Submission No 39

INQUIRY INTO WORKPLACE SURVEILLANCE

Organisation: Office of the Victorian Information Commissioner (OVIC)

Date Received: 2 August 2024

Office of the Victorian Information Commissioner

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

2 August 2024

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

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

Dear Chair,

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

Thank you for the opportunity to provide a submission in response to the Legislative Assembly Economy and Infrastructure Committee (**the Committee**) Inquiry into workplace surveillance (**the Inquiry**). The Office of the Victorian Information Commissioner (**OVIC**) has combined oversight of freedom of information, information privacy and information security, administering both the *Freedom of Information Act 1982* (Vic) (**FOI Act**) and the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

The PDP Act covers Victorian public sector (**VPS**) organisations and their collection, use, disclosure, retention, security and disposal of personal information. My office has a particular interest in workplace surveillance issues, given the potentially significant impacts on individuals' privacy rights.

The following submission outlines VPS organisations' obligations under the PDP Act when considering workplace surveillance. It draws on OVIC's Guiding Principles for Surveillance,[1] published in 2021, and includes recommendations for the Committee to consider in progressing the Inquiry.

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

Yours sincerely

[redacted]

Sean Morrison
Victorian Information Commissioner

[1] Available at https://ovic.vic.gov.au/privacy/resources-for-organisations/guiding-principles-for-surveillance/.

Submission to the Inquiry into workplace surveillance

Privacy is a fundamental human right enshrined in *Victoria's Charter of Human Rights and Responsibilities* (**the Charter**) and in the United Nations *Universal Declaration of Human Rights*. Privacy is central to an individual's right to live a full, free and dignified life, without fear of coercion or persecution for who they are or what they choose to believe. In this way, privacy is closely interlinked with other human rights such as the freedom of conscience, thought and belief, freedom of expression and freedom of association.

Any form of surveillance may interfere with this right to privacy. Surveillance in the workplace can include, but is not limited to, the use of CCTV, remote invigilator software, analytics software, user management and monitoring tools, artificial intelligence, or tracking employee logins and activity.

Workplace surveillance has increased in the last few years as technology makes surveillance tools more readily available. This has been aided by increasingly flexible work arrangements in some industries, including 'work from home' and 'remote working' models of employment. This equates to an increase in both the supply and demand of workplace surveillance technologies.

This submission will discuss:

- how the PDP Act and Information Privacy Principles (**IPPs**) relate to workplace surveillance;
- broader regulation of workplace surveillance;
- enquiries received by OVIC about workplace surveillance; and
- the potential impacts on individuals from workplace surveillance.

Current privacy laws

In Victoria, privacy and data protection practices of VPS organisations are governed by the PDP Act.

The PDP Act contains 10 IPPs for the collection, use, disclosure, security, retention and disposal of personal information. The IPPs exclude health information, as this is covered by the *Health Records Act 2001* (Vic) (**HR Act**), which is administered by the Health Complaints Commissioner.

Most VPS organisations are also bound by the Victorian Protective Data Security Standards (**VPDSS**) – 12 mandatory standards that protect public sector information across all security domains, including governance, information security, physical security, personnel security and ICT security.[2]

Contracted service providers (**CSPs**) to VPS organisations can also be bound by the IPPs if the contract between the parties so provides.[3] Under a contract, a CSP that chooses to subcontract a function or activity to a subcontractor may pass obligations under the IPPs to that subcontractor.

[2] See section 84 of the PDP Act for a list of organisations required to comply with Part 4 – Protective data security. The VPDSS are available at https://ovic.vic.gov.au/information-security/standards/.
[3] See section 17 of the PDP Act for the effects of outsourcing.

Private organisations are excluded from the PDP Act and are instead governed by the *Privacy Act 1988* (Cth) (**Privacy Act**), administered by the Office of the Australian Information Commissioner. The Privacy Act sets out 13 Australian Privacy Principles (**APPs**) that are largely similar, but not identical, to the 10 Victorian IPPs. The Privacy Act has exemptions from its application:[4]

- most small businesses with an annual turnover of $3 million or less;
- registered political parties;
- employee records of current or former private sector employees; and
- media organisations.

These four exemptions were recommended to be either removed or modified in the Attorney-General's Privacy Act Review Report 2022, however these changes are yet to be legislated.[5] This means any workplace surveillance activities administered by these types of organisations do not consider either the IPPs or APPs. The lack of privacy regulation for these entities can be detrimental to employees' privacy and employment conditions.

Surveillance more broadly is covered by the *Surveillance Devices Act 1999* (Vic). This legislation applies to all Victorians and Victorian organisations and provides regulation for the installation, use and maintenance of the following:[6]

- listening devices;
- optical surveillance devices;
- tracking devices; and
- data surveillance devices by law enforcement officers.

Part 2A pertains to workplace surveillance and prohibits:

- the use of optical or listening surveillance devices in toilets, washrooms and similar areas; and
- the communication or publication of a record or report of an activity monitored by the use of an optical or listening surveillance device.

Workplace surveillance and the IPPs

The IPPs provide a principles-based regulatory approach to safeguard citizens' personal information. The PDP Act defines personal information as:

> *information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.*

[4] See sections 6C, 6D, 7B, 7D of the *Privacy Act 1988* (Cth).
[5] Attorney General's Department (2022). *Privacy Act Review Report,* pages 6-7. Available at https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.
[6] Part 2, *Surveillance Devices Act 1999* (Vic).

Most surveillance activities require the collection of personal information, and any recorded opinion on an employee arising from that surveillance also constitutes personal information. Surveillance activities that do not collect personal information, as defined by the PDP Act, are not covered by the IPPs. This could include the collection and use of aggregated employee data, if an individual would not be reasonably identifiable.

IPP 1 – Collection

IPP 1 sets out obligations on VPS organisations when collecting personal information about an individual. It ensures that personal information is not arbitrarily collected. Surveillance that collects personal information must be necessary for one or more of the organisation's functions or activities and cannot be collected illegally, through unfair means or in an unreasonably intrusive way. This means workplace surveillance activities should not be utilised simply because they are available – but because there is no less intrusive means to achieve the desired outcome.

A VPS organisation that conducts any workplace surveillance activity that collects personal information must provide its employees with a notice of collection. This means any covert workplace surveillance activity that collects personal information is a breach of the PDP Act, unless enabled by other legislation. The notice of collection must include the following information, as required by IPP 1.3:

- the identity of the organisation and how to contact it in relation to the collected personal information;
- the fact that the individual is able to gain access to the information;
- the purposes for which the information is collected;
- to whom the organisation usually discloses information of that kind;
- any law that requires the information to be collected; and
- the main consequences for the individual if all or part of the information is not provided.

The IPPs do not require an employer to gain an employee's consent to collect their personal information. However, the collection of sensitive information, such as racial or ethnic origin, usually requires consent. See the discussion on IPP 10 below for more on sensitive information.

IPP 2 – Use and Disclosure

IPP 2 restricts the use and disclosure of personal information to the purpose for which it was collected (the primary purpose), with limited exceptions. In a workplace surveillance context, IPP 2 should prevent function creep of surveillance activities by an employer. For example, surveillance undertaken for the purpose of protecting employee physical safety cannot subsequently be sold to third parties for monetisation. Employers can seek consent from employees to use their personal information for

other purposes, however, consent may be void if it is coerced, for example, attained as a condition of continued employment.[7]

Organisations can use and disclose personal information for a purpose other than the primary purpose of collection in limited circumstances.[8] In some cases, organisations may be required to disclose personal information to a law enforcement agency investigating a breach of law. VPS organisations should familiarise themselves with the circumstances under which they can, or must, disclose personal information. Employees should also be made aware of organisations' obligations to disclose personal information at the time it is collected.

IPP 4 – Data Security

Surveillance activities generate personal information that may be susceptible to data breaches, meaning surveillance inherently increases privacy risk to employees. IPP 4 requires organisations to protect the personal information they hold from misuse, loss, and unauthorised access, modification or disclosure. Any personal information collected through surveillance must be securely stored, and once no longer needed for any purpose, destroyed or permanently de-identified. Retaining surveillance information for longer than required poses a security risk.

Most VPS organisations are also required to adhere to the VPDSS. The VPDSS are consistent with national and international security standards and cover governance, information security, personnel security, ICT security and physical security. Any handling of workplace surveillance information by VPS organisations covered by Part 4 of the PDP Act will be subject to the VPDSS.

IPP 5 – Openness

IPP 5 requires organisations to be transparent about their handling of personal information. Privacy policies should be clear and accessible. The primary purpose of the policy is to tell individuals how the organisation handles personal information. A clear and accurate privacy policy supports workplace surveillance activities and can inform workers of how their personal information is treated. OVIC recommends organisations schedule a regular review of their privacy policy, to ensure it accurately reflects their personal information handling practices.

IPP 9 – Transborder Data Flows

IPP 9 lists the circumstances by which an organisation may transfer personal information about an individual to someone who is outside Victoria. These circumstances include with the individual's consent, if the recipient is subject to a law substantially similar to the IPPs, or the organisation has taken reasonable steps to ensure that the information will not be handled by the recipient in a way that is inconsistent with the IPPs (for example, by contractually binding them to the IPPs).

[7] See the Guidelines to the Information Privacy Principles for further detail on what constitutes valid consent: https://ovic.vic.gov.au/book/key-concepts/#Consent.
[8] See IPP 2.1.

Surveillance activities in the workplace can involve the use of software to monitor employees' use of technology. The information gathered by this software is sometimes stored in servers in other jurisdictions that are beyond the control of the organisation conducting the surveillance. Organisations in other jurisdictions may not have the same controls in place as VPS organisations in Victoria, meaning VPS employees' personal information may not be protected when retained elsewhere.

IPP 10 – Sensitive Information

Sensitive information is defined in Schedule 1 of the PDP Act as information or an opinion about an individual's:

- *racial or ethnic origin; or*
- *political opinions; or*
- *membership of a political association; or*
- *religious beliefs or affiliations; or*
- *philosophical beliefs; or*
- *membership of a professional or trade association; or*
- *membership of a trade union; or*
- *sexual preferences or practices; or*
- *criminal record*
- *that is also personal information.*

IPP 10 outlines the circumstances in which organisations can collect sensitive information. One of these circumstances is with the individual's consent. Workplace surveillance activities that collect sensitive information may require the consent of the employee.

While the Privacy Act categorises biometric information as sensitive, the PDP Act contains no such protection.[9] Some forms of biometric information may be captured by the HR Act where it is also health information, however, biometric information used in technologies such as facial recognition, voice recognition, iris or fingerprint scanning, and eye movement detection, do not require consent to be collected under the IPPs.

OVIC strongly recommends that the Committee consider whether biometric information that is not captured by the HR Act should be included as sensitive information in the PDP Act. This would bring the treatment of biometric information in line with current federal privacy law, and with international jurisdictions.

While biometric authentication can offer some security advantages, the risks to individuals' privacy are greatly increased unless used in conjunction with significant protections. An example of this protection is facial recognition technology in iPhones. An iPhone uses biometric authentication (facial recognition) to unlock, but the "key" created with the biometric is stored only on the phone and is encrypted in a combination of the biometric template, the device ID on which the information is being encrypted, and another factor. This means the biometric information cannot be reverse engineered to

[9] See definition of 'sensitive information' in section 6 of the Privacy Act.

reproduce a person's face and makes the authentication information useless outside of unlocking that specific device. Biometrics in other contexts, such as fingerprint scanners, may be able to be linked directly to individuals and reverse engineered by malicious actors.

A limitation of biometric systems is that unlike passwords, biometric characteristics cannot be reissued or cancelled. If a person's fingerprint or other physiological biometric is compromised, it can be extremely difficult – if not impossible – to change.

Individuals use biometrics for a range of purposes not tied to their employment, and continuous advancements in technology are improving artificial reproduction of biometric information, such as deepfake technology. Any privacy breach resulting in the unlawful collection of an individual's biometric information could result in severe outcomes for that individual, such as ongoing identity fraud.

For these reasons, OVIC also recommends that the Committee consider the exceptional treatment of biometric information in relation to workplace surveillance. This could take the form of more stringent limitations or conditions on the use of biometric surveillance, or additional risk assessments undertaken prior to its commencement.

Recommendation 1: That the Committee consider whether biometric information that is not captured by the *Health Records Act 2001*, should be included as sensitive information under the PDP Act.

Recommendation 2: That the Committee consider the exceptional treatment of biometric information in relation to workplace surveillance.

Enquiries to OVIC regarding workplace surveillance

As the primary privacy regulator for the VPS, OVIC has received several enquiries from employees regarding workplace surveillance practices of organisations bound by the PDP Act. These enquiries have related to the following:

- use of CCTV in the workplace and appropriate notice of collection, security controls and retention policies;
- use of work mobile phones, including mobile phones that support multiple SIM cards and are for both personal and professional use;
- how employers can access private information on devices that are for both personal and professional use;
- use of location data applications that require staff to sign in (or check in) at certain locations when working off site;
- collection and policy requirements to use technical computer features to track staff when working remotely;
- when CCTV footage can be used and disclosed; and
- when organisations can access personal devices during investigations.

These enquiries demonstrate the prevalence of workplace surveillance within the VPS, and that VPS staff are concerned about their employers' potential or actual surveillance activities.

Artificial intelligence and workplace surveillance

Artificial intelligence (**AI**) monitoring tools are being increasingly adopted by employers for a range of purposes, including to surveil workers. AI surveillance systems can include automated evaluation of employee performance, monitoring of email and other digital content, or analysis of data collected through non-AI surveillance methods.[10] When VPS organisations collect personal information to train an AI model, feed personal information into an AI system, or use AI to infer information about individuals, the IPPs apply.

The use of AI systems should be necessary and proportionate to achieve the identified objective – they should not be deployed simply because they are available. This is particularly important given the potential risks associated with the use of an AI system, including the risk of discrimination, bias and inequality. This is compounded by 'AI hallucinations' where AI systems infer or provide information that is incorrect. The detection of AI bias and hallucinations in surveillance systems may be difficult to identify and lead to unfair treatment of employees or unjust recruitment processes.

Impacts and consequences of workplace surveillance

There are many reasons an employer may wish to surveil employees, such as performance management, workplace health and safety, and meeting other obligations such as the positive duty to prevent workplace sexual harassment. But regardless of its purpose, surveillance is an asymmetrical transfer of information and affects the balance of power between employees and employers. It gives control of employees' personal information to their employer, and interferes with employees' right to privacy.

Surveillance can deter people from exercising their right to freedom of expression and freedom of thought, conscience and belief. Some academics argue that the actual fear of being prosecuted for doing something wrong is unlikely to fully account for the self-censorship that surveillance can cause.[11] This means employees – in being aware of being surveilled – may overly self-censor in the workplace, affecting freedom of expression, openness and diversity within an organisation. In VPS organisations, this can manifest as cultures of fear and complicity. This is particularly problematic in a sector that requires impartiality, frankness and fearlessness from its employees. A culture of surveillance is not conducive to reciprocal trust.

Workplace surveillance activities collect additional information relating to employees than otherwise would have been collected if the activity did not take place. The more personal information retained by an organisation about an individual, the greater the risk of that individual's privacy being breached. A data breach occurs when personal information held by an organisation is subject to misuse or loss or to unauthorised access, modification or disclosure. A data breach can be caused deliberately because of a malicious act from an external or internal party or caused by human error or a failure to implement effective information management.

[10] Greenhouse S. (2024). *Constantly monitored': the pushback against AI surveillance at work.* Available at https://www.theguardian.com/technology/2024/jan/07/artificial-intelligence-surveillance-workers.
[11] Penney J. (2016). *Chilling effects: Online surveillance and Wikipedia use.* Berkley Technology Law Journal, 31(1). Available at https://btlj.org/data/articles2016/vol31/31_1/0117_0182_Penney_ChillingEffects_WEB.pdf.

The potential negative consequences of a data breach depend on the kind of information involved in the breach. The more intrusive a workplace surveillance activity, the greater the potential for negative consequences. Further, the duration of and unique familiarity in an employer-employee relationship means an organisation may collect a significant amount of varied personal information about an employee from surveillance activities. This puts employees at risk in the event of a data breach. Therefore, it is important that employers only collect personal information that is necessary for the functions or activities of the business. Employers should also have stringent safeguards against the misuse of, and strict criteria for access to, data collected through workplace surveillance. This is especially pronounced when considering 'work from home', 'remote working' and 'bring your own device' employment models.

These employment models are extending surveillance activities beyond the workplace and into the private lives of employees. Some employers use applications that provide access to employees' webcams, random screenshot monitoring and keystroke monitoring.[12] While these applications are increasing in popularity among employers, it is debatable that the same performance management outcomes cannot be achieved through less intrusive means. Employers should not use these surveillance methods simply because they are available – this type of use may represent an arbitrary interference with employees' privacy.

These concerns are exacerbated in workplaces that require employees to bring their own devices. Employers may install security and surveillance software on a device that is also for personal use by the employee. This may subject an employee's non-work-related personal information to a higher risk of incidental collection or data breach than otherwise would be the case.

Incidental collection can occur in many workplace surveillance activities. For example, an employee who is required to wear a bodycam may forget to switch off the bodycam upon returning home for a lunch break, or a non-work-related conversation between employees may be recorded. Incidental collection can also impact family members, including children, whose personal and sensitive information is collected. Any information collected through incidental collection that is not necessary for that organisation's functions or activities should be destroyed immediately. Upon discovering that incidental collection has occurred, the employer should disclose that collection to the employee in question.

Surveillance for 'work from home' employees and employees required to 'bring their own device' may require specific regulations given the degree of intrusiveness and increased risk of incidental collection of personal information that is not connected to the purpose of the surveillance activity.

Recommendation 3: That the Committee consider measures to reduce the impact of incidental collection through workplace surveillance.

Recommendation 4: That the Committee consider the unique risks of workplace surveillance for employees that work from home or from a device that is also for personal use.

[12] Herbert Smith Freehills (2021). *Future of Work Report.* Available at https://insights.hsf.com/fow2/p/5.

Regulation specific to workplace surveillance

New South Wales and the Australian Capital Territory have legislation specific to workplace surveillance that sits alongside privacy legislation. This enables issues specific to workplace surveillance to be addressed, such as permitting employers' use of covert surveillance in some circumstances.

While prohibited under the PDP Act, covert surveillance can be permitted after an approval process under New South Wales' *Workplace Surveillance Act 2005* (NSW).[13] Employers are required to apply for a covert surveillance authority through a magistrate. A covert surveillance authority can only be issued for the purpose of establishing whether or not an employee is involved in unlawful activity in the workplace.[14] This legislation also specifically addresses computer surveillance and covers the blocking of emails and internet access of employees at work. Despite this, the Select Committee on the impact of technological and other change on the future of work and workers in New South Wales found that the *Workplace Surveillance Act 2005* has 'not kept pace with advancements and that workers' protections are diminished as a result'.[15]

The IPPs are a principles-based framework that recognises the complicated and nuanced nature of privacy, and allow flexibility in how privacy can be protected in varying contexts and alongside evolving technologies and societal norms. However, the employer-employee relationship is a unique context, as it carries asymmetrical power dynamics, is sustained over long periods of time, affects intimate aspects of people's lives and is critical to an individual's ability to live. The ethical, social and psychological impacts mean the problem with workplace surveillance is not limited to the mishandling of personal information; it is the inherent intrusion into employees' right to privacy. The IPPs are designed to protect personal information specifically, and therefore may not be the correct instrument to regulate workplace surveillance.

The Committee may wish to consider whether the uniqueness of the employer-employee relationship warrants its own surveillance regulation mechanism that addresses the specific challenges therein. Any workplace surveillance regulation should be accessible to all employers and employees and address the diversity of surveillance technologies.

Recommendation 5: That the Committee consider whether a new regulatory framework would better reflect the asymmetrical and unique relationship between employees and employers, and the high privacy risks of workplace surveillance activities.

Toward a positive obligation on employers

Privacy is a non-absolute right, meaning that there can be limitations in its application provided those limitations are reasonable, necessary and proportionate. This is evident in Article 17 of the

[13] Part 4, *Workplace Surveillance Act 2005* (NSW).
[14] Section 20, *Workplace Surveillance Act 2005* (NSW).
[15] Select Committee on the impact of technological and other change on the future of work and workers in New South Wales (2020). *Final Report – Workplace surveillance and automation*, page 22.

International Covenant on Civil and Political Rights: 'No one shall be subjected to *arbitrary* [emphasis added] or unlawful interference with his privacy'. [16]

Surveillance activities, by their nature, are incursions on the privacy of those being surveilled. This means any surveillance activity must satisfy the following:

- pursue a legitimate objective; and
- be reasonable, necessary and proportionate in its application.[17]

Workplace surveillance activities that satisfy these conditions may be considered reasonable limitations on the right to privacy, and those that do not satisfy these conditions could be in contravention of the Charter.

Workplace surveillance is a one-way transfer of information relating to employees and employers. In this environment, employees are unable to hold employers accountable for their surveillance activities. Any mechanism designed to keep employers accountable for their workplace surveillance practices should consider that employees will not have access to the necessary information to determine whether their employer is in breach of a privacy or surveillance law.

Since workplace surveillance necessarily infringes on an employee's privacy, there should be a positive obligation on employers to demonstrate that any surveillance activity both pursues a legitimate objective and is reasonable, necessary and proportionate in its application. Requiring employers to articulate a clearly defined and specific purpose before engaging in a surveillance activity, particularly one with a high privacy risk, would also minimise the risk of function creep of that surveillance activity.

As part of this obligation, employers should be required to complete a privacy impact assessment[18] and a security risk assessment. These processes help employers understand the privacy risks of prospective surveillance activities, evaluate them for their intrusiveness and determine whether there is a less-intrusive means to achieve the stated objective.

Compulsory privacy impact assessments for activities with a high privacy risk were also proposed in the Attorney General's Privacy Act Review Report.[19] For VPS organisations, a clearly defined and recorded purpose is necessary under IPP 1 and helps to evaluate the surveillance activity in relation to the other IPPs. A positive obligation recognises that there may be legitimate reasons an employer would require undertaking a workplace surveillance activity, while balancing the privacy of employees.

Recommendation 6: That the Committee consider a positive obligation on employers to demonstrate, prior to its commencement, that a high privacy risk workplace surveillance activity pursues a

[16] United Nations General Assembly (1966). *International Covenant on Civil and Political Rights*, Treaty Series 999 (December).
[17] Attorney General's Department (n.d.). *Permissible Limitations.* Available at https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/public-sector-guidance-sheets/permissible-limitations.
[18] See OVIC guidance on privacy impact assessments for further detail, available at https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-impact-assessment/.
[19] Attorney General's Department (2022). *Privacy Act Review Report,* page 125. Available at https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report.

legitimate objective and is reasonable, necessary and proportionate. This should include both a privacy impact assessment and a security risk assessment.