Supplementary Submission No 39A

INQUIRY INTO WORKPLACE SURVEILLANCE

Organisation: Office of the Victorian Information Commissioner (OVIC)

Date Received: 2 October 2024

Office of the Victorian Information Commissioner

Phone: 1300 00 6842
Email: enquiries@ovic.vic.gov.au
PO Box 24274
Melbourne Victoria 3001

2 October 2024

Alison Marchant MP
Chair, Legislative Assembly Economy and Infrastructure Committee
Parliament of Victoria

By email only: worksurveillanceinq@parliament.vic.gov.au

Dear Chair,

Supplementary submission to the Legislative Assembly Economy and Infrastructure Committee Inquiry into workplace surveillance

Thank you for the opportunity to attend a hearing with the Committee on 3 September 2024. As discussed during our hearing, the Office of the Victorian Information Commissioner (**OVIC**) has prepared a supplementary submission that further clarifies its position on reforms to workplace surveillance.

The supplementary submission covers the following key points:

1. Expanding the application of Part 4 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).
2. Classifying biometric information as sensitive information.
3. Introducing a mandatory incident notification scheme.
4. Requiring organisations to ensure compliance with the Information Privacy Principles (**IPPs**).
5. Considering the design of, and regulatory responsibility for, prospective workplace surveillance laws.

If the Committee would like clarification on any points made in the supplementary submission or would like to discuss the privacy considerations of workplace surveillance further, please contact us through Cameron Cruwys, Senior Policy Officer, at [redacted]

Yours sincerely

[redacted]

Sean Morrison
Victorian Information Commissioner

Supplementary submission to the Inquiry into workplace surveillance

Summary of supplementary recommendations

1. That the following changes are made to the PDP Act:
    a. Expand the application of Part 4 of the PDP Act to include exempt entities.
    b. Change the definition of sensitive information to include biometric information.
    c. Introduce a mandatory incident notification scheme.
    d. Introduce a new IPP that places a positive obligation on organisations to ensure compliance with the IPPs.
2. That the Committee focus workplace surveillance reform on describing clear rules employers must follow to design and implement a workplace surveillance activity that respects and protects employees' right to privacy. These rules should be based on reasonableness, necessity and proportionality.
3. That the Committee insert new workplace surveillance rules into the PDP Act, with OVIC as the regulator.

Necessary changes to the PDP Act

OVIC is of the position that the PDP Act must be amended to sufficiently regulate Victorian public sector (**VPS**) entities' use of workplace surveillance. The required amendments are:

1. Expanding the application of Part 4 of the PDP Act.
2. Classifying biometric information as sensitive information.
3. Introducing a mandatory incident notification scheme.
4. Introducing a new IPP that places a positive obligation on organisations to ensure compliance with the IPPs.

Expanding the application of Part 4 of the PDP Act

Under Part 4 of the PDP Act, the Information Commissioner has developed the Victorian Protective Data Security Framework and Victorian Protective Data Security Standards (**VPDSS**).[1] The VPDSS establish 12 high-level, mandatory requirements to protect public sector information across all security areas including governance, information, personnel, Information Communications Technology and physical security.

[1] See more information on the Victorian Protective Data Security Framework at https://ovic.vic.gov.au/information-security/framework-vpdsf/, and on the Victorian Protective Data Security Standards at https://ovic.vic.gov.au/information-security/standards/.

However, Part 4 does not apply to certain entities that are subject to the other information privacy obligations under the PDP Act.[2] These include (but are not limited to):

- councils;
- universities; and
- public health service entities and public hospitals under the *Health Services Act 1988* (Vic).

These exclusions mean these entities are not subject to mandatory data security standards in the way that other VPS entities are. In the context of workplace surveillance, this means that personal information collected by these employers (via surveillance) may not be held and handled in ways that respect its confidentiality, integrity and availability.

In some circumstances, these employers collect delicate information[3] through surveillance activities, such as bodycam footage. Workplace surveillance activities mean more personal information about an employee is being collected than if the activity was not taking place. Therefore, more personal information is at risk of being compromised. OVIC's view is that the currently excluded entities should be required to comply with Part 4 of the PDP Act, to minimise the risk of compromise to personal information, and other public sector information.

Classifying biometric information as sensitive information

OVIC's previous submission detailed why it is critical for biometric information to be considered sensitive information under the PDP Act. In short, biometric information cannot be replaced or changed. This means a breach of this information could have devastating and ongoing consequences for a person. Growing accessibility of biometric surveillance technology is compounding this risk. Classifying biometric information as sensitive information will require employers to satisfy additional criteria before implementing biometric surveillance in the workplace.

Introducing a mandatory incident notification scheme

VPS organisations are not required to report incidents to OVIC, nor to affected individuals. Under the VPDSS, organisations must notify OVIC of certain information security incidents,[4] however this does not:

- extend to all information security and privacy incidents;
- include notification to affected individuals; or
- apply to all VPS organisations, given the limitations on the applicability of Part 4 of the PDP Act, as discussed above.

In contrast, organisations covered by the *Privacy Act 1988* (Cth) (**Privacy Act**) must notify affected individuals and the Office of the Australian Information Commissioner (**OAIC**) when a data breach is likely to result in serious harm to an individual whose personal information is involved. NSW carries a similar requirement that applies to NSW public sector organisations, and in July 2025, a similar scheme will commence in Queensland under the *Information Privacy Act 2009* (Qld). At the time of writing, a

[2] See section 84(2) of the PDP Act.
[3] 'Delicate information' refers to personal information that is of a private or personal nature, or information that the individual it is about would likely regard as requiring a higher degree of protection.
[4] See OVIC's website for further information on the information security incident notification scheme: https://ovic.vic.gov.au/information-security/ovic-information-security-incident-notification-scheme/.

Privacy and Responsible Information Sharing Bill is before the Western Australian Legislative Council, which also includes a mandatory information breach notification scheme.

The lack of a mandatory incident notification scheme in Victoria means individuals who are affected by a data breach may not even be aware that their personal information has been misused, lost or subject to unauthorised access, modification or disclosure. This can adversely affect that individual's capacity to minimise the harm of that data breach, for example, by cancelling a card or changing a password.

Workplace surveillance can collect delicate information about employees and some surveillance instances can be unavoidable. Therefore, a mandatory incident notification scheme should apply to this information and all Victorians' personal information held by VPS organisations. A mandatory incident notification scheme is in line with the fundamental principle of harm minimisation when a data breach occurs. This scheme should sit within the PDP Act *and* be included in the broader application of any workplace surveillance reform.

Introducing a new IPP that places a positive obligation on organisations to ensure compliance with the IPPs

Privacy governance is an increasingly important element of privacy protection. Australian Privacy Principle (**APP**) 1.2 requires Commonwealth agencies and private sector APP entities to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APP framework.

OVIC recommends a new IPP is introduced and modelled on APP 1.2. In the context of workplace surveillance, this would require employers to have systems, procedures and processes in place that govern a workplace surveillance activity. This means strengthening privacy awareness and embedding privacy into the design of a workplace surveillance activity, rather than viewing privacy as a mere compliance checkbox, or retrospectively considering the privacy implications of an active surveillance tool. This approach better reflects privacy as a human right.

The IPPs provide privacy protection but may not be accessible to non-VPS entities if applied to them

With these changes, OVIC believes the PDP Act and IPPs would be sufficient to regulate VPS entities' use of workplace surveillance. However, the PDP Act does not apply to private sector entities. Prospective workplace surveillance reform would presumably intend to cover both private and public sector organisations.

Applying the IPPs where a private sector organisation engages in an act of workplace surveillance may be a policy solution. Here, the IPPs would provide comprehensive surveillance protection for employees. Inserting a new Workplace Surveillance Part into the PDP Act would achieve this and should only apply to acts of workplace surveillance. Though, the Committee should consider whether compliance with and interpretation of the IPPs would be too burdensome for smaller organisations. Inaccessibility may lead to deliberate non-compliance or a greater volume of accidental non-compliance. Inaccessibility could also be an issue for aggrieved employees.

While some organisations may not have the resources or corporate knowledge to engage with the IPPs, the privacy risks inherent to a workplace surveillance activity are no less significant. Therefore, these and all organisations must be covered by prospective legislation.

While the IPPs would provide protection in theory, more prescriptive rules in relation to an act of workplace surveillance may be appropriate. For example, in the way the IPPs address proportionality regarding an act of workplace surveillance. IPP 1.2 states that an organisation should only collect information through fair means. OVIC is of the view that this provision captures that a workplace surveillance activity should be proportionate to its objective — that there is no less intrusive means to accomplish it. However, this may not be apparent to an organisation unfamiliar with the IPPs or legislative interpretation. A more prescriptive rule that makes proportionality more explicit may be of greater usability to employers and employees.

The Committee must also consider where regulatory responsibility for this more prescriptive workplace surveillance legislation should be placed.

Regulatory responsibility

Workplace surveillance interacts with two separate policy areas: industrial relations and privacy

Where regulatory responsibility for workplace surveillance should lie, depends on the design of prospective workplace surveillance laws. Workplace surveillance reform sits between industrial relations policy and privacy. Reforms that emphasise negotiation, bargaining and consultation between employers and employees would reflect an industrial relations approach. Whereas clear rules on collection, use, disclosure, retention, disposal, access to and security of data gained through workplace surveillance would represent a privacy-based approach. The Committee must decide how it will position its recommended reforms.

- **An industrial relations approach**

  Negotiation and bargaining between employees and employers could be the primary driver of workplace surveillance regulation. In this case, organisations such as WorkSafe or the Wage Inspectorate have the knowledge and existing relationships to most effectively regulate workplace surveillance. For example, where employees and employers have reached an agreement on the use of workplace surveillance, a dispute would likely involve a contract breach by either party and require industrial relations expertise to resolve.

- **A privacy-based approach**

  Alternatively, workplace surveillance laws could be regulated through the legislation of fundamental privacy rules or principles that employers must follow. A breach from this policy perspective would entail a breach of a worker's privacy rights. In this case, OVIC is the most appropriate regulator to oversee workplace surveillance in Victoria. This approach would ensure consistent enforcement and interpretation of privacy law in Victoria.

  Further, having a single regulator for privacy laws will make them easier for Victorians to navigate. OVIC recommends that if privacy-based workplace surveillance rules include private sector organisations, OVIC's jurisdiction should be expanded to include workplace surveillance activities undertaken by those private sector organisations. This would require coordination with the OAIC and the Privacy Act to ensure consistency and best practice between new workplace surveillance

rules and the APPs in relation to organisations covered by both. OVIC would be able to leverage its existing relationship with the OAIC to achieve this.

- Dual regulators

The Committee may also consider dual regulators for workplace surveillance. This approach would combine the two options above, where OVIC would be responsible for the privacy aspect of the legislation and another regulator (such as WorkSafe or the Wage Inspectorate) would be responsible for the industrial relations aspect of the legislation. For example, OVIC would administer the collection, use, disclosure, retention, security and disposal of employees' personal information collected through a workplace surveillance activity. Another body would administer any particular workplace agreement between employers and employees.

A similar structure is in place where OVIC regulates the IPPs which cover personal information, and the Health Complaints Commissioner (**HCC**) regulates the Health Privacy Principles (**HPPs**) that cover health information. Organisations have similar statutory obligations under both the IPPs and HPPs, however, the two-regulator approach creates administrative inefficiencies for those organisations and for the public when exercising their complaint rights. For example, a complaint that involves both personal (IPP-related) and health information (HPP-related) must be made to both OVIC and the HCC because of the limits of both regulators' enabling legislation. The Integrity and Oversight Committee has since recommended in its final report on the Inquiry into the operation of the *Freedom of Information Act 1982* (Vic) that the HPPs and IPPs should be consolidated because of administrative inefficiencies and potential for confusion.[5] OVIC is of the view that similar issues will arise if workplace surveillance laws were administered by two regulators and thus a single regulator would be more appropriate. Here, simplicity of design can enhance compliance.

Resourcing

Any organisation (or organisations) that takes on the role of workplace surveillance regulator will require greater resourcing. Access to surveillance technology is ever increasing, as mentioned in OVIC's initial submission, and governing employers' use of this technology will be a substantial and exponentially demanding task. Inadequate resourcing means ineffective regulation and an inability to resolve harmful incidences of workplace surveillance.

If the Committee intends to recommend that workplace surveillance oversight sit with an existing regulator (or regulators), OVIC recommends that the Committee discuss the potential resourcing requirements with that regulator, prior to making its recommendations.

[5] Integrity and Oversight Committee. The operation of the *Freedom of Information Act 1982* (Vic) — Final report. Recommendation 96.

The design of workplace surveillance laws

Negotiation-oriented rules may not protect workers and employers

The power dynamic in the employee-employer relationship can complicate the good faith of negotiation and authenticity of employee consent. Employees in some workplaces may feel pressured into consenting to something or may feel as though there is no other option. In this way, employees' privacy may not be sufficiently protected. This is heightened in industries where employment is highly competitive. It would be harmful to create an employment environment where those most willing to sacrifice their privacy are the most desirable employees.

Conversely, there may be some workplaces that require a particular workplace surveillance activity for health and safety purposes though employees refuse to consent to it. A law that focuses on the protection of Victorians' right to privacy can straddle these issues. Providing clear and uniform rules gives employees and employers regulatory certainty. It would balance the primary concerns of both parties — that is, protect employees' privacy while maintaining employers' discretion to implement necessary surveillance activities. Since privacy is a human right under the Charter of Human Rights and Responsibilities, legislating more prescriptive steps an employer must take if encroaching on this right makes sense.

OVIC's recommendations

OVIC is of the view that workplace surveillance is fundamentally a privacy issue, that is, an activity is harmful where it intrudes upon an employee's right to privacy. Protecting this right can mitigate the harm caused by workplace surveillance. It follows that the focal point of workplace surveillance law should be the protection of workers' right to privacy.

OVIC therefore recommends that the Committee focus prospective legislation on enshrining privacy protection in the workplace similar to, but more specific than, the protection found in the IPPs. Reform should require an employer to consider the reasonableness, necessity and proportionality of an act of workplace surveillance. Part of this should be a requirement for employers to document and provide to employees a clear, specific purpose for the workplace surveillance activity. This documentation is essential to identifying and preventing function creep, or the use of data collected for the specified purpose for another unrelated purpose. It is also a mechanism for accountability of the employer to the employees regarding the use of those employees' personal information without restricting *necessary* workplace surveillance activities.

Any new rules should be incorporated into the PDP Act. OVIC already regulates workplace surveillance in the VPS and to this end, OVIC has the institutional knowledge and experience to effectively regulate workplace surveillance more broadly. This would allow legislators to leverage an existing regulatory body and negate the administrative and resource-heavy process of establishing a new organisation.

OVIC already takes a consultative education role in relation to privacy and data security with VPS organisations. Any workplace surveillance-specific legislation will require the development of educative resources, direct engagement with organisations and public-facing material that helps

Victorians engage with the new laws. This critical component of compliance must focus on privacy as a human right to increase awareness of what workplace surveillance laws are trying to achieve and why it is worth achieving.

Workplace surveillance reform should also describe the rules of collection, use, disclosure, retention, disposal, access and security of employees' personal information. A key concern is that employers may not store data securely and may not dispose of data once it is no longer of use. Incorrect storage and unnecessary retention of data increases the risk of employees' personal information being misused or inappropriately accessed, and makes employers a target for malicious actors. Employers should be required to protect its employees' personal information particularly where it is collected through surveillance. Further, data should not be retained beyond use for the purpose for which it was collected. This means data cannot be retained 'just in case'. The statement of a clear purpose that satisfies reasonability, necessity and proportionality will help employers to understand what that specific purpose is and when data should be deleted.

If OVIC were to regulate workplace surveillance more broadly, OVIC would require referral powers similar to those in Division 2D of the *Ombudsman Act 1973* (Vic). There will be instances where a privacy complaint about a workplace surveillance activity may be part of a broader industrial dispute, or where workplace surveillance has been used to unfairly dismiss an employee. In these cases, OVIC would refer the complaint to a more appropriate body and provide advice to that body on the privacy aspects of the case.