to prevent similar contraventions? 30

The Deputy Commissioner's decision not to issue a compliance notice 33

Annexure A 34

Executive Summary

Background

In July 2024, media reported that the University of Melbourne (the **University**) had tracked students who staged a sit-in protest at the Arts West Building at the University's Parkville campus, using CCTV footage and Wi-Fi location data that the University intended using as evidence in misconduct proceedings.

Shortly after, the Privacy and Data Protection Deputy Commissioner commenced preliminary inquiries into the acts and practices mentioned in the article, and whether they complied with the Information Privacy Principles (**IPPs**) as outlined in the *Privacy and Data Protection Act 2014* (**PDP Act**).

The Deputy Commissioner's investigation

Following preliminary inquiries, the Deputy Commissioner determined that there remained issues that warranted more formal regulatory action, and that the nature of the issues raised serious concerns about compliance with the IPPs. She commenced an investigation under section 8C(2)(e) of the PDP Act.

During preliminary inquiries, the Deputy Commissioner had found that the University had not contravened the IPPs in relation to its collection and use of CCTV footage. The investigation therefore focused on the University's use of staff and student's Wi-Fi location data, and was expanded to include the University's review of a small group of staff members' email accounts, the access to which the University had disclosed to OVIC during the investigation.

Specifically, the Deputy Commissioner sought to determine:

- whether the University properly informed students and staff about how their personal information – in the form of Wi-Fi location data and staff emails – would be used (IPP 1.3); and
- whether the University's use of Wi-Fi location data and staff emails for the purpose of identifying individuals in a misconduct investigation was consistent with the primary purpose of collecting this information or was for an authorised secondary purpose (IPP 2.1).

The University's misconduct investigations

A pivotal event during the sit-in protest was the issuing of the Vice-Chancellor's Direction to Leave on 20 May 2024, which directed all persons occupying the Arts West Building to leave the University grounds and remove all personal property. It also advised that those refusing to comply with the direction would be subject to consequences such as suspension, internal disciplinary action, or referral to the police.

When it became clear that some individuals were not complying with the Direction, the University commenced investigations as to whether any student misconduct had occurred.

The University used a combination of student Wi-Fi location data, student card photographs and CCTV footage to identify students who failed to leave the Arts West Building after the Direction to Leave. In so doing, the University identified 22 students who were persistently in the building after the Direction to Leave was issued.

As a result of its investigations, the University brought misconduct proceedings against 20 of these students, alleging two disciplinary breaches:

1. failure to comply with a reasonable direction or request of a senior officer or a security officer, thereby engaging in general student misconduct under regulation 25(a) of the Vice-Chancellor Regulation and section 4.5(e) of the Student Conduct Policy; and
2. interference with and/or improperly, recklessly or unsafely using University property, facilities or services, thereby engaging in general student misconduct under regulation 25(a) of the Vice-Chancellor Regulation and section 4.5(f) of the Student Conduct Policy.

Of the 20 students who had disciplinary proceedings brought against them, 18 had the two allegations substantiated, one had one allegation substantiated, and one case was dismissed. In the 19 cases where allegations were substantiated, the students received a "reprimand and caution".

The University also identified that some staff were involved in the protest through analysis of Wi-Fi location data, CCTV footage, and a review of 10 staff members' email accounts. The email discovery process resulted in six staff being excluded from further investigation, and four staff being identified as having potentially failed to comply with the Direction to Leave.

Formal meetings were held with three staff members about allegations of potential misconduct. The University substantiated the allegations, with each of these staff members receiving a formal written warning.

Contravention of the IPPs

The Deputy Commissioner's investigation considered whether the University complied with IPP 1.3 and IPP 2.1 regarding its handling of Wi-Fi location data.

In terms of IPP 1.3, the Deputy Commissioner considered whether the University took reasonable steps to make students and staff aware of why their personal information was being collected, and how their personal information would be used. That is, that it could or would be used to determine their location as part of a misconduct investigation. Providing prior notice generally gives individuals the opportunity to consider whether they will proceed with their interaction knowing what information will be collected and how it will be used.

The University asserted that it made individuals aware that Wi-Fi location data could be used to identify their whereabouts as part of a misconduct investigation through its Wi-Fi Terms of Use, Provision and Acceptable Use of IT Policy, Property Policy, Student Privacy Statement, and Staff Privacy Statement. However, the Deputy Commissioner found these materials lacked detail, clarity and specificity. Even if individuals had read these policies, it is unlikely they would have clearly understood their Wi-Fi location data could be used to determine their whereabouts as part of a misconduct investigation unrelated to allegations of misuse of the Wi-Fi network. Given that individuals would not have been aware of why their Wi-Fi location data was collected and how it may be used, they could not exercise an informed choice as to whether to use the Wi-Fi network during the sit-in, and be aware of the possible consequences for doing so.

In terms of IPP 2.1, the Deputy Commissioner considered whether the University's use of Wi-Fi location data to identify students and staff for potential misconduct proceedings was for the same purpose as that

for which the information was originally collected or was for a permitted secondary purpose. The University asserted that this was the case.

The Deputy Commissioner determined, however, that it could not be said that the University's primary purpose or intention when it initially collected the Wi-Fi location data was to potentially investigate misconduct that was unrelated to the use of the University network. Therefore, for the University to establish that its use of personal information was permitted under the IPPs, it needed to demonstrate that it was for one of the limited permitted secondary purposes as set out in IPP 2.1(a)–(h). The University was unable to demonstrate this to the Deputy Commissioner's satisfaction, and so she found that the use of Wi-Fi location data to identify individuals in the Arts West Building was not for a permitted secondary purpose.

The investigation moved on to consider whether the University contravened the IPPs in relation to the review of staff emails. Ultimately, the Deputy Commissioner found that while the University did not demonstrate best practice in terms of governance and execution of this review, this did not amount to a breach of the IPPs.

Decision not to issue a compliance notice

The Deputy Commissioner conducted the investigation with a view to deciding whether to issue a compliance notice to the University under section 78 of the PDP Act. OVIC's commissioners may issue a compliance notice where they determine that an organisation has contravened one or more of the IPPs and, the contravention is serious, repeated or flagrant.

A compliance notice requires an organisation to take specified action within a specified period and is issued to ensure compliance with the IPPs.

In summary, the Deputy Commissioner found that the University contravened IPPs 1.3 and 2.1 in relation to the use of Wi-Fi data. Taking into account the number of individuals impacted and the level of impact on these individuals, the Deputy Commissioner determined that the contraventions were "serious". The decision on whether to issue a compliance notice therefore required the Deputy Commissioner to consider the causes of the contraventions, any relevant changes implemented by the University, or undertakings to do so, and whether any additional action would be required to ensure future compliance with the IPPs.

In the final stages of this investigation, the University advised the Deputy Commissioner that it had taken a range of actions aimed at satisfying the requirements of a potential compliance notice. Actions included developing a surveillance policy and associated procedures (in progress), promoting the new surveillance policy to all staff and students, amending the Wireless Terms of Use and Provision and Acceptable Use of IT Policy, and implementing a process for providing all new users of the University email system with a notice of collection. The University also undertook to report to the Deputy Commissioner when each of these actions have been implemented.

Based on the University's cooperation throughout the investigation, and its actions and undertakings above, the Deputy Commissioner decided that it was not necessary to issue a formal compliance notice. Nonetheless, the Deputy Commissioner remains concerned by the University's practices outlined in this report, and will continue to seek evidence and assurance that it has completed the actions it has agreed to implement.

The University's response to the investigation report

The University provided a brief response to the investigation's findings which is included as Annexure A to this report.

1. Background

1. In July 2024, *The Age* reported that the University of Melbourne (**the University**) had tracked students who staged a sit-in protest at the Arts West Building at the University's Parkville campus in May 2024, using CCTV footage and Wi-Fi location data that it intended using as evidence in student misconduct proceedings.[1]

2. The article referred to previous criticism from legal professionals and human right activists about the University's use of Wi-fi tracking.[2] In 2016, the University had responded to privacy concerns by claiming its tracking technology – which the University said was introduced to improve retention rates, and improve the student experience – could not be used to identify individual students. At the time, academics raised the concern of "function creep", warning the stated purpose for collecting the data could change over time.[3]

3. Shortly after the article appeared in *The Age*, the Privacy and Data Protection Deputy Commissioner commenced preliminary inquiries into the acts and practices mentioned in the article, and whether they complied with the Information Privacy Principles (**IPPs**) in the *Privacy and Data Protection Act 2014* (**PDP Act**).

2. The Deputy Commissioner's investigation

4. As inquiries progressed, the Deputy Commissioner found that the University did not contravene the IPPs in relation to its collection and use of CCTV footage.[4] However, the use of the Wi-Fi location function was of sufficient concern that the Deputy Commissioner commenced a formal investigation under 8C(2)(e) of the PDP Act in July 2024.

5. While the Deputy Commissioner's investigation identified that the University had also searched some staff email accounts to identify staff for disciplinary action, she found that this did not contravene the IPPs.

6. Therefore, the investigation focused on whether the University's collection and use of Wi-Fi location data to identify individuals for potential disciplinary action complied with:

---

[1] The Age, 'The university vowed not to spy on students. Now it's using tracking data to punish them', *The Age*, 7 July 2024, accessed 31 January 2025.

[2] Above, n.1.

[3] ABC News, 'University of Melbourne defends wi-fi tracking of students as planning move amid privacy concerns', *ABC News*, 12 August 2016, accessed 31 January 2024.

[4] OVIC considered that the collection of personal information by CCTV was for a necessary primary purpose – to detect unlawful or antisocial behaviour and to manage its property – and was therefore compliant with IPP 1.1. The University provided students with notice of the collection of their personal information, in line with IPP 1.3. And the use of the personal information in the CCTV footage as part of misconduct proceedings was consistent with this primary purpose in the circumstances and was therefore compliant with IPP 2.1.

- IPP 1.3 - which requires an organisation to take reasonable steps to make individuals aware of certain matters[5] – such as the purposes for which the information is being collected and how it will be used – when it collects personal information.

- IPP 2.1 - which sets out that an organisation must only use or disclose personal information for the primary purpose it was collected for, or for one of the limited secondary purposes listed in IPP 2.1(a) – (h).

7. The Deputy Commissioner conducted the investigation with a view to deciding whether to issue a compliance notice to the University under section 78 of the PDP Act. An OVIC commissioner may issue a compliance notice under the PDP Act where they determine that an organisation has contravened one or more of the IPPs, and the contravention is serious, repeated or flagrant.

8. A compliance notice requires an organisation to take specified action within a specified period and is issued to ensure compliance with the IPPs.

3. The sit-in protest and the University's misconduct investigations

Sit-in protest at the Arts West Building

9. The context for the investigation related to protest activity by students and staff at the University, the University's response to this, and whether that response and the mechanisms it relied upon were consistent with the IPPs.

10. In May 2024, a group of protesters staged a sit-in protest at the University's Arts West Building, stating that they would continue this protest until their demands were met. The University's Acting Provost attended the building and made a verbal request for protesters to leave the building.

11. The protest disrupted classes in the Arts West Building and an occupational health and safety inspection found safety issues including over-crowding, and damage and obstructions to emergency exits, fire panel access, and firefighting equipment. Consequently, the building was closed.

12. On 20 May 2024, the University posted a "Notice to All Persons in Arts West" on its website containing a direction to all persons occupying the building to leave the University grounds and remove all personal property (the Direction to Leave). It also advised that refusal to comply with the direction would be subject to consequences such as suspension, internal disciplinary action, or referral to police. The Direction to Leave was read over the public address system between 8am and 10am and anyone requesting entry to the building was verbally advised by security not to enter.

[5] These matters are listed at IPP 1.3(a) –(f), OVIC website, May 2021, accessed on 31 January 2025.

13. The University continued to communicate the building closure and Direction to Leave on subsequent days and, by the end of 22 May 2024, all protesters had left the building.

What form of misconduct did the University investigate?

14. The University said that, on 20 May 2024, it commenced investigations as to whether any student misconduct had occurred. It said that this step was taken when it became clear that some individuals were not complying with the Direction to Leave issued on that day.

Student misconduct

15. "Student general misconduct" is defined in regulation 25 of the University's *Vice Chancellor Regulation* and includes improper behaviour in contravention of a University policy relating to conduct. The *Student Conduct Policy* sets out a range of behaviours that students must not engage in, and provides that a failure by a student to meet expected standards of behaviour may be dealt with as student general misconduct and the student may be subject to disciplinary action.

16. Ultimately, as a result of its investigations, the University brought misconduct proceedings against students on two counts – alleging that identified students:

> 1. ***Failed to comply with a reasonable direction or request of a senior officer or a security officer*** *– thereby engaging in general student misconduct under Regulation 25(a) of the Vice-Chancellor Regulation and section 4.5(e) of the Student Conduct Policy.*
>
> 2. ***Interfered with and/or improperly, recklessly or unsafely used University property facilities or services -*** *thereby engaging in general student misconduct under Regulation 25(a) of the Vice-Chancellor Regulation and section 4.5(f) of the Student Conduct Policy.*

Staff misconduct

17. The *University of Melbourne Enterprise Agreement 2024* governs the employment relationship between the University and University staff. Misconduct is defined in clause 1.39.1 of the agreement as including "a contravention of a lawful direction given to the Employee by an authorised Employee of the University" and "a contravention of a provision of any relevant law, University statute or regulation, the Agreement or University Policy".

18. Employees are also obliged to adhere to University policies and procedures. Clause 4.8(f) of the University's Appropriate Workplace Behaviour Policy states that employees must comply with University policies and processes and any reasonable direction by the University. Clause 4.6 provides that a contravention of this policy may be considered to be inappropriate behaviour, and on occasion misconduct or serious misconduct, and that an employee in breach of the policy may be subject to disciplinary action.

19. Thus, in terms of staff members present in the Arts West Building, the University was investigating potential failure to comply with a lawful and reasonable direction – in the form of the Direction to Leave.

How did the University identify protesters who participated in the sit-in?

Identification of students

20. As part of its investigation into whether there was any student misconduct, the University sought to identify those students who participated in the sit-in *after* it issued its Direction to Leave. The key sources for doing so were:

- Wi-Fi location data was used to identify the usernames of individuals who logged on to the University network in the Arts West Building between 20 and 23 May 2024.
- Student card photographs were located for relevant students based on the Wi-Fi usernames.
- CCTV footage was used to verify students who were present – by reviewing limited sections of footage (based on the timing of Wi-Fi access) and matching footage of student faces against student card photographs.

Identification of staff

21. As part of its investigation of whether any staff failed to comply with the Direction to Leave, the University also used Wi-Fi location data and CCTV in the same way as it did for students. However, it considered information from these sources covering a wider date range for staff – covering the entire period of the sit-in (15 to 23 May 2024).

22. Additionally, having narrowed the range of relevant staff members using these methods, it then conducted a search of 10 staff members' email accounts.

23. The University contended that the "content and context" of staff emails could indicate whether staff had contravened or intended to contravene the Direction to Leave; whether they were, in fact, present in the Arts West Building during the relevant period; and the reasons for their presence in the building.

The University's decision to use Wi-Fi location data

24. Much of the University's discussion around using Wi-Fi location data as part of misconduct investigations was verbal, with little documentary evidence. The University acknowledged this, saying that "the authorisation and instructions for [using Wi-Fi location data] were largely verbal due to the dynamic and complex nature of the situation and operating environment at that point in time". The proposal to use Wi-Fi location data to identify relevant students first arose on 20 May 2024, and the authorisation for doing so came on the same day.

25. The University also explained that the Chief Information Officer's (CIO) authorisation to use Wi-Fi location data was informed by advice from the University's General Counsel and that her advice was, in turn, supported by information provided by the Manager, Information Regulation.

26. The University confirmed during the Deputy Commissioner's investigation that, at the time advice was provided to the General Counsel, it had not been appreciated that there had been technical issues impacting the display of the ToU to new users since April 2023. The University said that "it is not clear whether this would have meant that some individuals accessing Wi-Fi from within the Arts West Building would not have seen the Terms of Use".

The University's decision to conduct discovery of staff email accounts

27. Discussions relating to the decision on conducting discovery of staff email accounts were largely via email. A member of the Human Resources team made the initial request to access relevant emails to the Director of Enterprise Technology who sought further details about the request and noted the need to get approval of the CIO.

28. The Executive Director overseeing the Human Resources team responded by email on the same day noting that "the request for email sweep is to assist with our investigation into staff that might have participated in the Arts West occupation" and noting that "[the CIO] will be aware of the request when you seek authorisation".

29. The Director of Enterprise Technology then emailed the CIO seeking approval to conduct discovery of 10 staff members' email accounts based on 16 search terms. The CIO granted approval.

30. After considering the circumstances of the email discovery, the Deputy Commissioner found that the University did not contravene the IPPs in relation to that process.

Outcome of the misconduct investigations and proceedings

31. Of the 22 identified students, 20 were issued with allegation notices and were subject to misconduct proceedings. In 18 cases, two allegations of student misconduct were substantiated. In one case, only one allegation was substantiated, while the final case was dismissed.

32. In the 19 cases where one or both allegations were substantiated, the students received a "reprimand and caution".

33. Additionally, formal meetings were held with three staff members about allegations of potential misconduct. The University substantiated these allegations in all three cases, with each receiving a formal written warning. No misconduct charges were brought against a fourth employee who explained their reasons for being in the building to their Head of School in an informal performance discussion.

4. Did the University contravene the IPPs in relation to student and staff Wi-Fi location data?

34. The investigation considered whether the University complied with IPP 1.3 and IPP 2.1 with regard to its handling of Wi-Fi location data.

IPP 1.3 – Did the University take reasonable steps to make students and staff aware of the purposes for which their Wi-Fi location data was collected?

35. IPP 1.3 sets out that:

> *At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of—*
>
> *(a) the identity of the organisation and how to contact it; and*
>
> *(b) the fact that the individual is able to gain access to the information; and*
>
> *(c) the purposes for which the information is collected; and*
>
> *(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and*
>
> *(e) any law that requires the particular information to be collected; and*
>
> *(f) the main consequences (if any) for the individual if all or part of the information is not provided.*

36. The Deputy Commissioner's investigation focused on IPP 1.3(c), which relates to the purposes of collection. This requires an organisation to take reasonable steps to inform individuals about why their personal information is being collected and how it will be used.

37. The main purpose of the IPP 1.3 requirement has been described by Bell J in the matter of *Jurecek v Director Transport Safety Victoria* as being "to promote governmental transparency and respect for autonomy and dignity of individuals with respect to their personal information".[6] This requirement is usually met by the organisation providing an individual with a notice of collection.[7]

[6] [2016] VSC 285 at [120] ('*Jurecek*').

[7] OVIC, 'Collection Notices', OVIC website, June 2019, accessed 31 January 2025.

38. OVIC's IPP Guidelines describe the rationale in a more practical way: "providing prior notice generally gives individuals the opportunity to consider whether they will proceed with their interaction with government, knowing what information will be collected and how it will be used".[8]

39. Whether a step is considered "reasonable" for the purpose of IPP 1.3 depends on the relevant context and facts. Generally, the greater the impact of a practice on an individual's privacy, the higher the threshold in terms of steps that are considered reasonable.

The University's position

40. The University referred to the following documents in asserting that it made individuals aware that Wi-Fi location data could be used to identify their whereabouts as part of a misconduct investigation:

- Wi-Fi ToU
- Provision and Acceptable Use of IT Policy (Use of IT Policy)
- Property Policy
- Student Privacy Statement
- Staff Privacy Statement.

Wi-Fi ToU

41. The University explained that the Wi-Fi ToU are "typically" provided to users (students and staff) when they first connect a device to its Wi-Fi network. It asserted that users are required to "accept" the ToU on the first connection whereas "subsequent notification and acceptance are only provided and required when updates or amendments are made to the ToU".

42. However, technical issues affecting the display of the ToU from April 2023 meant it was probable that any new users between that time and the relevant period of the sit-in would not have been prompted with the ToU when first connecting to the Wi-Fi network.

43. For staff specifically, the University stated that the Wi-Fi ToU were available to all staff via the University's internal Knowledge Base on its Staff Hub.

44. While the Wi-Fi ToU may alternatively be accessed by navigating the section of the University website relating to wireless services,[9] this method of access was only introduced after the relevant period of the sit-in.

45. In terms of content, the University pointed to sections of the Wi-Fi ToU covering the types of personal information collected when users connect to the Wi-Fi and how this is subsequently used:

[8] OVIC, 'IPP Guidelines, IPP 1 Collection', (para 1.55), OVIC website, 14 November 2019, accessed 31 January 2025.

[9] University of Melbourne, 'IT and wireless – Terms of use', University of Melbourne website, n.d., accessed 31 January 2025.

- "This network may be monitored by the University… to investigate the use of the network for breach of any laws or University policies"
- "In carrying out these activities, personal information may be collected including account usernames, IP addresses, MAC addresses and network activity".

Use of IT Policy

46. The University asserted that students and staff agree to be bound by its regulations and policies and that clause 4.10 of the Use of IT Policy explained that:

> *All actions and usage of the University IT facilities may be logged, monitored, recorded and analysed by authorised staff to facilitate the investigation of an activity that may be contrary to University policy, or to substantiate an allegation of misuse.*

47. At the bottom of the webpage on the University website which explains how users can connect to the network, there is a list of "Conditions of Use" which includes a link to the Use of IT Policy.[10]

48. The University also noted that staff are prompted with notices reflecting relevant wording from the Use of IT Policy each time they log in to University managed laptops and desktops.

Property Policy

49. The University also submitted that its Property Policy applies to staff and students. It explains that its use of surveillance is not limited to CCTV. That is, the policy refers to CCTV "or similar systems" being used for the safety and security of people and property, including by "discouraging and/or detecting unlawful and antisocial behaviour in and around University property".[11]

Student and Staff Privacy Statements

50. The University said that its Student Privacy Statement is provided to all students, and that it sets out that the University processes students' personal information "to establish and maintain your student entitlements and obligations". It claimed that this processing is necessary to "provide and administer student support services, such as health and safety, physical security, and facilities services."

51. The Staff Privacy Statement advises employees that the University "will collect personal information about you throughout your employment" which includes "information relevant to your employment and work-related matters" and that the "primary purpose for collecting the information is to maintain your employee records and to administer your employment". The University said that compliance with employment-related policies aligns with this.

[10] University of Melbourne. 'The UniWireless Network', University of Melbourne website, n.d., accessed 31 January 2025.

[11] University of Melbourne, 'Property Policy', University of Melbourne website, 12 July 2024, accessed 31 January 2025.

The Deputy Commissioner's position

52. For the reasons below, the Deputy Commissioner found that the University failed to take reasonable steps to make individuals aware of the purposes for which their Wi-Fi location data was collected and may be used, in contravention of IPP 1.3.

53. Firstly, in assessing the relevant threshold of what would be reasonable in the circumstances, the Deputy Commissioner considered the nature of the practice in question.

54. Using Wi-Fi location data to determine a person's physical whereabouts as part of a misconduct investigation is a form of surveillance.

55. Given this, the Deputy Commissioner considered that reasonable steps under IPP 1.3 would require the University to be clear, explicit, and unambiguous with students and staff that their Wi-Fi location data may be used for such purposes.

56. Applying this lens in the current circumstances, the Deputy Commissioner found that the University failed to take reasonable steps to provide notice to students and staff that their Wi-Fi location data could be used to identify their whereabouts as part of a misconduct investigation unrelated to their use of the network.

57. As noted above, the function of the Wi-Fi location data system had been amended since it was first introduced, without the University engaging in discussion with students and faculty about the changes before they were implemented. This function creep, while it happened over many years, would have necessitated clear and unambiguous guidance to people connected to the network.

58. In terms of the form of providing notice:

    - While it was intended that new users would be prompted to read and "accept" the Wi-Fi ToU, as noted above, it appears that this functionality may not have been working from April 2023.

    - It is not reasonable to assume that all individuals would have searched for and read the Use of IT Policy, Property Policy, Student Privacy Statement, Staff Privacy Statement or the Wi-Fi ToU (for staff with access to the Staff Hub) that the University relied upon.

59. More significantly, in terms of the content of the materials that the University pointed to as providing notice of the use of Wi-Fi location data:

    - The Property Policy, Student Privacy Statement, and Staff Privacy Statement provide information that is general in nature, with no reference to Wi-Fi location data or specific explanation of the circumstances and purposes for which this could be used by the University.

    - While the Wi-Fi ToU reference monitoring of the Wi-Fi network for investigations, these are described as being limited to investigating breaches of laws or University policies where the relevant conduct relates to *how a person used the network*.

    - Similarly, the Use of IT Policy mentions that usage of IT facilities may be monitored or analysed as part of an investigation into activity that may be contrary to University policy, or

to substantiate an allegation of misuse. However, from the overall context and content of the policy, it is likely that this is designed to mean and would be understood as meaning an investigation of misconduct relating to misuse of the Wi-Fi network or other IT facilities.

60. The final point above can be seen in one of the four stated objectives of the policy which is "to provide authority for the University to investigate and act on allegations of misuse"[12] – with "misuse" being defined as any use other than the authorised use of IT facilities.[13]

61. Additionally, the Use of IT Policy contains a specific section dealing with "investigations" which explains the actions that an authorised investigator may take. Importantly, it sets out that such investigative actions relate to an allegation of "misuse" which, if substantiated, would be a "significant and unacceptable use of any facilities."[14] "Misuse" is defined as set out above and "facilities" are defined as "computing and network facilities".[15]

62. The Deputy Commissioner determined that a single clause about compliance with other University policies included in a policy related to IT network use was an insufficient method of attempting to communicate the broader purposes of collection and use that the University felt it wanted to undertake. It represented an important moment of failure in the need for clear and specific communication.

63. The IPP Guidelines issued by OVIC say:

> *The primary purpose needs to be clearly stated and generally must be more specific than a reference to some broad power, for example, 'administering revenue laws', 'licensing', 'oversight of planning' or 'peace and good order'.*[16]

64. The Deputy Commissioner would have expected the University to prompt users of the Wi-Fi network with information clearly explaining that it may use their Wi-Fi location data to determine their physical whereabouts in conducting any misconduct investigation – including those where the individual's use of the network is not the subject of the suspected misconduct.

65. This did not occur. The materials that the University pointed to lacked sufficient detail, clarity, and specificity. Even if individuals had read these materials, it is unlikely they would have clearly understood their Wi-Fi location data could be used to determine their whereabouts as part of a misconduct investigation unrelated to allegations of misuse of the Wi-Fi network.

66. Given that individuals would not have been aware of why their Wi-Fi location data was collected and how it may be used, they could not exercise an informed choice as to whether to use the Wi-Fi

[12] University of Melbourne, 'Provision and Acceptable Use of IT Policy', (cl 1(d)), University of Melbourne website, 8 November 2021, accessed 31 January 2025.

[13] Above n.12 at clause 5.21.

[14] Above n.12 at clause 5.28.

[15] Above n.12 at clause 7.

[16] OVIC, 'IPP 1 – Collection' (para 1.78), OVIC website, 14 November 2019, accessed 31 January 2025.

network in the context of the possible consequences for doing so in terms of the handling of their personal information.

IPP 2.1 – Was the University's use of Wi-fi location data for the primary purpose of collection?

67. IPP 2.1 sets out the "primary purpose rule" with regard to organisations' use and disclosure of personal information. It stipulates that, unless one of the exemptions listed from IPP2.1(a) to (h) applies:

> *an organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection*

68. In assessing whether an organisation's use of personal information was consistent with the primary purpose of collection, the starting point is to ascertain what that primary purpose was.

69. In doing so, the concept of "purpose" should be understood as being "synonymous with the intent with which personal information was collected"[17] and should be defined in a specific way.[18]

70. The primary purpose of collection can be inferred from or implicit in the circumstances of collection,[19] or it may be identified from the purposes listed in an organisation's notice of collection (if one exists).[20]

The University's position

71. The University's view is that the use of Wi-Fi location data to identify individuals in the Arts West Building was permitted because it was consistent with the primary purpose for which this personal information was originally collected and would have reasonably been expected.

72. The University asserted that it collects Wi-Fi location data for the primary purposes of:

- facilitating access to the Wi-Fi service
- maintaining the network

[17] *Ng v Department of Education* [2005] VCAT 1054 at [89].

[18] OVIC, 'Key Concepts' (para 1.95), OVIC website, 14 November 2019, accessed 31 January 2025; OVIC, 'IPP 2 – Use and Disclosure' (para 2.15), OVIC website, 14 November 2019, accessed 31 January 2025.

[19] OVIC, 'IPP 2 – Use and Disclosure' (para 2.15), OVIC website, 14 November 2019, accessed 31 January 2025.

[20] OVIC, 'IPP 1 – Collection', OVIC website, 14 November 2019, accessed 31 January 2025.

- IT security and threat detection, including where necessary, identifying individuals as part of investigating activities that may indicate a realised or attempt to compromise any of the University's systems or services

- facilitating the investigation of an activity that may be contrary to University policy, or to substantiate an allegation of misuse

- performing the powers of the University under the *University of Melbourne Act 2009* (Vic) to control and manage its property, and to regulate persons entering onto the property of the University.

73. The University went on to argue that using Wi-Fi location data to identify a person's physical whereabouts as part of a misconduct investigation (even where unrelated to allegations of misuse of the Wi-Fi network) was therefore for the same purpose as that for which the information was originally collected.

The Deputy Commissioner's position

74. Wi-Fi location data is collected along with other Wi-Fi log-in information when an individual connects to the University Wi-Fi network. As noted above, this means that when an individual connects to the University network, the University collects information about which Wi-Fi access point their device is connected to and the location of this.

75. Based on the design the University has chosen for network security, the collection of Wi-Fi location data is therefore important to the operation of the University's secure Wi-Fi network, for the purposes of monitoring reliability, coverage and access. Therefore, the Deputy Commissioner considers that the primary purpose of collecting this personal information is self-evident – to facilitate access to and maintain the security of the Wi-Fi network.

76. The University asserted that, in addition to this purpose, another primary purpose of collecting Wi-Fi location data is for investigating all forms of misconduct including those unrelated to the use of the University network.

77. While accepting that an organisation may have more than one primary purpose when collecting personal information, in the present circumstances the Deputy Commissioner could not accept that investigating misconduct was a primary purpose of collecting Wi-Fi location data.

78. The University confirmed to OVIC that it collects Wi-Fi location data on a continuous basis for every user who is connected to its Wi-Fi system, but that it had never previously used Wi-Fi location data to determine an individual's whereabouts as part of a misconduct investigation.

79. Taking these facts into account, it clearly cannot be said that the University's primary purpose or intention when it initially collected the Wi-Fi location data of staff and students was to investigate misconduct that was unrelated to the use of the University network. It was about the security and functionality of the network.

80. Therefore the University's use of Wi-Fi location data in the circumstances was not for the primary purpose of collection, but was instead for a secondary purpose. In order for the University to

establish that its use of personal information was lawful, it must demonstrate that it was for one of the limited permitted secondary purposes as set out at IPP 2.1(a) – (h).

81. The University asserted alternative positions, claiming that its use of Wi-Fi location data was permitted under IPP 2.1(a) and/or IPP 2.1(e).

IPP 2.1(a) – Was the use of Wi-fi location data for a secondary purpose that an individual would reasonably expect?

82. Under IPP 2.1(a), an organisation may depart from the primary purpose rule and use personal information for a secondary purpose if:

> *Both of the following apply –*
>
> *(i) The secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;*
>
> *(ii) The individual would reasonably expect the organisation to use or disclose the information for the secondary purpose.*

The University's position

83. The University asserted that even if its use of Wi-Fi location data was not for the primary purpose of collection, it would be authorised as a use of personal information for a secondary purpose in line with IPP 2.1(a).

84. The University did not address the first limb of IPP 2.1(a). That is, it did not put forward an explanation as to how the primary and secondary purposes were "related".

85. Rather, the University's argument in relation to IPP 2.1(a) was based on its contention that "individuals would reasonably expect the use of the information for the secondary purpose" owing to the content of relevant University policies. It pointed to its Use of IT Policy, Wi-Fi network Conditions of Use, Student Conduct Policy, Appropriate Workplace Behaviour Policy, and Wi-Fi ToU.

The Deputy Commissioner's position

86. For the reasons below, the Deputy Commissioner found that the use of Wi-Fi location data to identify individuals in the Arts West Building was not for a related secondary purpose that individuals would have reasonably expected.

Related Secondary Purpose

87. As explained above, the Deputy Commissioner considered that the primary purpose of collecting Wi-Fi location data was to facilitate access to and maintain the security of the Wi-Fi network.

88. It is possible that using Wi-Fi location data to investigate usage of the Wi-Fi network – investigating a network security breach, for example – would be considered a purpose related to the primary purpose.

89. However, the use of Wi-Fi location data in the circumstances was not focussed on how individuals used the Wi-Fi network. It was used to determine their physical whereabouts, as part of a misconduct investigation unrelated to how they used the Wi-Fi network.

90. Therefore, the connection between the primary purpose of collection of Wi-Fi location data and the secondary purpose for which it was used is too remote to be considered "related".

Reasonably expected secondary purpose

91. Despite the above finding that the secondary purpose was not related to the primary purpose, the Deputy Commissioner nevertheless considered the second limb of IPP 2.1(a).

92. To assess whether a use for a secondary purpose would be "reasonably expected," it is necessary to objectively consider what an ordinary person (in the position of the person who the information is about) would consider reasonable.[21]

93. Generally, a notice of collection can create an expectation that information is to be used for related secondary purposes.[22] In this instance, IPP 2.1(a) requires that the individual would reasonably expect that the University would use their Wi-Fi location data to identify them as part of an investigation into general misconduct, unrelated to their use of that network.

94. However, as set out above, the Deputy Commissioner found that the University contravened IPP 1.3 by not taking reasonable steps to make individuals aware of the purposes for which their personal information may be used.

95. That is, in response to media reports in 2016 about concerns around the University tracking students using Wi-Fi data, the University said that:

- it "monitors and analyses Wi-Fi traffic as part of a project that's examining how intensely and effectively the University's infrastructure is used" with the project only looking at "aggregate data" rather than focusing on "individual student behaviours."[23]

- the data would be used to understand the movements of people across the campus[24] but "there was no way of identifying them individually".[25]

---

[21] OVIC, 'IPP 2 – Use and Disclosure' (para 2.35), OVIC website, 14 November 2019, accessed 31 January 2025.

[22] OVIC, 'IPP 2 – Use and Disclosure' (para 2.40), OVIC website, 14 November 2019, accessed 31 January 2025. It should be noted, however, that providing a notice of collection in compliance with IPP 1.3 will not necessarily always mean that a subsequent use is "reasonably" expected and complies with IPP 2.1(a).

[23] University of Melbourne, 'University statement on Wifi analysis on campus', University of Melbourne website, 12 August 2016, accessed 31 January 2025.

[24] ABC News, 'University of Melbourne defends wi-fi tracking of students as planning move amid privacy concerns', *ABC News*, 12 August 2016.

[25] The World Today, 'Melbourne Uni data-tracking students and staff', *The World Today*, ABC Radio National, 12 August 2016, accessed 31 January 2025.

- if the University was proposing to use the Wi-Fi location data to identify individuals, it would need to seek permission from those individuals.[26]

96. While this media coverage was from 9 years ago, it appears that the University changed policies since this time. Given the prominence and clarity of the University's public position that it would not use Wi-Fi location data to identify individuals, the Deputy Commissioner considered that there was greater onus on the University to be transparent with students and staff if it sought to depart from this position. The University did not provide individuals with a notice of collection clearly explaining that their Wi-Fi location data could be used to determine their whereabouts as part of a misconduct investigation unrelated to allegations of misuse of the Wi-Fi network. Instead, the University relied on the inclusion of a brief reference to this in its Use of IT policy to notify staff and students.

97. In conjunction with the unfortunate use of the IT policy as the mechanism for explaining use and misuse, the University did not communicate its change of position with the requisite degree of transparency. The Deputy Commissioner therefore considers that, in the present circumstances, individuals would not have reasonably expected that the University would use their Wi-Fi location data to determine their physical whereabouts as part of a misconduct investigation unrelated to how they used the Wi-Fi network.

98. Accordingly, the fact that the University subsequently decided to vary those conditions goes directly to an important concept in the interaction between privacy and technology: function or scope creep.

99. The Guidelines to the Information Privacy Principles published by OVIC say, in part:

> *'Function creep' refers to situations where personal information collected for one stated reason is later used for other purposes, perhaps quite unrelated to the original purpose of collection. The term usually arises where individuals might not have willingly provided their information or tolerated the introduction of a new potentially intrusive practice had they known what uses would eventually be made of their information. Particularly, this occurs where privacy invasive secondary uses were not originally envisaged or where assurances had been given that functions would not 'creep' or expand and the eventual uses would not occur. Function creep undermines the transparency objective of the PDP Act and is destructive of public trust in government.*[27]

IPP 2.1(e) – Was the use of Wi-fi location data a necessary part of an investigation into unlawful activity?

100. Under IPP 2.1(e), an organisation may depart from the primary purpose rule and use personal information for a secondary purpose where:

[26] Above n.24 and n.25.

[27] OVIC, 'Key Concepts' (para 1.99), OVIC website, 14 November 2019, accessed 31 January 2025.

> *a) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in; and*
>
> *b) the use or disclosure is a necessary part of the organisation's investigation of the matter or in reporting its concerns to relevant persons or authorities.*

The University's position

101. The University explained that it used Wi-Fi location data as a necessary part of its investigation based on its reasonable suspicions about the following unlawful activity:

    - Property damage, violence, and trespass offences
    - Breach of University statues and regulations.

102. The University noted that property damage and trespass are criminal offences pursuant to the *Summary Offences Act 1966* (Vic). It stated that it had reason to suspect that individuals participating in the sit-in after the Direction to Leave was issued on 20 May 2024 were engaging in trespass, noting that the Direction had specified that any individuals failing to comply would be committing trespass.

103. The University submitted that the term "unlawful activity" for the purpose of IPP 2.1(e) should not be limited to criminal activity, but should be understood as including activity contrary to civil law and rules. It therefore argued that a breach of University statutes and regulations constitute unlawful activity.

104. In terms of staff involvement in the sit-in, the University submitted that it "was investigating potential failure to comply with a lawful and reasonable direction by an employee". It elaborated that University employees are bound to adhere to the provisions of the University of Melbourne Enterprise Agreement 2024. Misconduct is described in the Agreement at clause 1.39.1 to include "a contravention of a lawful direction given to the Employee by an authorised Employee of the University".

105. The University said that the Direction to Leave was issued under the Vice Chancellor Regulation, and that it constituted both a reasonable direction under this instrument and a lawful direction under the Enterprise Agreement.

106. The University further argued that "University employees are obliged as a condition of employment to adhere to University policies and procedures". The Appropriate Workplace Behaviour Policy states at section 4.8(f) that employees must comply with University policies and processes and any reasonable direction by the University.

107. In terms of the necessity of using Wi-Fi location data as part of its investigation of suspected unlawful activity, the University said that the "use of the Wi-Fi location data to assist in identifying students or staff was a proportionate response in relation to the sit-in led by students," noting that "it was difficult to accurately identify those who were present using only the CCTV footage".

108. It asserted that not using Wi-Fi location data would have required more extensive use of the CCTV footage which "would likely have been more intrusive for the individuals concerned (including risk of mistaken identity in the absence of Wi-Fi data) and significantly more resource intensive for the University in terms of time taken and labour spent".

109. The University said that the sit-in had a "significant impact" on the University's operations and property, as well as on the wellbeing of staff and students. It asserted that the sit-in led to 814 classes and 16,950 students being impacted, with graduate researchers and staff members losing authorised access to their offices.

110. It therefore submitted that the impact on individuals' privacy through the use of their Wi-Fi location data was proportionate to the University's legitimate interests in maintaining "the good order of the University" through enforcing compliance with University statutes, regulations, policies and procedures and deterring future misconduct.

The Deputy Commissioner's position

111. The Deputy Commissioner did not consider that the use of Wi-Fi location data to identify students and staff in the Arts West Building was necessary for the purpose of investigating suspected unlawful activity. The reasons for her position are set out below.

Suspicion of unlawful activity

112. Property damage and trespass have the character of "unlawful activity" as they are criminal offences. While the University may have had reasonable suspicions about these criminal offences, it did not use Wi-Fi location data or information in staff emails in relation to these. Instead, it specifically used these to investigate student and staff misconduct.

113. The University's investigation focused on whether any students committed "student general misconduct" as defined in Regulation 25 of the *Vice Chancellor Regulation*. The definition sets out that such misconduct can include behaviour that contravenes a University policy.

114. The Deputy Commissioner agrees that unlawful activity for the purpose of IPP 2.1(e) is not limited to criminal activity[28] and should be understood as meaning contrary to law, whether civil or criminal. Additionally, the Deputy Commissioner agrees with the University's interpretation that University Statutes and Regulations have the necessary character of legislative instruments.

115. Therefore the Deputy Commissioner found that in the case of students, the relevant conduct could amount to unlawful activity, because the University was investigating contraventions of sections 4.5(e) and 4.5(f) of the *Student Conduct Policy* (failure to comply with a reasonable direction and interference with and/or improperly, recklessly or unsafely using property facilities or services, respectively), which can amount to misconduct under the *Vice Chancellor Regulation*. The Deputy Commissioner accepted that the University had reason to suspect that such unlawful activity was being or had been engaged in.

[28] *McLean v Racing Victoria* (2019) 59 VR 422 at [63] – [66].

116. However, the University's case relating to staff members relied on different instruments, namely misconduct under the University of Melbourne Enterprise Agreement 2024 and breaches of the University's Appropriate Workplace Behaviour Policy.

117. The University argued that it was "investigating potential failure to comply with a lawful and reasonable direction by an employee". The University was entitled to issue such a direction under both the Enterprise Agreement and at common law, and it says the direction was also issued under the Vice Chancellor Regulation. While the Vice Chancellor Regulation is a legislative instrument, what the University was investigating was whether staff had engaged in misconduct either under the Enterprise Agreement or, in the case of the casual staff, their employment arrangements. The Deputy Commissioner does not consider the Enterprise Agreement to be a legislative instrument.

118. The Deputy Commissioner therefore considers that the University did not have reason to suspect that unlawful activity was being or had been engaged in by staff who were involved in the sit-in. Even if it were the case that the impugned conduct of staff could amount to unlawful activity, the Deputy Commissioner considers that the same reasoning as is set out below in relation to whether it was necessary to use Wi-Fi location data to investigate students, would equally apply with respect to the situation of staff members.

Necessary part of investigation

119. The Supreme Court of Victoria has recognised that the IPPs should be interpreted as beneficial human rights legislation, noting that they give domestic legal effect to Australia's international human rights obligations.[29]

120. In *Jurecek v Director Transport Safety Victoria*, the Supreme Court described that an interpretation of what is necessary[30] should be informed by the concept of "reasonable proportionality" which requires:

> *'a consideration of what is at stake for the individual (including the nature of the personal information in question) and balancing, in a reasonably proportionate way, the nature and importance of any legitimate purpose and the extent of the interference'.*[31]

121. In the context of IPP 2.1(e), the proportionality test means that even where an organisation is investigating potentially unlawful activity in the furtherance of legitimate purposes, it cannot do so at all costs to individuals' privacy.

---

[29] *Jurecek* (n 6) [64].

[30] *Jurecek* (n 6) 70. The Court specifically considered the interpretation of the word "necessary" in the context of IPP 1.1. It is advanced, however, that the same reasoning applies to the interpretation of evaluative standards expressed throughout the IPPs.

[31] *Jurecek* (n 6) at [70]. See also *Mulholland v Australian Electoral Commission* (2004) 209 ALR 582 at [36]–[37]. This case was cited by the University in support of its interpretation of "necessity". However, that matter involved interpretation of "necessity" in the context of constitutional provisions relating to the implied freedom of political communication rather than in a human rights context, with Chief Justice Gleeson recognising the prominence of the test for proportionality in the context of human rights legislation.

122. The privacy impacts of using the personal information must be proportionate to the ends being pursued by the organisation. Broadly speaking, the more serious the unlawful conduct being investigated, the more invasive the privacy impacts that are likely to be justified.

123. In the present circumstances, it is clear that the use of Wi-Fi location data was useful to the University – in that, at a minimum, it likely sped up the investigations and made them less resource intensive.

124. However, in order to be "necessary" for the purpose of IPP 2.1(e), it is not sufficient that the use of the Wi-Fi location data was relevant, useful, or convenient[32] to achieving the ends pursued by the University, but whether it was a proportionate way of achieving such ends. This requires an assessment of the impacts on individuals' privacy weighed against the nature and importance of any legitimate purposes being pursued by the University through the investigation.

125. In the Deputy Commissioner's view, the extent of the impact on the individuals whose Wi-Fi location data was used to determine their physical whereabouts was significant. Each was subjected to a form of surveillance – in that they would not have expected that by choosing to avail of the Wi-Fi service provided by their University, their location may later be determined in an investigation unrelated to their use of the network. They are likely to have experienced a significant breach of trust.

126. Against this, the University's purpose for using individuals' Wi-Fi location data as part of misconduct investigations was to ensure the good order of the University – by taking action against non-compliance with University statutes, regulations, policies and procedures and thereby deterring future misconduct.

127. The Deputy Commissioner found that, while this was a generally legitimate purpose for the University to pursue, the nature and importance of it did not justify the extent of the impacts on individuals' privacy in the circumstances. In other words, the use of Wi-Fi location data was excessive and disproportionate.

128. The Deputy Commissioner's focus in conducting this balancing exercise was on the impact to individuals' privacy, rather than the disciplinary outcomes that resulted from using Wi-Fi-location data. The Deputy Commissioner's position would remain the same regardless of whether *not* using Wi-Fi location data would mean:

- the University could not have identified some individuals and could not have brought disciplinary action against them; or
- all relevant individuals would still have been identified through other means and would have still faced disciplinary action.

[32] OVIC, 'Key Concepts', (para 1.103), OVIC website, 14 November 2019, accessed 31 January 2025.

5. Whether to issue a compliance notice

129. Under section 78 of the PDP Act, the Information Commissioner or Privacy and Data Protection Deputy Commissioner may issue a compliance notice where it appears that there has been a serious, flagrant or repeated contravention of the IPPs. A compliance notice requires an organisation to take the action specified by the relevant OVIC Commissioner within a specified timeframe to ensure compliance with the IPPs.

130. As set out above, the Deputy Commissioner found that the University contravened IPPs 1.3 and 2.1. Taking into account the number of individuals impacted and the level of impact on these individuals, the Deputy Commissioner determined that the contraventions were "serious" for the purposes of section 78(1)(b)(i).[33]

131. The decision on whether to issue a compliance notice therefore required the Deputy Commissioner to consider the causes of the contraventions of the IPPs, any changes implemented by the University, and whether any additional action is required to ensure future compliance with the IPPs.

How did the contraventions occur?

IPP 1.3 – Failure to make individuals aware of how Wi-Fi location data could be used

132. The materials that the University pointed to as providing notice to individuals in accordance with IPP 1.3 mentioned monitoring of the IT network and use of surveillance in a general sense. Where the materials referred to investigations specifically, the context indicated that these related to investigations into the misuse of the Wi-Fi network or other IT facilities.

133. These materials were not clear, explicit, and unambiguous in informing individuals that their Wi-Fi location data may be used to identify their whereabouts as part of a misconduct investigation unrelated to their use of the network.

IPP 2.1 – Use of Wi-Fi location data for an unauthorised secondary purpose

134. For such intrusive uses of personal information, the Deputy Commissioner would have expected that any decision to proceed would have been informed by a robust analysis of the privacy impacts of using Wi-Fi location data, and whether this would comply with IPP 2.1. This did not occur.

135. Rather, there was a series of emails between the CIO, General Counsel and other relevant staff members on 20 May 2024, at the height of the sit-in, seeking to determine whether there were relevant provisions in various University policies allowing the use of the Wi-Fi location data for the desired purpose. There was only superficial consideration of IPP 2.1 in these discussions.

[33] See OVIC, Regulatory Action Policy, pp. 18-19 for a discussion of factors considered when determining whether a contravention of the IPPs is "serious", OVIC website, October 2022, accessed 31 January 2025.

136. In the Deputy Commissioner's view, this lack of basic consideration of privacy impacts was a consequence of an absence of any University policy, process, or procedure to regulate its use of surveillance and to assess whether any proposed surveillance – such as the use of Wi-Fi location data – would comply with the IPPs.

137. The Deputy Commissioner expects that any organisation considering surveillance activities should have a policy articulating its approach to surveillance and setting out appropriate roles and responsibilities for assessing, approving, and monitoring surveillance activities. This should be accompanied by a procedure requiring relevant persons to conduct an assessment of relevant factors to evaluate whether any surveillance activity would comply with the IPPs.

Does the University have sufficient controls in place to prevent similar contraventions?

138. Having made the above assessment, the Deputy Commissioner turned her attention to whether the University has sufficient controls in place now to prevent future contraventions of IPPs 1.3 and 2.1. In doing so, the Deputy Commissioner put a proposed compliance notice to the University and sought its comments on any relevant improvements the University has made since the investigation commenced. The University provided its response in a written submission, as well as an in-person discussion with the Deputy Commissioner.

Surveillance policy and procedure

139. The first proposed action was for the University to develop a surveillance policy and associated procedure:

    a) setting out a definition of surveillance; the circumstances in which surveillance may be considered for use; and a list of the different surveillance activities that it undertakes or could undertake

    b) requiring the University to properly assess whether any proposed surveillance activity complies with the IPPs (including an assessment of whether it is reasonably proportionate to the privacy impacts on individuals)

    c) setting out how any surveillance activity will be monitored while it is ongoing

    d) setting out appropriate roles and responsibilities relating to the assessment, approval, and monitoring of surveillance activities.

140. The proposed compliance notice further required that the University proactively promote the surveillance policy and associated procedure to all staff and students.

141. The Deputy Commissioner considered 12 months to be a reasonable timeframe for completing these actions, although the University indicated its intent to complete this action within a shorter timeframe, potentially towards the end of 2025.

142. The University advised that work has commenced on the development of a new surveillance policy and supporting documentation. An initial draft of the surveillance policy has been reviewed by internal subject matter experts and a further version is being prepared prior to broader stakeholder consultation.

143. The policy is supported by associated standard operating procedures (SOP) which are in the final stages of review. They include:

    a) A Wireless Network Data SOP. This describes in detail the steps governing the collection, storage, use, disclosure, retention and deletion of wireless network data. It clarifies the circumstances under which the data may be released, and the authorising environment required.

    b) A Security Safety Systems SOP. This describes the University Security Office use of systems such as fixed CCTV, Body Worn Cameras, and mobile cameras. While similar in intent to the Wireless Network Data SOP, this SOP incorporates the common use-case of law enforcement requests for CCTV footage (for example, Victoria Police).

144. The University advised that it will use existing staff and student communication channels to promote awareness of the new surveillance policy. For staff, this includes a weekly newsletter and for students, it will be via the University's student portal, the student IT page, the student IT newsletter, and the 10 faculty newsletters.

Wireless Terms of Use

145. The proposed compliance notice required the University to amend its Wireless Terms of Use to make it explicit that the University may use information from the Wi-Fi network to determine or infer an individual's location, and to explain the circumstances in which it may do so (including for misconduct investigations where an individual's usage of the network is not the subject of misconduct allegations).

146. The University advised the Deputy Commissioner that this action has been addressed. It has drafted the text in accordance with the proposed compliance notice, with the updated text used in communications to all students commencing from 24 March 2025, requesting that they accept or decline the new Terms of Use. Additionally, the University implemented a new wireless terms of use portal to capture explicit acceptance or otherwise of the updated Terms.

147. The University also advised that it will communicate the changes to the entire University community as part of its response to the first proposed action outlined above.

148. The University is currently considering amendments to the wording of the Terms of Use based on feedback received and intends to publish an updated version.

Provision and Acceptable Use of IT Policy

149. The proposed compliance notice included two actions relating to the University's IT Policy.

150. The first requires the University to amend its Provision and Acceptable Use of IT Policy to include a specific section dealing with matters relating to Wi-Fi usage which:

    a) makes it explicit that the University may use information from the Wi-Fi network to determine or infer an individual's location; and

    b) explains the circumstances in which it may do so (including for misconduct investigations where an individual's usage of the network is not the subject of misconduct allegations).

151. The second involves amending the Provision and Acceptable Use of IT Policy to include a specific section dealing with matters relating to email usage which:

    a) sets out the personal information the University collects as part of its management of the email system; and

    b) explains the purposes for which the University may review the contents of staff or student email accounts (including for misconduct investigations where the individual's email usage is not the subject of misconduct allegations).

152. The University advised that it has amended the Policy to clarify the matters raised by the Deputy Commissioner.

Notice of Collection

153. The proposed compliance notice included an action to implement a process for providing all new users of the University email system with a notice of collection that includes:

    a) an explanation of the personal information the University collects as part of its management of the email system; and

    b) an explanation of the purposes for which the University may review the contents of staff or student email accounts (including for misconduct investigations where the individual's email usage is not the subject of misconduct allegations).

154. The University advised that it has created a new Recruitment and Employment Privacy Collection Notice to cover the stages of recruitment and ongoing collection of staff information through the employment lifecycle.

155. It has updated its Staff Privacy Notice to reflect changed work practices in the new system and to be consistent with the above Privacy Collection Notice.

Report to OVIC

156. The final action in the proposed compliance notice was for the University to report to the Deputy Commissioner when each of the above actions have been implemented, including specific details of the activities undertaken for each action and provision of any documents that are revised or created as a result of the compliance notice.

157. The University agreed to provide the details and evidence requested.

The Deputy Commissioner's decision not to issue a compliance notice

158. Based on the University's cooperation throughout the investigation, and its undertakings in writing and in person to meet the above requirements, the Deputy Commissioner decided that it was not necessary to issue a formal compliance notice. Nonetheless, the Deputy Commissioner remains concerned by the University's practices outlined throughout this report, and will continue to seek evidence and assurance that it has completed the actions it has agreed to.

Annexure A

Professor Emma Johnston AO
Vice-Chancellor
FAA FTSE

11 August 2025

Ms Rachel Dixon
Privacy and Data Protection Deputy Commissioner
Office of the Victorian Information Commissioner
PO Box 24274
MELBOURNE VIC 3001

By email: investigations@ovic.vic.gov.au

Dear Ms Dixon,

Subject: Final report on investigation into the University's surveillance of protesters

Thank you for your letter of 5 August and for the opportunity to respond to your final report. Please find the University's response as follows:

The University takes its privacy obligations seriously and has cooperated openly and responsively to the Deputy Commissioner in the conduct of her investigation which is the subject of this Report. We have appreciated the opportunity to engage throughout the process.

The University is committed to complying with the *Privacy and Data Protection Act 2014* and the Information Privacy Principles and will implement the actions proposed by the Deputy Commissioner in the Report. The University has already completed a number of these and all others are in train.

The University acknowledges that it could have provided clearer active notice to students and staff members in relation to the use of WiFi location data. However, the University does not accept that any shortfall constituted a serious contravention of IPP 1.3.

The University also maintains that the use of WiFi location data in student misconduct cases was a necessary part of the University's investigation into potentially unlawful activity, and so was permissible under IPP 2.1(e). Unlawful activity covers activity contrary to student policies. The use of this technology in the circumstances was reasonably proportionate, given the limited personal information involved, the small number of people who had access to that information and the overriding need to keep our community safe and conduct our core activities of teaching, learning and research.

Yours sincerely,

Professor Emma Johnston
Vice-Chancellor

cc: privacy-officer@unimelb.edu.au

3684833, 3682072

Office of the Vice-Chancellor
The University of Melbourne, Victoria 3010 Australia
T: +61 3 8344 6134 | E: vc@unimelb.edu.au | **unimelb.edu.au**