No Blood-No Job:
Australia's privacy laws and workers' rights

Dr Lisa Heap

The Centre for Future Work at the Australia Institute

August 2024

The Australia Institute
Research that matters.
Centre for FutureWork

About the Australia Institute

The Australia Institute is an independent public policy think tank based in Canberra. It is funded by donations from philanthropic trusts and individuals and commissioned research. We barrack for ideas, not political parties or candidates. Since its launch in 1994, the Institute has carried out highly influential research on a broad range of economic, social and environmental issues.

Our Philosophy

As we begin the 21st century, new dilemmas confront our society and our planet. Unprecedented levels of consumption co-exist with extreme poverty. Through new technology we are more connected than we have ever been, yet civic engagement is declining. Environmental neglect continues despite heightened ecological awareness. A better balance is urgently needed.

The Australia Institute's directors, staff and supporters represent a broad range of views and priorities. What unites us is a belief that through a combination of research and creativity we can promote new solutions and ways of thinking.

Our Purpose – *'Research That Matters'*

The Institute publishes research that contributes to a more just, sustainable and peaceful society. Our goal is to gather, interpret and communicate evidence to both diagnose the problems we face and propose new solutions to tackle them.

The Institute is wholly independent and not affiliated with any other organisation. Donations to its Research Fund are tax deductible for the donor. Anyone wishing to donate can do so via the website at https://www.tai.org.au or by calling the Institute on 02 6130 0530. Our secure and user-friendly website allows donors to make either one-off or regular monthly donations and we encourage everyone who can to donate in this way as it assists our research in the most significant manner.

Level 1, Endeavour House
1 Franklin St, Manuka, ACT 2603
Tel: (02) 61300530
Email: mail@australiainstitute.org.au
Website: www.australiainstitute.org.au

About the Centre for Future Work

The Centre for Future Work is a research centre, housed within the Australia Institute, to conduct and publish progressive economic research on work, employment, and labour markets. It serves as a unique centre of excellence on the economic issues facing working people: including the future of jobs, wages and income distribution, skills and training, sector and industry policies, globalisation, the role of government, public services, and more. The Centre also develops timely and practical policy proposals to help make the world of work better for working people and their families.

www.futurework.org.au

About the Author

Dr Lisa Heap is a labour lawyer and researcher with a research focus on gender and inequalities at work, work health and safety and the regulation of work.

The author acknowledges the assistance of Lily Raynes (former Anne Kantor Fellow), Dr Fiona Macdonald, Policy Director Industrial and Social and Dr Jim Stanford, Economist and Director of the Centre for Future Work, in the preparation of this report.

The author also wishes to thank the members and officials of the Electrical Trades Union who shared their knowledge and experiences with the author.

Contents

Introduction

Organisations[1] in Australia are using blood analysis as a means of screening future employees for 'health risks' that they allege may impact on their performance of work. Collecting sensitive information from blood analysis is restricted under Australia's privacy laws. This is because the mishandling of this information can have a substantial detrimental impact on those who have provided the information. Requiring workers to submit to blood analysis is just one example of how organisations are now routinely collecting sensitive information from workers, sometimes without adhering to the requirements of privacy laws. Other examples include using fingerprint and facial recognition software and sensors that collect physiological and psychological data about workers.

The protection from arbitrary interference with a person's privacy is a fundamental human right. Interfering with this right, by collecting sensitive personal information, should occur in limited circumstances and only where necessary. However, this report shows that some organisations in Australia, are not treating the collection of sensitive information from workers as an exception. They are collecting sensitive information as a routine step in their employment processes. Reports have also highlighted examples of organisations using biometric applications, such as facial recognition software and fingerprint technology, that collect sensitive information, as mechanisms to surveil workers (White, 2020). The findings of this report raise concerns about power, privacy, fairness, and the potential for discrimination in the practices being adopted by some organisations. These findings also show that Australia's current privacy and workplace relations laws do not adequately address these concerns.

Amendments to Australian privacy laws are currently being considered by the Australian Government with reforms likely to be put before the Australian Parliament before the end of 2024.[2] This report examines the need for new provisions within either or both privacy or workplace relations laws that set out the rights of workers to protect their sensitive information. It argues that regulation should be geared towards, not only protecting workers' rights to privacy, but to providing a disincentive to

[1] The *Privacy Act 1988* (Cth) regulates Commonwealth Government agencies, organisations with a turnover of over $3 million and a limited number of other organisations. This report focuses on private sector and non-government organisations referred to as 'organisations' throughout the report.

[2] These proposed amendments to the Privacy Act included changes to privacy laws generally including contexts beyond the work-related reforms considered in this report.

organisations hoarding (Minderoo Tech & Policy Hub, 2021, 5) and misuse of the personal and sensitive information of workers.

The worker-centric approach called for in this report includes:

- the development of one system of regulation to protect the privacy concerns of all workers regardless of employment status or work context

- defining the collection of workers' personal and sensitive information as high risk requiring both specific and detailed justification for the collection of this information and the genuine informed and affirmative consent of workers

- the establishment of a tripartite mechanism to assist the regulator to develop and manage processes for dealing with the privacy and related human rights concerns of workers

- the use of codes and frameworks, developed via a tripartite mechanism, to set out when and how workers' information can be collected and used

- the development of an easy to access, and timely, worker centered mechanism to address concerns about the collection and use of workers' information.

The purpose of a worker-centric approach with these features is to place the protection of workers' privacy at the heart of work-related privacy laws.

First the report provides an overview of Australia's privacy laws as they relate to work. Following this, the gaps in laws related to workers' privacy are discussed. An illustrative example describes the privacy concerns of some workers in the mining and resources sectors and the issues arising from compulsory blood testing of workers during recruitment. An analysis of the gaps in protections for workers' privacy follows. Risks related to collection and use of workers' sensitive information are explored.

The final sections of the report consider current proposals for law reform to protect workers' privacy. The government's work-related proposals for change to the Privacy Act, arising from a review of the legislation, are examined. These proposals fall short of what is needed to protect workers' privacy. Key aspects of a more worker-centric approach to privacy are detailed in the final section of this report. We argue workers' genuine consent to provide information must be gained, and workers and their representatives must be involved in decision-making to ensure that sensitive information is only collected where it is necessary.

Australia's national privacy laws

In Australia there are legal rules around the collection, use, sharing, access to, and disposition of, personal (including sensitive) information by Australian Government agencies and business entities with an annual turnover of over $3 million.[3] Privacy regulation includes the *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles ("APP") which are contained within the Privacy Act.[4]

The Privacy Act provides a higher standard of protection for sensitive information.[5] Under the Privacy Act sensitive information can only be collected where the information is reasonably necessary for one or more of the entity's functions or activities,[6] or where the collection is authorised by law.[7] Sensitive information cannot be collected without the consent of those providing that information.[8]

In this report one type of sensitive information - workers' blood and the analysis arising from the testing of this blood - is used as an illustrative example of how some organisations have built in the collection of sensitive information from workers as routine. Blood and the analysis of this blood is sensitive information because it falls within the definition of health information or genetic material contained in the Privacy Act.[9]

The application of the Privacy Act in the context of work is complex. The Fair Work Commission ("FWC"), Australia's national workplace relations tribunal, has considered how the provisions of the Privacy Act apply in the work context. In cases before the FWC the question of whether collecting sensitive information from a worker is

[3] Business entities are referred to as organisations in this report.

[4] For the purposes of this report the focus is on federal privacy and workplace relations laws. In addition to the Privacy Act provisions, the handling of personal information may also be subject to state and territory health records legislation (Victoria, New South Wales and the Australian Capital Territory), state and federal surveillance legislation, and federal law around email marketing legislation, marketing and telemarketing. State and Territory based government agencies must comply with state and territory privacy laws.

[5] Categories of sensitive information are contained in s.6 of the Privacy Act. Sensitive information is personal information that includes information or an opinion about an individual's: racial or ethnic origin; political opinions or associations; religious or philosophical beliefs; trade union membership or associations; sexual orientation or practices; criminal record; health or genetic information; some aspects of biometric information.

[6] APP 3.3

[7] APP 3.4 – which includes several circumstances where this might apply.

[8] APP 3.3

[9] Privacy Act s.6FA(a)(i) and (c).

reasonable has been contested with different decisions in different contexts (Attorney General, 2022, 64-71; Allen et al 2013).

Also, the question of what genuine consent is when a worker is facing unemployment or disciplinary action if they don't agree to provide this information has been considered by the FWC differently in different contexts. On the one hand the FWC has concluded that a worker's consent to provide their sensitive information was likely to have been overridden by threats of disciplinary action if consent was not given.[10] On the other, the threatened termination of employment of an employee who did not provide a COVID-19 vaccination certificate that contains sensitive information, was not seen as overriding the requirement for genuine consent under privacy laws.[11]

Concerns about workers'privacy include concerns about how sensitive information collected from employees will be used by employers. Once this information becomes part of an employee record use of it is not restricted under privacy laws. This is because there is an exemption for employee records from privacy laws. The *Fair Work Act 2009* (Cth) (Fair Work Act) deals with how information in employee records can be treated. There is evidence information in employee records is sometimes sold to third parties without workers' informed consent (Chen & Howe, 2022).

When introduced in 1988 the Privacy Act operationalised Australia's obligations under OECD international trade guidelines and international human rights covenants. First, the Privacy Act put in place general data gathering rules that would better facilitate international trade and commerce that relied on data sharing. These rules, developed at the international level, were contained in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which Australia adopted in 1984 (ALRC, 2007 [1.2]; Lucy, 2012). Second, the laws, in a limited way,[12] also responded to provisions within Article 12 of the *UN Declaration of Human Rights* (UNDHR) and Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) which mandate that no person should be subjected to arbitrary or unlawful interference with their privacy (ALRC, 2007; Witzleb, 2018). Australia is a signatory to both the UNDHR and the ICCPR.

Through the adoption of UNDHR and the ICCPR the right to privacy has been recognised as a fundamental human right that warrants protection in Australia.

[10] *Lee v Superior Wood Pty Ltd* [2019] FWC 2946
[11] *CFMMEU & Ors v BHP Coal* [2022] FWC 81.
[12] The Privacy Act only deals with data/information privacy. The right to privacy under Article 17 of the ICCPR is a broad right that could include territorial or bodily privacy.

Protecting privacy is linked to ideas of maintaining a person's individual dignity, their personal autonomy, and their liberty (Falk 2020; Gligorijevic 2020). Privacy laws play an important role in ensuring that people are not put under unwarranted surveillance or are not asked to provide information about themselves where providing this information is unwarranted or unreasonable. Privacy laws are also designed to place responsibilities on entities that collect information to ensure requests for information are not excessive and that, once information about an individual is obtained, it is treated in an appropriate way.

Once thought of as an individual right, in a modern networked world, with increasingly sophisticated use of technology, privacy can also be a collective right. As a society we collectively have an interest in ensuring that everyone's privacy is protected. Approaches that lead to breaches of one person's rights can impact on others, as is the case with mass data breaches. These breaches can undermine collective confidence in systems of data gathering and storage and undermine democratic processes (Fraser et al, 2020, 4-5).

The framing of the Privacy Act attempts to balance individual freedoms and rights to protection of personal information with ensuring barriers to free trade are avoided and a flow of data across national borders is not interrupted.[13] The Office of the Australian Information Commissioner (OAIC), the regulatory body with responsibility for monitoring compliance with the Privacy Act, describes the focus of the Privacy Act as a "framework for the protection of fundamental privacy rights and [emphasis added] an enabler of innovation that supports economic growth" (Falk, 2020, 6).

However, in the way the Privacy Act has been applied the balance has been tipped in favour of organisations' desires to collect information for their commercial interests and away from individuals' rights to protection. This shift has been confirmed by the OIAC. The OIAC recently concluded that changes in technology and methods of service delivery have resulted in "a dramatic increase in the amount of data and personal information collected, used, and shared"(Falk 2020, 6) by entities covered by the Privacy Act. The OIAC stated this greater emphasis on collection and use of data by entities warrants changes in the Australian approach to privacy to place "greater emphasis on the rights of individuals and the obligations of entities to protect those rights" (Falk, 2020, 6). The OAIC has also called for a "more central focus on protecting individuals from the harms associated with current and emerging practices around the collection, use and disclosure of their personal information" (Falk, 2020, 6).Without amendments to the Privacy Act the balance is likely to be tipped further away from

[13] Privacy Act s.2A Objects.

workers' rights to privacy given the transformations in data collection facilitated by innovations in technology and the increased use of artificial intelligence (AI) at work.

The efficacy of existing laws for protecting rights to privacy in the collection and use of personal and sensitive information is becoming a pressing issue in Australia as it is around the world.[14] Data breaches are increasingly common with reports of these breaches becoming a daily occurrence. In the work context privacy concerns about the collection of workers' information intersect with concerns about the increased application of AI, including algorithmic management and automated decision-making at work, creating greater momentum for reform of privacy laws that apply at work (Macdonald & Heap 2024).[15] There is certainly a view that the current provisions of the Privacy Act do not regulate all aspects of how information can be collected, used, and disclosed by AI systems including in the work context (Blackman, 2024).

[14] There are currently numerous parliamentary and other inquiries including ACCC *Digital Platforms Inquiry* https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25; the Attorney-General *Privacy Act Review* https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988; Senate *Select Committee on Adopting Artificial Intelligence (AI)* https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Adopting_Artificial_Intelligence_AI/AdoptingAI; the House of Representatives Standing Committee on Employment, Education and Training *Inquiry into the Digital Transformation of Workplaces* https://www.aph.gov.au/Parliamentary_Business/Committees/House/Employment_Education_and_Training/DigitalTransformation.

[15] This is a theme in numerous submissions to the House of Representatives Standing Committee on Employment, Education and Training Inquiry into the Digital Transformation of Workplaces https://www.aph.gov.au/Parliamentary_Business/Committees/House/Employment_Education_and_Training/DigitalTransformation.

Gaps in protections for workers

There are gaps in the Australian regulation of data collection and use when it comes to workers' personal and sensitive information. There is also confusion regarding how the laws apply in different circumstances. Confusion and gaps lead to a lack of clarity about workers' rights and organisations responsibilities. It is difficult for workers to understand whether they are required to provide information to prospective or current employers, or for contract workers organisations that engage them. The asymmetrical nature of the employment or commercial relationship (where a worker is a contractor) means that withholding consent is often not an option if a worker fears they may be excluded from recruitment for a job or disciplined for refusing (Attorney General's Department, 2022, 66).[16]

Two exemptions within the Privacy Act impact on workers' rights to privacy. First, small business is largely exempt from the operation of the Privacy Act (Attorney General's Department, 2021, 53-54). Therefore, workers engaged by small business are not covered by the protections within that Act. Second, organisations are also exempt from the Privacy Act for activity related to employee records. This exemption applies once the information forms part of the employee record and where that information directly relates to the employment relationship between the employer and that employee.[17] For example, this means the requirements under the Privacy Act which relate to organisations taking reasonable steps to protect information they have collected from misuse, interference, loss, and from unauthorised access, modification and disclosure, that exist under the Privacy Act, do not apply to information within employee records. [18]

However, information gained from prospective employees or information that is not yet maintained in employee records is covered by the Privacy Act.[19] So for example, the collection of personal and sensitive information from workers prior to employment, as part of a recruitment process, is covered by the Privacy Act. The collection of this material from contractors is also covered by the Privacy Act. Also, the

[16] This issue was raised by numerous submitters to the Attorney General's 2022 review of the Privacy Act.

[17] Privacy Act s.7B(3)

[18] APP 11.1. Note the Australian Fair Work Ombudsman states that it is best practice (although not a legal requirement in relation to employee records) for employers to meet the requirements within the APPs (Fair Work Ombudsman, 2023).

[19] *'QF' & Others and Spotless Group Limited (Privac*y) [2019] AICmr 20; Jeremy Lee v Superior Wood Pty Ltd [2019] FWCFB 2946 (1 May 2019)

handling of employee information by third party contractors on behalf of an employer – for example if an employer has outsourced recruitment activities -is covered by the Privacy Act.

This system of different rules, depending on the size of the organisation, based on employment status of the worker, on what is within an employee record or not, or whether acts are related to the employment relationship or not, is confusing and creates uncertainties that are difficult for both organisations and workers to understand (Ng et al, 2022). This confusion and uncertainty undermine the efficacy of privacy laws and leaves circumstances where the personal and sensitive information of some workers is not protected. When workers do not understand their rights and organisations are not clear on the extent of their responsibilities, the protections within the law are undermined.

The exemption under the Privacy Act for employee records was made on the basis that privacy matters related to employees were better left to be regulated by workplace relations law.[20] The Fair Work Act governs rules around the collection, maintenance and accessing of employee information contained within employee records. These provisions set out requirements to collect and maintain information largely geared towards demonstrating compliance with the provisions of the Fair Work Act including 'time and wages' records.[21] More recent provisions have been included which are designed to facilitate pay transparency and establish rights for workers to share information about their employment conditions.[22]

However, the Fair Work Act provisions provide limited privacy protections for employees. The focus of the Fair Work Act is on record keeping and compliance with workplace laws rather than protection of privacy (Attorney General's Department, 2022, 69). There are no protections within the Fair Work Act that are the equivalent of the rights that individuals have under the Privacy Act in relation to collection of information and data breaches (Attorney General's Department, 2022, 64).

The gaps in protections in privacy laws are not the only concern. Whether organisations adhere to these requirements in practice is another problem. In the following section the experience of some workers who have been required to provide sensitive information as part of recruitment processes is discussed. Collecting personal

[20] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth); Commonwealth, Parliamentary Debates, House of Representatives, 12 April 2000, 15752 (Daryl Williams, Attorney-General). The Parliament of The Commonwealth of Australia.
[21] Fair Work Act s.535; Fair Work Regulations 2009 r.3.31-3.48.
[22] Fair Work Act s.333B.

and sensitive information from workers during the recruitment process is covered by the Privacy Act. The examples of workers interviewed as part of this research shows that some companies are taking advantage of their position of power when recruiting workers giving minimal, if any, consideration of privacy requirements.

No Blood-No Job: the experience of electrical trades workers

Australia's system of workplace regulation allows for workers to be subject to testing – including, for example, alcohol and drug testing where there is an established need that can be linked to assessing the capacity of a worker to fulfil the inherent requirements of the job.[23] The illustrative example presented in this section examines the experience of workers who have been subjected to blood testing at the pre-employment process stage. The example reveals privacy and human rights concerns for the workers arising from employers' practices and it highlights some of the gaps in protections for workers in current privacy laws.

Centre for Future Work researchers interviewed electrical trades workers who were required to provide blood samples for testing as a precursor to recruitment to work in the construction of mine sites and in oil and gas exploration operations. Four workers, seeking employment with three different companies, were interviewed.[24] Researchers also discussed the issue of blood sampling of electrical trades workers with senior national officials of the Electrical Trades Union (ETU). Access to the information in the ETU's files regarding the experience of other workers who had been required to provide blood samples to prospective employers/employers was also made available to the Centre for Future Work.

The workers indicated they had limited interaction with, or knowledge of, the companies they were seeking employment with prior to being contacted and advised they should attend a medical examination with a third-party organisation. Appointments were organised through email and/or text, again reinforcing a level of distance between the potential employer and the worker. The workers advised this made it difficult for them to seek out information about the tests. The workers were advised by the prospective employers that testing was a standard part of the recruitment process.

Workers told researchers they were given numerous forms with little explanation of details in the forms. They were required to sign the forms before attending medical

[23] *Shell Refining (Australia) Pty Ltd, Clyde Refinery v CFMEU* [2008] AIRC 510; *Endeavour Energy v Communications, Electrical, Electronic, Energy, Information, Postal, Plumbing and Allied Services Union of Australia and others* [2012] FWA 1809 (26 March 2012); *Briggs v AWH Pty Ltd* [2013] FWCFB 3316.

[24] Two workers were applying to the same company.

appointments. Forms included requests to provide consent to undertake a series of medical tests, including providing blood samples. Forms also included blanket authorities for the company (the prospective employer) to receive and use the analysis of the results of these tests.

Workers also said they were unclear about the reasons for undertaking the test at the time the samples were taken. One man indicated he was told by another worker that blood testing may be related to cardiovascular risk scores, but he did not know if this was the reason he was required to provide blood samples. In another instance the company had stated in writing that the reason for requiring blood samples was to 'meet legal obligations'. For one worker, the requirement to undergo a test occurred when the job he was performing was in effect transferred from one company to another. There was no material change in the nature or location of his work. There was also no indication that there was any need, related to the requirements of the job, that required the test to be carried out. This worker was informed they would not be allowed to stay in the job they had been doing for several years without the test.

ETU personnel advised that, when the union has sought clarification about the reasons for blood testing, companies have not always been clear about their rationales for testing. In one case a company changed its rationale after questions were raised by the ETU. In the first instance the company concerned indicated that they needed to do this as part of a contractual obligation they had to a third-party head contractor. After further enquiries by the union, this company indicated that blood sampling and analysis was necessary to obtain prospective employees' cardiovascular disease risk scores as a health and safety measure.

The consent forms from one company, sighted by the researchers , authorised the use of the data collected from blood testing by the company, its subsidiaries, and related entities without any restrictions on this use. The following statement was included in the consent forms:

> I also acknowledge that my personal information may be provided by [company] to its clients and other external personnel for the purposes of its business and consent to [company] disclosing and retaining my personal information for this purpose.

In this example the worker was also asked to consent to waive any privacy rights associated with the prospective employer providing the sensitive information to overseas entities, thus effectively authorising the use of the sensitive information by clients and any part of the organisation or related entity including those overseas who may or may not meet the requirements of Australian privacy laws.

Two workers indicated they were asked to sign an additional consent form provided by the medical service conducting the tests. There was little explanation of the purpose of these consent forms. The workers did not have copies of these consent forms or remember what was contained in them.

The examples of electrical trades workers explored in this report illustrate company practices that provide no opportunity for worker involvement in decision making about the collection of their sensitive information. The ETU, as the union representing these workers, has advised that it was not consulted about the introduction of blood testing as part of pre-employment processes. Further, trying to resolve disputes where workers are concerned about being required to provide blood samples has been costly. Information provided by the ETU shows that the union's efforts to clarify and resolve concerns has taken a significant amount of union financial resources and personnel time.

The ETU raised their concerns about the extensive resources used to pursue resolution of workers' privacy concerns as part of the Attorney General's review of the Privacy Act. According to the union's submission to the review, the expenditure of resources included in one case[25] an application to the Federal Court designed to force the company to provide information about the reasons for testing and whether genuine consent could be given where testing was required as a prerequisite to going through the recruitment process (ETU 2021, 2). This case was settled confidentially between the parties so the details cannot be shared. Whether collecting sensitive information via blood testing at the recruitment phase is unlawful is a matter that may be contested before the Courts again in the future.

All the workers interviewed told researchers that, if they did not consent to the medical tests, they would not move through the recruitment process. One worker did not consent and therefore did not progress through the recruitment process, thus missing out on being considered for a job. A worker, after participating in the initial tests, was required to attend further medical tests, at their own cost, to get clarification of the results contained in the initial blood tests and analysis. They understood that if they didn't undergo this further testing, at their own cost, they would not be considered for position. Other workers interviewed, who themselves were not referred for further test, told researchers that they had heard of workers who had been required to do this further testing at their own expense.

[25]Of a worker not interviewed for this research.

In the mining and resources sectors there appears to be a level of acceptance of some forms of testing (urine samples) in some limited circumstances (where heavy machinery is involved). This was confirmed by the workers interviewed. However, these workers interviewed expressed skepticism about the requirement for blood tests as part of the recruitment process. Some said it felt controlling. Some said it felt like the companies were overstepping into areas that should be between themselves and their own doctor. They all expressed resentment about being forced into the process as prerequisite for being considered for a job.

These experiences of the workers in the mining and resources sectors are unlikely to be unique. Medical testing is being promoted as a standard step in the recruitment process in all industries in Australia. A simple Google search brings forward several examples of companies in Australia advertising testing services for all roles within organisations. The need for a link between collecting sensitive information from workers and the requirements of the job appears to have been lost. For example, one organisation states on its website that any "well-known and respectable business will use testing, which may include taking urine, hair samples, as a common aspect for the job application process for any position" [emphasis added] (Australian Drug Testing, n.d.). The same organisation offers blood screening but at least notes that most employers do not use it as it is "so intrusive" (Australian Drug Testing, n.d.).

Another organisation advertises that pre-employment drug testing offers employers insight into the "character and tendencies [emphasis added] of prospective employees and an added layer of security" (Safework Health,2023). In yet another example, information on a Victorian Government sponsored website, that is part of an initiative to inform young workers of their work rights, normalises the concept of drug and alcohol testing in both pre-employment processes and at work (Youth Central, n.d.). None of the sites examined in the preparation of this report provided information that linked the use of testing, including via blood samples, to specific business needs or requirements of the job.

The risks to workers' privacy

The experience of electrical trades workers outlined in the previous section of this report shows how some organisations, even though they have obligations to comply with privacy laws in relation to workers' sensitive information, are acting in ways that give at best cursory attention to the requirements of these laws. In these examples the balance has well and truly swung in favour of organisations interests and against the privacy of individuals, undermining the protective intent of privacy laws. Drawing on this information and the research conducted for this report several practices that present risks to workers' privacy can be identified. These practices and the risks that they present are described below. Figure 1 sets out these practices and risks graphically.

Unilateral decision making by organisations

Under Australian privacy laws decision-making about the collection of sensitive information is solely in the hands of the organisations collecting that information. Organisations can decide to collect this information without consultation with workers or their representatives. These organisations are the arbiters of decisions about whether there is adequate justification for collection of information and whether the amount and type of information collected is proportionate to the need for it. There is little meaningful restriction on their decision-making under privacy laws and little requirement to assess the organisation's needs for the information against the risks to workers' privacy created by collecting that information. This means that there is little incentive for organisations to consider alternative methods, rather than the collection of sensitive information from workers, to address their needs. It also means that workers have limited information and little, if any, capacity to assess whether the requirement to provide the information is reasonable and/or lawful.

Using generic rationales to justify collecting information

In the examples provided in this report, companies were not transparent about the need for the blood testing. When pressed, one company came forward with 'health and safety' as a catch-all rationale to justify collection of workers' sensitive information. However, in the examples presented in this report the relevance of tests for the purposes of health and safety was questionable. As outlined above, some workers believed that the blood testing was required to assess their risk of cardiovascular disease. The information provided by the ETU also indicated that the

attainment of a cardiovascular risk score was the rationale given eventually by one company it sought information from. A cardiovascular disease risk score ("CRS") provides an assessment of the potential level of risk of cardiovascular disease of an individual over a five to ten-year period into the future. It is designed for doctors to work with patients to identify health and lifestyle changes to help patients avoid the risk of heart attack and stroke in the future (Better Health, n.d.).

It is difficult to see how an assessment of potential vulnerability to disease in the long-term is justified when a worker's suitability for the job is being assessed. Further, testing of this nature may be discriminatory where this information is used to screen for diseases or genetic predisposition that may not be relevant to the work situation. Offering a generic rationale, such as 'health and safety', in this way should be challenged. A general reference to health and safety as justification is not a sufficient for the use of intrusive testing or the collection of sensitive information.

Requiring blanket consent

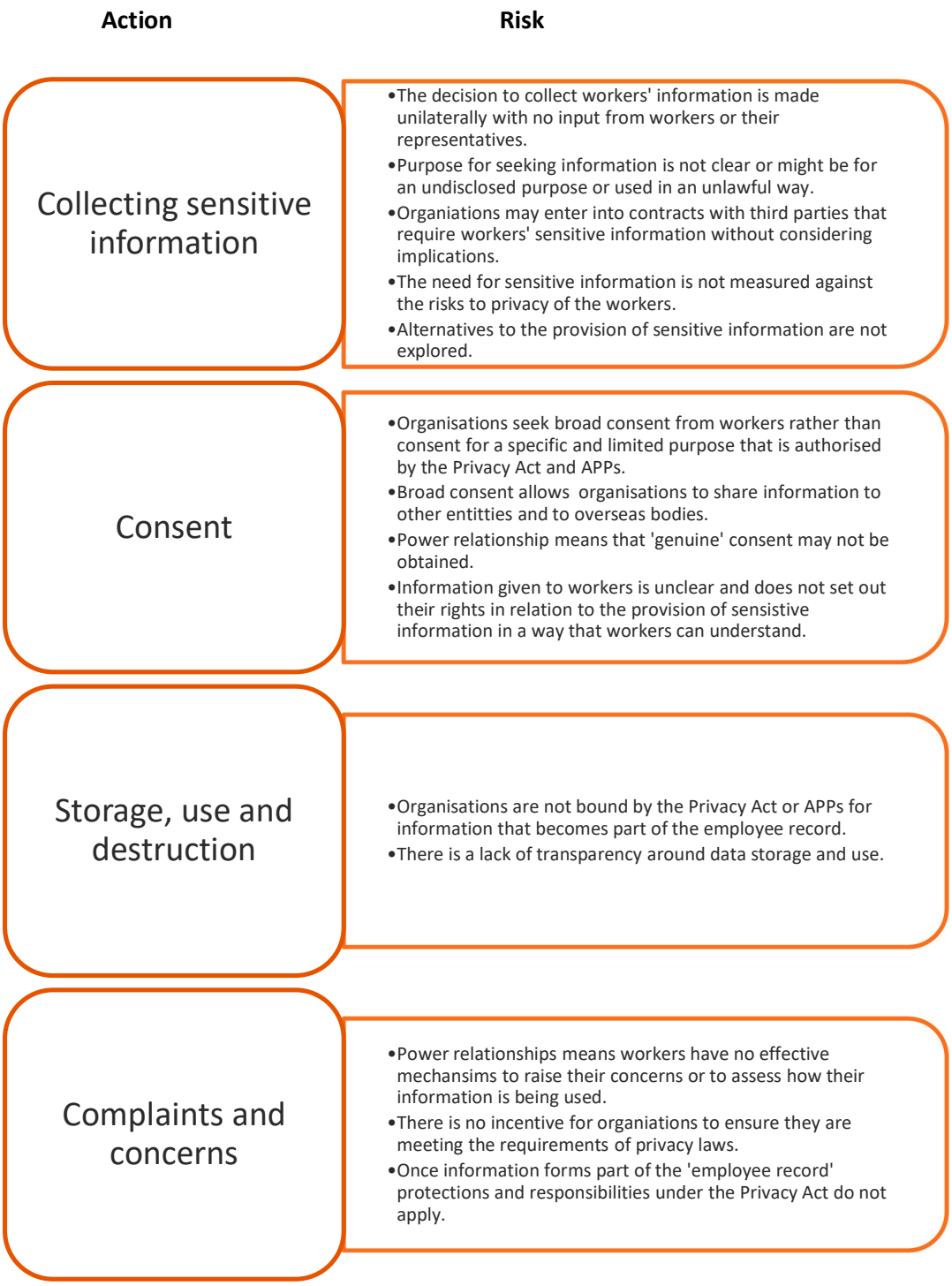
The examples in this report show that the companies involved did not establish processes that provide specific and easily digestible information to workers about the rationale for tests, nature of the blood tests, uses of the data provided, or how it will be stored or destroyed. Workers were asked to give the broadest consent with limited information about how the sensitive information collected could be used. Dealing with consent in this way at least undermines the essence of privacy laws if not also being in fact unlawful under the Privacy Act. It suggests a lack of diligence, care, or concern in the way some organisations are treating workers' sensitive information. It also creates suspicions that blood samples (and other sensitive information) may be collected for undisclosed purposes. In a world where personal and sensitive information is being sold as a commodity by organisations and software providers, these suspicions may be well founded.

Limiting workers' opportunity to challenge collection

The lack of information provided to workers about what they may be consenting to, or how their sensitive information might be used, limits their capacity to challenge how this information is collected and used. Workers who have provided the information as part of recruitment, but then do not go on to employment with the organisation, are not likely to be able to dispute whether the collection, use, storage and destruction of this information is consistent with the law or with any consent form they signed. For a worker who is employed, the privacy risks are compounded if the sensitive information

becomes part of the ‘employee record’. The exemption from the Privacy Act for employee records means that employers are under none of the obligations around collection, use and destruction contained within that Privacy Act. In figure 1 actions taken by organisations to collect sensitive information from workers and the risks they present are set out graphically.

Figure 1. Organisations' actions and risks to privacy of workers



Conclusions regarding risks to workers' privacy

A factor underpinning the practices discussed in this section is the complete asymmetry of power between worker and potential employer/employer. Privacy laws in Australia fail to account for this asymmetry of power. In their current state Australian privacy and workplace relations laws are not sufficient to protect workers' rights to determine if their sensitive information should be collected and used by organisations that employ or contract them.

To address the risks to workers' privacy outlined in this report law (either privacy or workplace relations or both) reform is needed. This reform should give primacy to workers' rights to privacy and control over their personal and sensitive information. A new approach for the collection and use of workers' personal and sensitive information should be adopted. This framework should include the involvement of workers and their representatives in decisions about how workers information is collected and used. In the following section current proposals for privacy law reform are considered, keeping in mind the risks identified in this report.

Review of the Privacy Act

Australia's privacy laws are currently under review with reforms likely to come before the Australian Parliament in the second half of 2024 (Dreyfus, 2024).[26] A review of the Privacy Act was conducted by the Attorney-General's Department during the period 2020 to 2022 (Attorney General's Department, 2022). The review was motivated by the need to address risks associated with increased digitisation and from growing expectations from the Australia public for greater protections in light of data breaches and the increased incidence of identity fraud (Attorney General's Department, 2022, 2).

In response to the review of the Privacy Act the Australian Government has set out its 'blueprint' for change (Commonwealth of Australia, 2023). The approach to reforms set out in this blueprint seeks to align Australian privacy laws more closely with those of the General Data Protection Regulation in the European Union (GDPR) and United Kingdom (UKGDPR). The European and UK regulations are more comprehensive and include protections for data collected from employees including that within employee records.

It is not clear whether changes to the Privacy Act in Australia will include removing the exemption for employee records. The recommendations from the Attorney General Department's review of the Privacy Act suggested further consultation between the government, employers' representatives and unions should be undertaken on this issue. This suggestion has been accepted by the Australian Government (Commonwealth of Australia, 2023, 24). The following is a summary of some of the proposed changes contained within the Australian Government's blueprint, that will apply in the work context.

Fair and reasonable test

The proposed reforms include the introduction of a 'fair and reasonable' test to apply to the collection, use and disposal of personal information (Commonwealth of Australia, 2023).[27] What is fair and reasonable will include consideration of whether the impact on privacy is proportionate to the benefit to the entity collecting the information. This is referred to as the proportionality principle. Currently in Australia

[26] Some amendments to the Privacy Act have already been made through the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth)*. As the name suggests these changes relate to an increase in enforcement provisions for the regulator and tougher penalties for data breaches.

[27] Proposal 12.1 & 12.2.

the Australian Privacy Principles ("APPs") require that the collection of information should be reasonably necessary for the entity's functions or activities. The proposed fair and reasonable test will add a consideration of the fairness of this requirement for information. However, the version of proportionality in the government reform proposal provides less protection than is provided under the European GDPR provisions.[28] Under the GDPR, the collection of information must be both strictly necessary and proportionate to this need.

Further, the European DGPR includes a data minimisation principle. This principle states that data collection should be specific, explicit and for a legitimate purpose and that only that data which is adequate, relevant and limited to what is necessary should be collected. Australian privacy laws should include this data minimisation concept. A restriction on organisations so that they only collect sensitive information that is strictly necessary should assist in curtailing what appears to be the default position of some Australian organisations to collect large amounts of personal and sensitive information from Australian workers.

The proposed fair and reasonable test is unlikely to address the privacy risks to workers experiencing the problems discussed in this report. To do so the test would need to be accompanied by a requirement to consult with workers and their representatives about the nature of the information requested and about the circumstances within which collecting the information is fair and reasonable.

Impact assessments

In another reform the Australian Government supports the inclusion of a requirement for organisations to complete a Privacy Impact Assessment ("PIA") for activities with high privacy risks to individuals (Commonwealth of Australia, 2023, Proposal 13.1). Commonwealth Government agencies already have this obligation. The Australian Government has accepted that areas of high privacy risks include the use of facial recognition technology and collection of biometric information. Other areas of high risks are not identified however the idea that these will be identified is agreed in principle in the Australian Government's blueprint. Requiring workers to provide blood samples and the gathering of biometric information from workers should be included as high risk activities that require a PIA.

[28] For a discussion of proportionality in the European context see https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

Under the Australian Government proposal, PIAs would be carried out by the organisation collecting the information without further oversight. There is no requirement for the approval of the regulator before high risk activities are embarked upon. In the proposal, the regulator may review the PIA from time to time. However, it is difficult to see how such assessments would protect workers given there is no requirement for workers to have a role in the assessment process.

In contrast with the Australian reform proposal, employees in Europe would have far greater rights to information and monitoring of employers' decisions in what are deemed high-risk circumstances. A framework of information sharing and involvement of workers in matters relating to their privacy underpins the GDPR. Under the GDPR the processing of sensitive information of all employees (who are defined as vulnerable data subjects) is prima facie prohibited unless specific circumstances exist.[29]

The emphasis in the GDPR is on data controllers (employers) safeguarding data subjects' (employees) privacy rights when relying on an exemption from the prohibition on the collection of this data. The circumstances where the exemption applies include where processing data "is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment"[30] or where "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee…"[31] In these circumstances under the GDPR a Data Protection Impact Assessment (DPIA) is required.[32] Provisions must be in place to notify employees of the rights they have under the GDPR in relation to their data as well as the way (including nature and scope of processing) the data is being used. Employees must be informed their consent is required for their data to be used in particular circumstances. Employers must ensure there are arrangements in place that allow employees to exercise their rights under the GDPR, and they must ensure there are mechanisms that support employees to monitor an employer's compliance with these requirements. Employees must also be advised of data breaches.[33] Under the GDPR, the processes surrounding how data is processed in the employment context can also be the subject of collective agreements.[34]

[29] GDPR Article 9.
[30] GDPR Article 9(2)(b).
[31] GDPR Article 9(2)(h).
[32] Article 35.
[33] GDPR Articles 12, 13, 14, 15.
[34] GDPR Recital 155.

In current Australian privacy or workplace relations law there is no framework of information sharing and involvement of workers in matters relating to their privacy. The Australian Government proposal to require Privacy Impact Assessments does not address the current absence of any requirement for worker involvement in decision making. The reform proposals do include additional rights to enhanced transparency and control for individuals. These rights allow individuals to request information and challenge information handling practices of an entity (Commonwealth of Australia, 2023, 18). The difficulty with this approach is that it places the obligation on individuals to assert these rights rather than emphasising the responsibility of entities to create a framework of information sharing and involvement of persons from who they are collecting information in decision making about the collection of that information.

Consent

The Australian Government's blueprint includes changes to the rules around consent. In this proposal consent must be voluntary, informed, current, specific, and unambiguous (Commonwealth of Australia, 2023). This concept of consent is not as tight as that in the GDPR which requires 'affirmative consent' which means that there is either a statement or a clear affirmative act confirming consent.[35] The Australian Government proposal appears to maintain a capacity for organisations to rely on implied as well as explicit consent (Read et al, 2023). This would mean organisations could collect information from workers and rely on the absence of objection by these workers to the collecting of this information as consent.

In the Australian reform proposals the validity of consent will be linked to capacity to consent. This means that valid consent requires that the capacity of a person to give this consent must be considered (Commonwealth of Australia, 2023).[36] The issue of capacity in this reform proposal relates to age and to persons who may be experiencing particularly vulnerabilities. It is proposed that a non-exhaustive list is developed that indicates when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information (Commonwealth of Australia, 2023).[37] However, there are no indications that the test of capacity would take into account the asymmetry of power in the relationship between workers and organisations. There is an argument that in the context of work, and this asymmetry of power, consent cannot be freely given by a worker (Abraha

[35] GDPR Article 7 and Recital 32.
[36] Proposal 16.2.
[37] Proposal 17.1.

2024). Concerns about the capacity of workers to genuinely consent could be balanced by incorporating mechanisms for worker involvement and decision making in processes around data gathering.

Removal of exemptions

Both the small business and employee records exemptions were considered in the review of the Privacy Act. The government is proposing to remove the small business exemption following some further consultation in that area (Commonwealth of Australia 2023, Proposal 6.1). This means that for contract workers or prospective employees or employees engaged by small businesses (where information is not part of the employee record) the Privacy Act will apply. In the case of employees of small business who have information which forms part of the employee record the Privacy Act will not apply to this information unless the employee records exemption is removed.

Whether the Australian Government is proposing to remove the employee records exemption is not clear. The employee records exemption means the Privacy Act does not apply to information contained within employee records. The reform proposals address the employee records exemption by stating that there should be greater protections for private sector employees. However, the Government has proposed that how reforms related to work are to be addresses should be the subject of further consultations with employer and employee representatives. It states this consultation should include the relationship between privacy and workplace relations laws and could include the possibility of developing privacy codes of practices through tripartite processes (Commonwealth of Australia, 2023, 24).

Whilst seeking to enhance transparency for employees around how their personal and sensitive information is used, the proposed reforms also include recognition of the need for employers to have adequate flexibility to collect, use and disclose employees information that is reasonably necessary to administer the employment relationship. This includes addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information (Commonwealth of Australia, 2023, Proposal 7.1).

The proposed reforms therefore leave open the question of removal of the employee records exemption. The idea of tripartite processes to develop privacy codes of practices for workers is a welcome one. The Australian Government's response also suggests that whether consent should be required to collect employees' sensitive

information should be discussed further. If consent was not required employees would continue to receive less protection of their personal and sensitive information from their employer than the clients or customers of the same organisation have.

Employer bodies, and some individual employers participating in the government's review of the Privacy Act argued that the removal of the employee records exemption would make administering the employment relationship difficult and would be burdensome (Attorney General's Department, 2021, 53-54). On the other hand, academics, unions and civil society groups, concerned with the protection of privacy and those advocating for workers' rights, submitted that the employee records exemption should be removed or substantially altered to provide employees with the same privacy rights as others under the Privacy Act (Attorney General's Department, 2021, 50-57). The Australian Law Reform Commission (ALRC) has proposed the removal of the employee record exemption for the collection of health and biometric information since 2003 (ALRC, 2023, 69). The ALRC did not accept that the compliance burden on employers would be significant. The removal of the employee records exemption would bring the Privacy Act into closer alignment with the DGPR and the UKGDPR. There is no blanket exemption for employee records in these overseas regulations.

Conclusions regarding review of the Privacy Act

The Privacy Act review reform proposals do make significant efforts to improve information privacy rights in Australia however, they fall short of addressing the risks to workers' privacy outlined in this report. A difficulty with the reforms proposed by the Australian Government is they still fail to address the power imbalance in work relationships and they don't fully integrate workers and their representatives as part of the decision making about the collection and use of workers' personal and sensitive information. The information organisations collect about workers is now extensive. Rather than starting from a principle that collecting this information is standard and a routine part of the recruitment process, or employment, the principle should be that organisations only have access to the minimal amount of information and only that which they can demonstrate is strictly necessary. What is strictly necessary in a particular context is something which workers and their representatives should be involved in determining in collaboration with organisations and the regulator. In the following section aspects of a more worker-centric approach to privacy are proposed.

A worker-centric approach to privacy

Addressing the specific risks related to work and employment-related matters should be a priority in any reform of privacy laws. Whilst privacy laws may seek to strike a balance between the rights of workers to maintain their privacy and the interests of organisations who demand information, there must be mechanisms to stop organisations overreaching in their demands for the provision of personal and sensitive information from workers, and there must be greater protection of workers' privacy rights. This section presents key aspects of a worker-centric approach to the protection of workers' information privacy. Figure 2 sets out the key aspects of the proposed worker-centric approach graphically.

The purpose the worker-centric approach is to make the protection of workers' privacy the focus. The proposed approach addresses the concern, identified by the Office of the Information Commissioner that, in the context of new technological developments and innovations, privacy laws in Australia have swung too far in favour of organisations gathering information and away from the individuals whose information is being gathered. In the context of the asymmetrical power structures at work, the worker-centric approach outlined here emphasises collective processes necessary to ensure that power imbalances between data controllers and data subjects are addressed. In the rest of this section the key aspects of this worker-centric approach are outlined.

A single system that protects all workers' (contractors, prospective employees, and employees) privacy rights is required to fill gaps in protections and to address current confusion about what rights and responsibilities apply. The current exemption from privacy laws for employee records should be reviewed. Either the exemption from the Privacy Act should be removed (along with further reforms of that Act) or comprehensive privacy protections for workers should be incorporated in the Fair Work Act. The latter approach would be more difficult, but not impossible, for ensuring the privacy rights of workers who are not employees are protected. The international trend is towards having employment related information and employee records dealt with through privacy laws rather than employment laws. There is an argument that having workers' privacy concerns dealt with by the privacy regulator would mean that the subject matter expertise of the privacy regulator can be utilised.

The collection of any information from workers should be treated as high risk and therefore subject to a high standard of care. The collection and use of workers' information can impact on workers' identity and livelihoods. Organisations should be encouraged to take the greatest care when collecting this information. This will be an increasingly important principle as we see a greater use of AI - including automated decision making and algorithmic management- in relation to workers.

Related to the above aspect is the requirement that collecting sensitive information from workers and conducting invasive tests on workers to collect this information should only occur when strictly necessary and when a defined need can be established. There needs to be a move away from organisations collecting sensitive information as a routine practice. An overarching principle of data minimisation must guide practice. There should be a presumption in law that sensitive information should only be collected when there is an established and specific need for which no alternative (other than the provision of this sensitive information) exists.

Even when a specific need can be established, the impact on workers' privacy must be considered. Assessing the impact on workers should include assessing whether the organisation can demonstrate an ability and willingness to use this information only for the purpose for which it is collected and to store this information in a manner that ensures workers' privacy. The collection of sensitive information should be preceded by a worker impact assessment. Impact assessments should consider both the privacy and potential human rights concerns (such as discrimination) arising through requests to provide sensitive information.

The provision of sensitive information should be subject to workers' genuine consent. Genuine consent can be facilitated if there are collective processes (see below) which involve workers and their representatives. These processes should include considerations of the circumstances in which seeking this information is warranted and what forms of information gathering (including testing) are acceptable. Individual workers should then be provided with a specific request from the organisation and be given information to enable them to assess whether the request meets the collective standard.

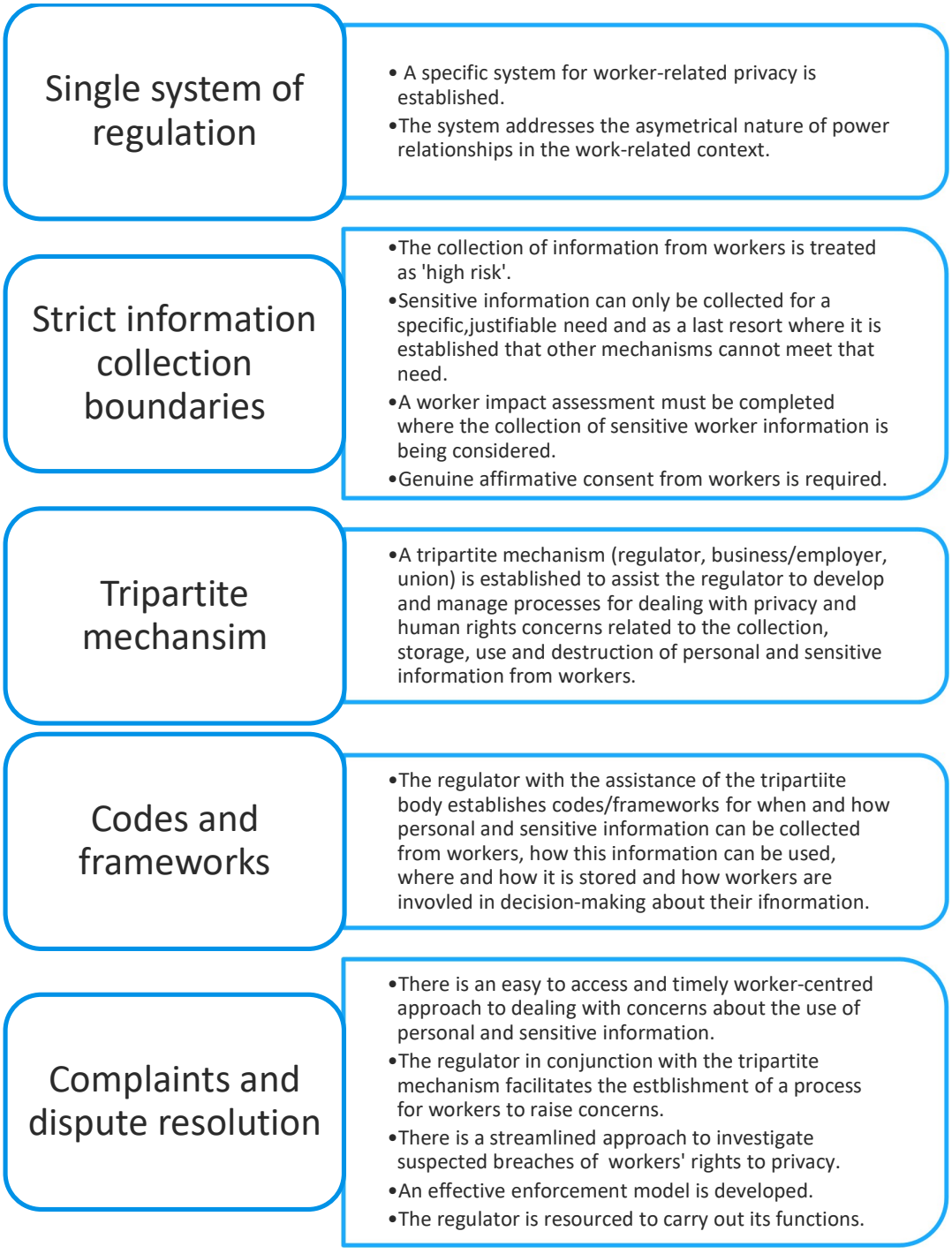
Finally, the regulation of workers privacy rights should involve tripartite forums that allow for workers and their representatives to be involved in decision making about what, when, and how to collect, use, and dispose of workers' private and sensitive information. A tripartite mechanism including the regulator, organisation representatives and union representatives should be established at the national level to manage the privacy and human rights concerns related to the collection of personal and sensitive information from workers.

The tripartite mechanism could determine

- Codes or standards in industries or sectors where the need to collect sensitive information may be justified.
- Processes for workers and their representatives to be involved at the organisation/entity level in decision making about whether, and how to collect sensitive information, obtaining informed genuine consent, uses storage and destruction of information.
- Streamlined, worker-centric processes, allowing workers to easily raise concerns about demands to provide sensitive information in the pre/employment context can be established.
- Processes that can be used for reporting of breaches of worker privacy.
- Effective mechanisms for enforcement of privacy rights for workers.

Whilst enforcement of workers' privacy rights has not been discussed in detail in this report, effective enforcement must be a component of any new worker-centric privacy approach. A model of enforcement is outside the scope of this report. However, things that may form part of effective enforcement could include: mandatory, positive obligations on organisations for the timely reporting of breaches of worker privacy; meaningful penalties that act as a deterrent to organisations breaching the law; and co-enforcement models that include unions in enforcement activities.

Figure 2. Key aspects of a worker centric approach to privacy



Conclusion

The findings in this report show that some workers have little choice but to agree to undertake invasive testing that allows organisations (and third parties) to use the sensitive information gathered through these tests. In the examples discussed in this report workers were presented with a take it or leave it decision - No blood – No job. Australia's privacy laws offer little protection for such workers. Changes to privacy laws are needed to ensure workers have genuine control over their personal and sensitive information.

The gathering of sensitive information from workers should not be routine: it should be an exception that requires considerable justification. The imbalance of power in work relationships justifies comprehensive work-related provisions designed to address privacy and human rights concerns associated with the collection of personal and sensitive information from workers. Workers and their representatives should be involved in decision making and design of processes related to the collection and use of this information.

The use of biometric applications which gather some of the most sensitive information from workers is only likely to grow. The use of this sensitive information by AI systems in business and human resources processes adopted by organisations is also growing. Data breaches are becoming more common. Now is the time to tackle this difficult issue and to mandate that organisations respect workers' rights to have control over their personal and sensitive information.

References

Abraha 2024, *Bargaining over Workers' Data Rights: How Unions and Works Council Can Use Collective Bargaining to Specify Workplace Data Protection Norms*, Friedrich-Ebert-Stiftung Competence Centre on the Future of Work

Allen, Pritchard & Griggs (2013) 'A Workplace Drug Testing Act for Australia', *University of Queensland Law Journal,* 32(2), 219-235

Attorney General's Department (2021) *Privacy Act Review Discussion Paper October 2021*, Commonwealth of Australia

Attorney General's Department (2022) *Privacy Act Review: Report 2022*, Commonwealth of Australia

Australian Drug Testing (n.d.) *Pre-employment drug test: Everything you need to know*, https://www.australiadrugtesting.com/what-you-need-to-knnow-about-pre-employment-drug-test/

Australian Law Reform Commission (ALRC) (2000), *Review of Australia Privacy Law:* (Discussion Paper 72)

Australian Law Reform Commission (ALRC) (2023), *Essentially Yours: The Protection of Human Genetic Information in Australia* (Report 96)

Better Health (n.d.) *Heart attack and stroke- Calculating your risk score*, https://www.betterhealth.vic.gov.au/health/conditionsandtreatments/heart-disease-and-stroke-your-risk-score

Blackman (2024), *Submission to the Select Committee on Adopting Artificial Intelligence (AI)*, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Adopting_Artificial_Intelligence_AI/AdoptingAI/Submissions

Chen & Howe (2022) *Worker Data Right: the digital right of entry -Policy Brief 5, 2022*, Centre for Employment and Labour Relations Law, Melbourne Law School, University of Melbourne

Commonwealth of Australia (2023) *Government Response: Privacy Act Review Report*, https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report

Dreyfuss (2024) Speech to the Privacy by Design Awards, 2 May 2024, https://ministers.ag.gov.au/media-centre/speeches/privacy-design-awards-2024-02-05-2024

ETU (2021) *Submission to the Attorney General's Department Review of the Privacy Act 1998*, https://www.etunational.asn.au/wp-content/uploads/2022/04/220404-ETU-Sub-Privacy-Act-Review.pdf

Fair Work Ombudsman (2023), *Workplace privacy: Best Practice Guide*, https://www.fairwork.gov.au/sites/default/files/migration/711/workplace-privacy-best-practice-guide.pdf

Falk (2020) *Privacy Act Review: Issues Paper, Submission by the Office of the Australian Information Commissioner*, https://www.oaic.gov.au/__data/assets/pdf_file/0018/1773/privacy-act-review-issues-paper-submission.pdf

Fraser, Lindsay, Molitorisz, Wilding (2020), *Privacy Act Review Issues Paper, October 2020, Submission to Attorney-General's Department,* Centre for Media Transition, UTS

Gligorijevic (2020), *Submission to Review of the Privacy Act 1988,* http://dx.doi.org/10.2139/ssrn.3883020

Lucy (2012) Australian privacy legislation: An overview, *Precedent* (108), 4–9, https://search.informit.org/doi/10.3316/informit.272062569355854

Macdonald & Heap (2024) *Submission to the House of Representatives Standing Committee on Employment, Education and Training Inquiry into the Digital Transformation of Workplaces,* https://futurework.org.au/report/submission-to-the-house-of-representatives-standing-committee-on-employment-education-and-training-inquiry-into-the-digital-transformation-of-workplaces/

Minderoo Tech & Policy Lab, UWA Law School (2021), *Submission to the Review of the Privacy Act 1988 (Cth) – Issues Paper*, https://www.ag.gov.au/sites/default/files/2021-01/minderoo-tech-and-policy-lab-university-of-western-australia-law-school

Ng, Paterson, Pittard & Witzleb 2022, *Attorney-General's Department Review of the Privacy Act 1988: Submission in response to the Discussion Paper*, Castan Centre for Human Rights Law, Monash University

Read, Kantor, Graves, Lauder, Kallenbach (2023) *The most sweeping reforms to Australian privacy law in over twenty years,* https://www.minterellison.com/articles/the-most-sweeping-reforms-to-australian-privacy-law-in-over-twenty-years

Safework Health (2023), *Pre-employment drug and alcohol testing: What employers should know,* https://safeworkhealth.com.au/pre-employment-drug-testing-what-employers-should-know/

White (2020) 'Security guard at government building wins fight against boss over facial recognition technology', *The Canberra Times,* 27 July 2020, https://www.canberratimes.com.au/story/6837708/security-guard-at-government-building-wins-fight-against-boss-over-facial-recognition-technology/

Witzleb, (2018), 'Determinations Under the Privacy Act 1988 (Cth) as a Privacy Remedy' in Varuhas and Moreham (eds), *Remedies for Breach of Privacy*, Monash University Faculty of Law Legal Studies Research Paper No. 318939, https://ssrn.com/abstract=3189397

Youth Central (n.d.), *Drug testing at job interviews*, https://www.youthcentral.vic.gov.au/jobs-and-careers/job-interviews/attending-interviews/drug-testing-at-job-interviews#