Submission No 38

INQUIRY INTO WORKPLACE SURVEILLANCE

Organisation: Australian Nursing and Midwifery Federation, Victorian Branch

Date Received: 2 August 2024

Australian Nursing & Midwifery Federation
VICTORIAN BRANCH

ANMF House
535 Elizabeth Street
Melbourne Victoria 3000
ABN 80 571 091 192

Box 12600 A'Beckett Street PO
Melbourne Victoria 8006

anmfvic.asn.au
t 03 9275 9333
f 03 9275 9344
e records@anmfvic.asn.au

LF:sg

1 August 2024

Alison Marchant MLA
Chair
Economics and Infrastructure Committee
Parliament of Victoria
Melbourne VIC 3002

[redacted]

Dear Chair

Inquiry into workplace surveillance

The Australian Nursing and Midwifery Federation (ANMF), Victorian Branch extend our gratitude for the opportunity to contribute to the important inquiry and provide the following submission on behalf of ANMF Vic Branch members.

The ANMF (Vic Branch) represents more than 106,000 Victorian nurses, midwives and personal care workers (the latter predominantly in the private residential aged care sector). Our members are employed in a wide range of enterprises in urban, rural and community care locations and within the public and private health and aged care sectors.

The core business for the ANMF (Vic Branch) is the representation of the professional, industrial and occupational health and safety interests of our members and the professions of nursing and midwifery.

The following submission conveys and addresses the experiences of ANMF Vic Branch members, from the perspective of registered nurses, registered midwives and carers. As an affiliate of the Australian Council of Trades Union, The ANMF endorse the Victorian Trades Hall Council submission and support the commonalities experienced by Victorian workers.

ANMF Vic Branch would welcome the opportunity to discuss the submission should you require further information.

[redacted]

Lisa Fitzpatrick
Secretary
ANMF (Vic Branch)

Australian® Nursing & Midwifery Federation
VICTORIAN BRANCH

ANMF (Vic Branch)
535 Elizabeth Street
Melbourne Victoria 3000

Box 12600
A'Beckett Street PO
Melbourne Victoria 8006

anmfvic.asn.au
t 03 9275 9333
f 03 9275 9344
e records@anmfvic.asn.au

ABN 80 571 091 192
RTOID: 22609

ANMF (Vic Branch) Submission to Parliament of Victoria

Workplace Surveillance Victorian Parliamentary Inquiry

The ANMF (Vic Branch) participates in the development of policy relating to nursing and midwifery practice, professionalism, regulation, education, training, workforce, and socio-economic welfare, health and aged care, community services, veterans' affairs, occupational health and safety, industrial relations, social justice, human rights, immigration, foreign affairs and law reform.

Our strong and growing membership and integrated role as both a professional and industrial organisation, with responsibilities across workplace health and safety and education and training, provide us with a complete understanding of all aspects of the nursing and midwifery professions and see us uniquely placed to defend and advance our professions and interests.

The ANMF (Vic Branch) represents members that are employed in health, aged and/or community services that have already implemented or are considering implementing workplace surveillance technologies in a variety of care contexts across the Victorian care sectors. These workplace surveillance technologies include but are not limited to operational monitoring (of both employees and consumers), as well as e-intelligence or digitally based surveillance systems or technologies.

The ANMF (Vic Branch) acknowledges that there are legitimate reasons for employers to adopt temporary and/or continuous workplace surveillance monitoring. They are also entitled to preserve their operational interests by ensuring the security of premises and property (both physical and digital). However, the interests of employers and employees must be appropriately balanced and robust legislation is required to protect the personal privacy, interests and psychological safety of Victorian workers.

The current legislation applicable in Victoria is insufficient and does not appropriately protect the interests of workers. Furthermore, Victoria is trailing other Australian states and the international community when it comes to legislative implementation and reform to address the use of workplace surveillance.

ANMF (Vic Branch) provides a summary of our members' experiences to the Legislative Assembly Economy and Infrastructure Committee Parliamentary Inquiry into Workplace Surveillance in Victoria and highlights key considerations arising in the healthcare context to enable effective legislative reform. We understand that the broad terms of reference for the probe, is examining five key areas:

1. current workplace surveillance practices and the handling of associated data in Victoria;
2. regulation of workplace surveillance including the effectiveness of privacy laws;
3. potential privacy and data security risks posed by workplace surveillance;
4. impact of workplace surveillance on workers, their families and workplace relations;
5. best practice workplace surveillance and privacy laws interstate and overseas.

This submission focuses on the particular risks to ANMF members, in particular those nurses and midwives who are professionally exposed because of the lack of legislative protections for workers.

The effectiveness of current privacy and workplace laws when it comes to employee workplace surveillance

Nurses, midwives and carers rights at work in relation to their privacy is not always made clear. Workplace surveillance is increasingly prevalent across public and private health and aged care workplaces, it is the view of the ANMF (Vic Branch) that State legislation has not kept pace with the evolving modes of contemporary surveillance and artificial intelligence technologies. Consequently, due to the lack of any clear, legislative obligation imposed on employers, they often fail to appropriately disclose to employees how workplace

surveillance technologies are utilised and the subsequent implications for individual employees. Therefore, the extent of transparency around workplace surveillance varies between workplaces and is highly discretionary. Surveillance of ANMF members is not limited to employer surveillance. As nursing and midwifery practice extends to home care services, for example domiciliary midwifery or Hospital in the Home, members now provide patient care in around 32% of private residences. ANMF understands that in this at home care context, members are being surveilled with private CCTV cameras or concealed recording devices in addition to employer surveillance.

The *Surveillance Devices Act*[1] currently applies in Victoria. Under the *Surveillance Devices Act* it is an offence to use a listening or optical surveillance device to record or observe a *private conversation*[2] or *activity*[3] without the expressed or implied consent of the parties being monitored. The definition of *private conversation* and *activity* is confined to that which is *"carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be heard/observed only by themselves"*[4]. The legislation prohibits employers from using listening or optical devices in workplace toilets, bathrooms, change rooms and lactation rooms. However, workplace surveillance in all other areas of the workplace premises (wherein which intimate, or inherently private activities such as toileting would not generally occur) remains unregulated. Aside from these limited exceptions, employers have unfettered discretion to monitor the conduct or conversations of their employees in the course of their work, regardless of consent.

The *Privacy Act*[5] applies to all Australian States, including Victoria. The *Privacy Act* regulates the collection, use and disclosure of personal information, including identifiable information such as a person's image. It is an offence to breach the Australian Privacy Principles, as set out in Schedule 1 of the *Privacy Act*. However, the protections afforded by the *Privacy Act* are limited and the Act enables employers to collect and utilise personal information if it is *"reasonably necessary for, or directly related to, one or more of the entity's functions or activities*"[6]. Matters related to an entity's functions or activities are extensive and broad and can include the general monitoring of an employee's productivity and performance. Employers are not required to obtain consent for the collection or utilisation of employees' personal information and the Act does not impose any notification requirements on employers.

In Victoria, the *Privacy and Data Protection Act 2014* (Vic) operates similarly to the Commonwealth *Privacy* Act but serves to bind Victorian public sector entities such as government agencies. The combined effect of the *Surveillance Devices Act* and the *privacy Acts (Privacy Act 1988* (Cth) and *Privacy and Data Protection Act 2014* (Vic)) is that employers are afforded considerable power and discretion to monitor workers in Victoria. Conversely, workers are often ignorant to the extent of surveillance in their workplaces and how that surveillance may be used or disseminated.

The impact of surveillance in healthcare for registered healthcare workers and a patient's right to privacy / right to knowledge of surveillance.

Many employers of nurses, midwives and carers have adopted various forms of workplace surveillance. Such surveillance in the health and aged care sectors may include recorded video surveillance, computer

[1] *Surveillance Devices Act 1999* (Vic)
[2] Ibid. Section 6.
[3] Ibid. Section 7.
[4] Ibid. Section 3.
[5] *Privacy Act 1988* (Cth)
[6] Ibid. Schedule 1, Australian Privacy Principles. Principle 3.

monitoring, telephone monitoring, email monitoring, personal retina, finger, hand and facial recognition scanning.

Employers commonly use workplace CCTV surveillance and other digital monitoring to review workplace incidents and investigate employee performance deficiencies or misconduct. This frequently results in employers relying on CCTV footage to justify disciplinary action.

Furthermore, employers of healthcare workers often disclose information about employees (including information about an employee's digital activity and CCTV footage) to independent regulators, including the Australian Health Practitioner Regulation Agency (AHPRA). Employers have mandatory reporting obligations in certain circumstances. However, employers regularly make voluntary and discretionary notifications to AHPRA about ANMF (Vic Branch) members and provide the regulator with a suite of evidence to which the employee is forced to respond[7].

Ahpra and the Nursing and Midwifery Board of Australia (NMBA) can make decisions about the safety and quality of the practitioners practice and restrict their ability to work as a nurse or midwife, or indeed cancel their registration, based on their assessment of the information provided by the employer. The significance of this in relation to workplace surveillance is crucial in highlighting the professional vulnerability experienced by our members when surveillance is improperly obtained and disseminated.

Employers often provide select and specific evidence to AHPRA in isolation which fails to demonstrate the relevant context or appropriately outline an employee's defense to allegations made against them.

However, the right to review and rely upon CCTV footage is not equally afforded to employees. Instead, the CCTV footage is often in the control of an external entity and the nurse, midwife or carer has no rights in relation to its use, storage or destruction. Furthermore, members have advised ANMF (Vic Branch) that CCTV is infrequently used to review and identify injuries sustained by employees during the course of their employment.

In 2017, in an Australian first, the Victorian government introduced new statewide guidelines detailing minimum requirements for Victorian public hospitals to develop and implement processes to improve emergency responses to occupational violence and aggression (OVA)[8] An element of this strategy was the introduction of Body Worn Cameras (BWC) for paramedics in the healthcare setting. This strategy has since been adapted in both private and public health services for their security personnel.

> ***Nursing and Midwifery Board of Australia (NMBA) Decision Making Framework:***
> *For nurses and midwives workplace surveillance is also entwined with obligations to uphold the NMBA decision-making framework (DMF).*
>
> *The DMF details clear guidelines to scope of practice, practice decisions and delegation and supervision for nurse practitioners, registered nurses, registered midwives and enrolled registered nurses[1].*

The introduction of BWC has been established both nationally and internationally with an intent to reduce the

[7] Ahpra 2024 Making a mandatory notification
[8] https://www.premier.vic.gov.au/ausralian-first-policy-prevent-violence-hospitals

instances of Occupational Violence and Aggression (OVA) in healthcare settings.

Case study 1:

ANMF (Vic branch) member contacted seeking representation following receipt of formal disciplinary proceedings from her public health employer. The disciplinary allegations were in relation to misconduct and performance concerns. The member was a registered nurse and was working as the Nurse in Charge at a major metropolitan public health service.

The allegations related to the management of a patient on the acute medical ward. The patient was a 65-year-old male with a complex medical history admitted for management of acute behavioral deterioration and aggression secondary to dementia and delirium.

In summary:

1. The nurse was rostered as 'in charge' of the night shift.

2. During the preceding shift, the patient had physically assaulted the nurse allocated to his care resulting in significant injuries including her nose being fractured. The patient had also physically assaulted one patient on the ward.

3. Due to the patient's ill health and resultant behaviors, there was significant distress to other patients and staff.

4. During the members night shift, there was a further physical assault to another patient, during this altercation the patient fell to the floor.

5. A further Code Grey (behavioral aggression response) was activated, and two security guards attended wearing Body Worn cameras (BWC).

6. Our member undertook a preliminary clinical assessment, underpinned by her knowledge of the situation and patient vulnerabilities, and her obligations associated with the DMF.

7. Due to the multitude of risks including the significant patient agitation and ongoing threats of aggression to both patients and staff, the nurse advised staff to delay approaching the patient again, until the imminent arrival of the doctor to assess the patient and determine the safest care option.

8. The resultant disciplinary actions were based off excerpts of the audio-visual footage captured by the BWC. This did not protect the privacy of the patient or consider the risk to others. The excerpts from the footage were transcribed as evidence without the aforementioned context, and the footage was not provided to the nurse in the first instance.

9. This scenario demonstrates the risk of unregulated surveillance ANMF members are exposed to, in addition to the lack of privacy protections and patient dignity. The footage obtained by the BWC was captured by the security personal, who are contracted by external providers and are not employed by the health service. As such the footage is not privy to the health service privacy and process.

The interaction between healthcare and the Surveillances Devices Act (SDA)

BWC, captures footage of both workers and patients during interactions of care. The footage is defined as

'Protected Information' under the Surveillances Devices Act (SDA), with a recent amendment in 2021 to incorporate the protected information obtained from BWC by a police officers and Ambulance Officers. What isn't contemplated in the amendment, is footage captured within the healthcare setting.

What the SDA does not include nor contemplate is footage obtained, inclusive of BWC within aged care settings and clinical hospital settings. The ethical consideration of BWC and CCT footage within healthcare, is that though these are public places, the footage may capture interactions, and information that is in fact deemed private and obtained without consent. Additionally, though the SDA does contemplate police offices and ambulances officers as defined, the Act does not include Nurses, Midwives or personal carers. Though our members in most instances do not wear the BWC, they are implicated in the clinical setting and will most likely be included in the audiovisual evidence.

Pilots of BWCs have been instituted with paramedics, and they have now been included in the SDA. It is therefore possible that ANMF (Vic Branch) members may, in the future, be required wear BWCs in their workplaces. The *Surveillance Devices Act* requires amendment to anticipate this likely development in workplace surveillance practice and ensure healthcare workers are protected (like paramedics and police officers are under section 7(2)(d) and (e)) from prosecution where private activities are inadvertently captured on BWCs used in the course of ordinary duties. In Victoria, the template for Body-worn cameras policy, developed through the department of health, has not been updated since 2018 and would most likely not be fit for purpose for current practices in Victoria's health and aged care sector.[9]

Further, the overlap of legislation such as the Surveillance Devices Act, Privacy and Data Act and Health Records Act, is all intertwined and poorly defined in the healthcare setting. As such ANMF members encounter professional repercussions which are being justified by employers as part of workplace monitoring and surveillance. As with CCTV footage, this again raises concerns related to questions of data storage and accessibility for workers and patients and the provision of safeguarding for nurses and midwives in healthcare remains unclear. ANMF members are experiencing scrutiny and repercussion not only from their employer, but also, again through AHPRA, multiple health, aged care, disability and quality and safety commissions, health care complaints department and other regulatory bodies.

The ownership of workplace surveillance data and an employee's ability to access that data

In almost all contracts of employment, there is either an express or implied term stipulating that material and information produced within the course of employment belongs to the employer. Employers have proprietary rights over documents, correspondence, images and footage produced in the course of employment, including CCTV footage depicting employees. Conversely, employees do not generally have any proprietary rights to the work, information or intellectual property produced in the course of employment, or any image of them produced by the employer.

An employee's right to access workplace surveillance data is derived from various Commonwealth and State Acts. This is not a proprietary right, but rather a right to a degree of privacy and of access to private information in certain circumstances. The Freedom of Information Acts[10] apply to Commonwealth and Victorian government departments and agencies and provide a formal channel through which information held by those agencies can be accessed. Furthermore, the *Privacy and Data Protection Act 2014* (Vic) outlines the Information Privacy Principles and the

[9] Department of Health 2024 Body worn cameras policy template

[10] *Freedom of Information Act 1982* (Vic) and *Freedom of Information Act 1982* (Cth)

Privacy Act 1988 (Cth) outlines the Australian Privacy Principles. Each of these legislative frameworks regulate the nature of personal information employers can lawfully obtain (albeit with very limited restrictions on the scope of the personal information that can be obtained), restrict disclosure of that information and provide rights of access to personal information for employees[11].

Both the Victorian and Commonwealth privacy legislation provides for complaints mechanisms. The Office of the Australian Information Commissioner is authorised to receive and deal with complaints regarding breaches of the Australian Privacy Principles, to implement a range of regulatory measures and to prosecute entities for non-compliance. Similarly, the Office of the Victorian Information Commissioner deals with complaints under the Victorian privacy legislation. However, neither the Commonwealth nor Victorian legislation allows for an individual complainant to initiate proceedings against an employer for privacy breaches. Whether an employee's privacy concern can be resolved depends on the effectiveness of the relevant Commission's complaints and dispute resolution process, their resourcing and their internal policies regarding prosecuting breaches of the Act. Overall, employees are relatively powerless when it comes to holding employers to account for breaches of privacy laws, including failures to release and disclose personal information upon request.

The protection of the privacy, autonomy and dignity of workers and other individuals, and the potential for privacy and data security risks to individuals, workers, businesses, communities and Victoria

The Health Records Act 2001 and the Privacy and Data Protection Act 2014 mandate that 'health information' and 'personal information' must be collected only when necessary and, with limited exceptions, used and disclosed solely for its original purpose. Given the nature of audiovisual recordings from body-worn cameras in healthcare settings, health services should anticipate the capture of both health and personal information. It is recommended to conduct a Privacy Impact Assessment to identify and mitigate any privacy risks associated with body-worn cameras.

According to the Public Records Act 1973, hospitals and health services are obligated to retain public records and dispose of them in compliance with approved standards from the Public Records Office. Depending on the circumstances, camera footage may need to be retained and made accessible for public purposes.

Unregulated workplace surveillance can have significant consequences for both patients and registered workers. These consequences can have broad reaching impacts on workers particularly when working in sensitive clinical settings.

Furthermore, workplace surveillance for nurses, midwives and carers presents ethical challenges which impact on their individual privacy, trust with their employer and their working environment together with the ethical dilemmas of patient care and obligations as registered practitioners.

The personal impact of workplace surveillance on Victorian workers, such as on their physical and mental safety

There are significant impacts of workplace surveillance on nurses, midwives and personal carers, primarily on their psychological safety. These can be both positive and negative, depending upon the consultation, implementation and use of such surveillance.

[11] Privacy and Data Protection Act 2014 (Vic) Schedule 1, The Information Privacy Principles.

As noted previously, one of the purposes for workplace surveillance is as a deterrent for occupational violence and aggression. Providing clear notification that a person's acts are being recorded appears to lessen the likelihood of escalation of a situation in many circumstances. When this is the purpose of surveillance, and the workers are advised of such, involved in the implementation and there is evidence of the surveillance being used for such purposes, this supports the psychological sense of safety that workers feel.

However, when such surveillance is implemented unilaterally by employers and without appropriate consultation with affected employees, ANMF (Vic Branch) members report that they feel apprehensive about the use of surveillance and whether it is intended to control rather than protect employees. Additionally, where an unfortunate incident of occupational violence does occur, and the footage is used in a positive incident investigation (i.e. where the incident is looked at, and clear, proactive mechanisms are implemented to prevent future occurrences), this can be psychologically protective of the worker who has been involved. This is contrary to where the footage is used only to identify potential mistakes the worker may have made, or in a culture of blame. Where surveillance is used primarily as a tool for identifying disciplinary issues, staff become distrustful of workplace surveillance. This results in a lack of trust between workers and their employer leads to decreased employee performance, poor staff retention and increases in workplace psychological hazards and psychological injuries sustained by employees in the healthcare industry.

Surveillance is also used by patients, visitors or family members to record interactions with staff during care provision, which causes significant psychological distress to the healthcare workers involved. Most care providers (acute, aged care and community) have limited or no policies in place to manage or prevent healthcare workers being recorded by patients or their family members. Furthermore, healthcare workers are not educated on what action they can take to protect themselves or intervene in such a situation. ANMF (Vic Branch) members have been the subject of online harassment and scrutiny, after being filmed, photographed or identified on social media by patients and their families. Often with limited support from their employers, healthcare workers are left despondent and have little recourse to enable the removal of their personal information or image from social media or from the general public domain.

Australia's obligations under international law, including International Labour Organization Conventions

The United Nations (UN) Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights both set out fundamental international principles and human rights aims. These are foundational instruments from which the UN and its member States have developed subsequent international law. Whilst the Declaration and the Covenant are non-binding, there is nonetheless an expectation that Australia, having ratified these instruments, should adopt the relevant principles and implement them into domestic law. Both the Declaration of Human Rights[12] and the Covenant on Civil and Political Rights recognise the privacy of individuals and establish a general right to privacy[13]. Article 12 of the Universal Declaration of Human Rights states, *"no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".*

The International Labour Organisation (ILO) is an agency of the UN tasked with setting universal minimum standards for international labour rights. The ILO Declaration of Philadelphia sets out the aims and purposes of the ILO, including that *"all human beings, irrespective of race, creed or sex, have the right to pursue both their material well-being and their spiritual development in conditions of freedom and dignity, of economic security and equal opportunity"*[14]. Notably, the principles of freedom and dignity are fundamental considerations of the ILO and of

[12] The Universal Declaration of Human Rights, 1948. Article 12.

[13] International Covenant on Civil and Political Rights, 1976. Article 17.

[14] The Declaration of Philadelphia, 1944. Part II (a).

broader international labour standards. As a founding member of the ILO, Australia should be at the forefront of domestic legislative developments to implement the principles of worker freedom and dignity.

The ILO Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy states that, *"governments should ensure that both multinational and national enterprises provide adequate safety and health standards and contribute to a preventative safety and health culture in enterprises progressively achieving a safe health working environment"*[15]. Psychosocial hazards are now recognised in domestic occupational health and safety legislation as workplace safety hazards. It is therefore incumbent on Australia to identify and appropriately address all health and safety risks, including those that pose a psychosocial hazard for workers. Furthermore, the Tripartite Declaration states that *"multinational enterprises should maintain the highest standards of safety and health… bearing in mind their relevant experience within the enterprise as a whole, including any knowledge of special hazards*[16]". The healthcare industry arguably poses a unique suite of *"special hazards"*. The ILO has recognised the unique challenges posed by the healthcare sector and the nursing profession and encourages member States to *"endeavour to improve existing laws and regulations on occupational health and safety by adapting them to the special nature of nursing work and of the environment in which it is carried out"*[17]. There must be sufficient legislative impetus for healthcare employers to adequately address these special hazards and take steps to guard against workplace psychosocial injury. Legislating the use of workplace surveillance devices to protect the freedom, dignity and occupational health and safety of workers is critical to upholding Australia's international obligations.

The ILO is yet to establish a specific convention regarding the use of new technologies and workplace surveillance. However, in recognition of the emerging global issue of data security and workplace surveillance, in 1997, the ILO published a Code of Practice on the Protection of Workers' Personal Data. Many of the general principles outlined in section 5 of the Code of Practice are reflected in Australian domestic legislation, including the *Privacy Act 1988* (Cth) and the *Privacy and Data Protection Act 2014* (Vic). However, there are certain key recommendations in the Code of Practice which are not codified in the domestic laws affecting Victorian workers. Notably, the Code of Practice recommends that if workers are monitored via CCTV, that workers should be informed in advance of the reasons for monitoring, the time schedule of any monitoring, the techniques for monitoring deployed and the nature of data to be collected[18]. Additionally, the Code recommends collective rights for workers and the right for unions to be consulted prior to the implementation of digital surveillance in the workplace[19]. The Code also recommends against the use of secret monitoring unless the employer holds a reasonable suspicion that criminal activity or other serious wrongdoing is occurring in the workplace[20].

Unlike many other countries, Australia's constitution does not codify any individual privacy rights. **It is therefore critical that Australia, both Federally and at the State level, implements progressive legislation in line with its international obligations.**

International or domestic examples of best practice workplace surveillance regulation and privacy protection

Due to the non-binding nature of international law, including the instruments discussed above, there is little consistency across regions and nation States when it comes to workplace surveillance standards. However, certain countries have implemented progressive domestic legislation that reflects, and in certain cases exceeds the ILO recommendations.

[15] Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy. Paragraph 43.
[16] Ibid. Paragraph 44.
[17] ILO Nursing Personnel Convention No 149, 1977. Article 7.
[18] ILO Code of Practice- Protection of Workers' Personal Data, 1997. Principle 6.14(1).
[19] Ibid. Principle 12.2.
[20] Ibid. Principle 6.14(2).

In 2018, the European Union (EU) published the General Data Protection Regulation. The General Data Protection Regulation is binding on EU member States. Whilst the Regulation is not specific to the employment or workplace context, its broad provisions provide robust protections for individuals the subject of digital surveillance. In summary, individuals have eight data protection rights under the Regulation: the right to be informed about data collection and use; the right of access to personal data; the right of rectification of inaccurate personal data; the right of erasure of personal data; the right to restrict the use and processing of personal data; the right of data portability; the right to object to the nature of data processing; and the right to opt-out of automated data processing and profiling.

The Council of Europe published non-binding recommendations regarding personal data protection in the employment context[21]. These recommendations recognise that automation and data processing is beneficial to employment relationships but nonetheless acknowledges individual privacy as a fundamental human right. The recommendations advance the idea of fully informed consent to workplace surveillance following consultation with workers and unions where surveillance is used to monitor the movements and productivity of workers (particularly where an employer proposes to introduce novel technologies to the workplace)[22]. Certain European countries have implemented domestic legislation that goes beyond the requirements of the General Data Protection Regulation.

For example, in Norway the data regulation legislation provides that any digital monitoring or surveillance systems traceable to an individual (for example an individual employee) require a government license from the national Data Inspectorate[23]. All applications for licenses must be made on justifiable grounds, such as the prevention of criminal activity. In certain workplace contexts, the legislation goes so far as to prohibit the use of CCTV solely to monitor employee activity[24]. Furthermore, in 1970 Italy introduced legislation prohibiting the general use of audio-visual equipment to monitor workers[25]. The legislation provides that where an employer wishes to implement audio-visual monitoring equipment, they must outline the commercial justification for the surveillance equipment and obtain consent from the relevant union. The legislation also provides for a dispute resolution mechanism and deferral of the decision to a national labour authority if the employer and union cannot reach agreement.

In Australia, the *Workplace Surveillance Act 2005* (NSW) is the best example of workplace surveillance regulation. The Act prohibits employers from implementing workplace surveillance without first notifying affected employees at least 14 days prior[26]. The Act also imposes additional requirements on employers to clearly signpost the use of CCTV at the entrance to the employer's premises[27]. However, whilst the *Workplace Surveillance Act* protects the privacy interests of workers to a degree and implements some consent requirements, the Australia Institute has nonetheless criticised the legislation as not being sufficient and has recommended a model similar to the EU's General Data Protection Regulation[28].

---

[21] The Council of Europe, Recommendation (89)2E, Protection of Personal Data for Employment Purposes, 1989.

[22] The Council of Europe, Recommendation (89)2E, Protection of Personal Data for Employment Purposes, 1989. Recommendation 3.1.

[23] See ILO Conditions of Work Digest, Volume 12 No. 1, 1993. Workers' Privacy Part II: Monitoring and Surveillance in the Workplace. Page 230.

[24] Ibid. Page 233.

[25] Ibid. Page 199.

[26] Workplace Surveillance Act 2005 (NSW), section 10.

[27] Ibid. Section 11.

[28] The Australia Institute, Workplace Surveillance- Submission to the Select Committee on the Impact of Technological Change on the Future of Work, 2020. Page 13. https://australiainstitute.org.au/wp-content/uploads/2020/12/P954-Responsible-Tech-Workplace-Surveillance-Submission-Web.pdf

The potential consequences of unregulated surveillance on health workers and the requirement for legislative reform

As discussed above, there are numerous privacy considerations that underpin the issue of workplace surveillance. Currently in Victoria, employers have considerable discretion over how workplace surveillance is utilised and whether employees are consulted and educated on the subsequent policies. Furthermore, there are limited restrictions on the types of workplace surveillance technologies that employers can deploy. Other than being restricted from installing listening or optical surveillance devices in private locations such as bathrooms[29], employers can choose to implement a range of invasive audio-visual and online tracking technologies to closely monitor the activities of their employees.

The employment relationship gives rise to legislative exceptions that result in a greater extent of lawful surveillance by employers of employees than is otherwise accepted. For example, the Victorian *Surveillance Devices Act* prohibits a person from installing a tracking device, capable of identifying someone's geographical location[30]. However, this prohibition does not apply where a person is considered to have impliedly consented to the geographical tracking as in the course of an employment relationship, or where an employee is utilising equipment owned by the employer[31].

Electronic medical records:

The rapid expansion and widespread implementation of virtual, telehealth and extended models of care such as hospital in the Home, has also brought to light emerging privacy and data security risks. This is due several factors which leave nurses and midwives vulnerable in addition to increasing risks of unintentional data breaches for the public.

The nature of home base care and patient in reach programs encourage the use of mobile phones to access the relevant and required patient information via a nominated app. In recent years most major Victorian public sector hospitals have transitioned from paper-based systems to Electronic Medical Records (EMR). EMR can also be accessed by heal care workers via a nominated and linked phone applications (apps) from an external private provider.

This progressive approach enables nurses and midwives timely access to patient information, including health conditions, diagnostics, treatments, medications, allergies etc.

Case Study 2:

A registered nurse of 24 years, employed at a major metropolitan hospital contacted ANMF Vic Branch seeking assistance with a workplace disciplinary matter. The member had received a letter of allegations detailing concerns of serious misconduct pertaining to patient privacy breach. The employer had implemented the EMR platform and had issued correspondence by way of an all-staff email update detailing EMR access can be obtained via a nominated application (App) for work purposes. Following a written enquiry, our member received approved access by the health providers IT department.

Our member reviewed various patient profiles including presentation, disease process pathophysiology and treatment pathways for professional development reasons. Our member had received approved unfettered access to not only her employer's patient database, but the app also had unrestricted access to several other health services using the EMR forum associated with the nominated app. There were no credentialed 'break

[29] Surveillance Devices Act 1999 (Vic) Sections 6 and 7.
[30] Ibid. Section 8.
[31] Ibid. Section 8(1)(a) and (b).

walls' warnings or required credentialled access to patient profiles whilst utilising application. At no point was there any redistribution, patient identification and or malicious intent.

Our member received formal disciplinary proceedings following an external health provider undertaking data audits, identified and reported heath data and privacy breach to the members employer. The member was not aware that she was being surveyed via the digital footprint. Nor was she made aware that though she had approved access for the application, did not equate to approved access for viewing patient profiles.

This member's experience highlights the impact where employers' neglect to provide their employees with specific education in relation to their responsibilities and clear, relevant and robust policies and safeguarding systems to ensure the protections of workers and sensitive patient information.

The *Privacy Act 1988* (Cth) and the *Privacy and Data Protection Act 2014* (Vic) afford minimal rights and protections to employees. The scope of personal information that employers can lawfully obtain is broad, given the Commonwealth Act defines personal information as *"information or an opinion about an identified individual"*[32] . Employers need only to surpass a low threshold of relevance in order to record and retain personal information about an employee, that being that the information need only be *"reasonably necessary for, or directly related to, one or more of the entity's functions or activities*[33]".

In light of the deficiencies in Victorian legislation and the best practice domestic and international examples highlighted above, it is clear that the Victorian Parliament should legislate to protect workers privacy rights and psychosocial safety in the workplace. The ANMF (Vic Branch) is of the view that this is particularly important in the healthcare context.

ANMF (Vic Branch) therefore recommends that Victorian workplace surveillance legislation considers:

1. Improved employer obligations to consult with workers, their union representatives including in relation to proposed implementation of changes to policy and procedure.
2. Strengthening worker protections in relation to the use of surveillance footage, preventing its routine use for individual disciplinary procedures.
3. In relation to BWC, extend protections to surrounding employees who may be involved or implicated in relation to a workplace patient interaction.
4. The introduction of an independent regulator of workplace surveillance.
5. Given the nature of audiovisual footage and the interactions recorded by workplace surveillance and body-worn cameras in healthcare settings, health services should anticipate the collection of health and personal information. Mandating employers undertake Privacy Impact Assessment to identify and mitigate any associated privacy risks. Where private companies own the audiovisual information that the requirements for storage and disposal of the footage are publicly available for employees of the health service and there are legislative obligations for the private entity to also consider the rights of the health service employees.
6. Department of Health to develop and make available consistent workplace surveillance and data privacy policies for Victorian public health services to ensure all employees are aware of their rights and responsibilities and can easily access this information.

[32] *Privacy Act 1988* (Cth). Section 6.

[33] Ibid. Schedule 1, Australian Privacy Principles. Principle 3.1.