PRIVACY ACT REVIEW

MARCH, 2023

ETU Submission to the Commonwealth Attorney General's Department's Review of the Privacy Act

31 March 2023

About the ETU

The Electrical Trades Union of Australia ('the ETU')[1] is the principal union for electrical and electrotechnology tradespeople and apprentices in Australia, representing well over sixty-thousand workers around the country.

Acknowledgement

In the spirit of reconciliation, the ETU acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all First Nations peoples today.

The ETU thanks the Department for the opportunity to participate in the Attorney General's Department (AGD) review of *the Privacy Act 1988 (Cth)* (Privacy Act) to date and the further opportunity to respond to the Privacy Act Review Report (the Report). This submission seeks to reiterate several areas the ETU is concerned the Report's proposals do not adequately address. It also reiterates our recommendations on what is needed to improve workers privacy.

Contents

[1] Being a division of the CEPU, a trade union registered under the *Fair Work (Registered Organisations) Act 2009* (Cth).

Divisional Secretary Allen Hicks
The Electrical Division of the Communications, Electrical, Electronic, Energy, Information, Postal, Plumbing and Allied Services Union of Australia
PO Box 380, Rosebery NSW 2018 | Suite 408, Level 4, 30-40 Harcourt Parade, Rosebery NSW 2018 | Ph: (02) 9663 3699 | Fax: (02) 9663 5599

Introduction

The ETU's focus is on the growing encroachment upon workers' rights by employers. Whilst there is a strong focus within the report on companies' obligations as they relate to consumer privacy and the need to bolster protections for customers, the same cannot be said for the rights of employees. A fundamental issue that needs to be addressed is why should employees not have at least the same rights as consumers. Workers are experiencing an unnecessary and expanding encroachment to their privacy during pre-employment processes, throughout the employment period, and with regard to post employment practices.

The ETU once again submits that practical steps must be taken by the AGD to vary relevant policy instruments in order to protect all workers' rights to privacy at all stages of the employment cycle.

The ETU believes structural reform is needed to:

1. Develop arbitrated privacy codes: developed, implemented, monitored, and reviewed on an industry basis;
2. Improve standing rights for workers and unions in privacy disputes, breaches, consultations, and complaints;
3. Introduce mandatory, positive obligations on employers for the timely reporting of breaches of worker privacy, with penalties for non-compliance;
4. Add express inclusion of privacy practices for the purpose of investigating a contravention under the right of entry provisions of the *Fair Work Act 2009* and other instruments

The right to privacy is fundamental, and the mere entering into an employment contract should not be licence for the abrogation of these rights. Rights to privacy in the employment context must be subject to equivalent protections as are found in other contexts. The nature and scope of employment, and the volume of data collected by employers incidental to the employment relationship has grown exponentially in recent times. This information encompasses highly sensitive subject matters (such as medical reports, medical and psychologist records, and disclosures of family and domestic violence) and includes information which, if collected in another context (such as a customer/supplier relationship), would be subject to the utmost protections.

Case Study – Pre-Employment Blood Testing

The ETU is concerned that private employers of its members are engaging in a practice of requiring prospective employees to undergo blood testing (which is undertaken by a third-party medical provider) as part of their pre-employment medical screenings. Such practice is being engaged in with the "consent" of the employee however, in reality, that "consent" is only provided because the prospective employee would otherwise not be considered for employment. It appears that employers are justifying this practice on the basis of their WHS obligations (to their employees) and contractual obligations (to their clients). Further, the ETU is concerned that such employers may be disclosing the results of the blood tests to overseas recipients. The National Office is not presently aware of how widespread this practice is.

Background

By way of example, in 2019 **SNC-Lavalin** introduced a practice of pre-employment blood testing. Prospective employees were asked to consent to the testing and to the information obtained from the testing being disclosed to:

a. Its related bodies corporates which are located overseas, noting that those overseas entities may use and disclose the information and that SNC-Lavalin is not required to ensure that those entities comply with Australian privacy laws; and
b. To its clients and other personnel.

SNC-Lavalin asserted that the practice was reasonably necessary for its activities, noting that:

a. It has WHS obligations to ensure that its employees are fit for their intended duties and work conditions, including remote work and operating vehicles; and
b. It has contractual obligations to its client (Shell/QGC) to undertake certain pre-employment medical examinations for prospective employees, including an assessment of their Cardiovascular Risk Score (**CRS**) which requires the taking of a blood sample.

The ETU obtained medical evidence to the effect that the blood testing (known as a lipid test) does not provide an answer to the risk of a patient having a cardiac event (in the next five to ten years) as it is only one element of a total risk profile for calculating such a risk and, further, that a person's risk profile can be reduced if they make lifestyle changes. The ETU then initiated proceedings against SNC-Lavalin, which prompted SNC-Lavalin to cease the practice.

Legal Context

It is arguable that private employers with an annual turnover of more than $3 million are contravening APPs 3, 5 and/or 8 in implementing a practice of pre-employment blood testing.

Whether or not an employer has contravened APPs 3, 5 and/or 8 will depend on:

a. The employer's specific purpose in requiring the blood testing;
b. Any expert evidence as to whether blood testing is capable of achieving that purpose;
c. The specific functions and activities of the employer;
d. How the jurisprudence in this area of law develops (noting that there are currently no analogous cases); and
e. Whether and how the Privacy Act is amended following this review.

The Privacy Act Review Report 2022 recommends that the Act should be amended to:

a. Introduce a further requirement that the collection of personal information must be "fair and reasonable in the circumstances"; and
b. Make clear that it is an objective test to be assessed from the prospective of a reasonable person.

It appears, although is not clear, that this recommendation also applies to the collection of sensitive information. The extension of this recommendation to the collection of sensitive information would assist in protecting prospective employees subjected to this practice.

Further, we note that the Report proposes the introduction of a statutory tort for serious invasions of privacy in the form recommended by the Australian Law Reform Commission (ALRC) in their Report No 123 of 3 September 2014. Whilst we acknowledge some benefit in this proposal, the tort will not assist in stamping out employer overreach in pre-employment blood testing because it is recommended that a defence of consent be available. As outlined at the beginning of this section, the reality is employers are obtaining prospective employees' 'consent' to the blood testing through the coercion of the employment offer. The proposed tort will not address this.

Given the ambiguous and untested nature of this area of law, legislative amendments that provide a right to employees and prospective employees to withhold consent to the collection of their personal and sensitive information are recommended in order to properly protect employees from this practice.

Necessary Structural Reform

Invasive breaches of workers privacy occur every single day in Australia with regard to fitness for work tests. Despite there being significant academic research and an Australian Standard that recognises that sobriety at work is best assessed using non-invasive breath and swab testing, employers continue to demand highly invasive urine, hair follicle and blood tests from the workforce under the guise of workplace health and safety. Adding insult to injury, the methodology for specimen testing can be deeply invasive, including at the extreme, urine sampling that requires the worker to provide a sample in direct line of sight of the testing personnel in a practice shockingly referred to as 'view stream'.

The Australian Government is a signatory to the *International Covenant on Civil and Political Rights: 1753*[2]*. Article 17* of that covenant says:

- *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*
- *Everyone has the right to the protection of the law against such interference or attacks.*

Arbitrated Privacy Codes

The ETU notes that the Report acknowledges that amendments are required, and that further consultation is required between employer and employee representatives to determine what those amendments should be. The ETU is prepared to and available to participate constructively in these discussions and believes they would be best facilitated by an amendment to the Privacy Act which requires privacy codes to be established in a manner similar to other Codes of Practice.

A broad approach (such as through amending privacy legislation) may not be able to effectively or adequately account for differences in which information may be considered relevant or necessary for employers to collect, store, and/or access across a range of industries. There is a clear need to establish a framework, similar to that adopted for safety codes of practice, that develops through arbitration, or equivalent if necessary, industry or

[2] https://indicators.ohchr.org/

sector based privacy codes.

Sectoral codes of practice for workplace privacy would allow a greater level of industry-specificity, ensuring that less workers are exposed to unnecessary overreach and providing clearer guidelines to assist employers in developing appropriate policies – rather than the race to the bottom we currently see in many industries.

Improved Standing Rights for Workers and their Representatives

Workers and their unions are severely limited in their ability to raise complaints against employers for invasive practices or actions otherwise covered by the *Privacy Act 1988* due to certain exemptions, vague definitions, and a fundamental misunderstanding of the nature of consent in the workplace built into the legislation. Further, unions are unable to make complaints to the Australian Information Commissioner in their own name on behalf of a group of workers (e.g. all prospective employees subject to pre-employment blood testing) without obtaining the written consent of each of those workers, even if those workers are members of eligible to be members of the union.

The Act specifically exempts employer practices directly related to their employee records, defined so broadly as to include health records and medical histories, from scrutiny. This exemption serves as a major roadblock for unions seeking to represent their members in instances wherein they believe such information to have been improperly collected, stored, or used. In order to improve the legal standing of employees and their union representatives seeking to remedy identified breaches of workers' right to privacy, the exemption for employee records ought to be removed from the Act and unions should be given standing to make complaints on behalf of persons whom are eligible to be their members.

Mandatory Breach Reporting

Data breaches and cybersecurity threats are becoming increasingly commonplace in the Australian private and public sectors, acknowledged by the Commonwealth in other portfolios with major investments into enhanced cybersecurity capabilities. As identified in the Department's Report, "the sensitivity, volume, and variety of information about employees held by employers put them at significant risk of harm".

Investments in cybersecurity and positive data protection obligations are an important step in limiting the capacity of these breaches to cause harm to employees, however it would be naïve to think that they will prevent them in their entirety. Employees deserve to be notified when a breach has occurred that has impacted their personal information similarly to existing provisions for breaches of consumer data. Security requirements under the Act and obligations under the NDB scheme ought to be applied in a workplace context, creating a positive obligation to notify employees of a breach and the ability to seek civil remedies for any fault that may lie with employers, or for failure to notify employees of a breach in a timely manner.

Right of Entry Provisions

Union officials are able to serve an essential function in assisting employees to identify, rectify, and report suspected breaches of an employee's right to privacy, however, under

current legislation there is almost no scope for officials to gain right of entry permits for the purposes of investigating the suspected mishandling or misuse of employee personal information. Investigation of privacy practices should be included explicitly in right of entry provisions of the *Fair Work Act 2009*.

Enabling employee representatives to take a more active role in protecting worker privacy at the ground level may assist the OAIC by alleviating some investigative workload and will add a further layer of deterrence for entities not to breach privacy laws, answering questions raised in 25.2 of the Report.

It is incumbent on the Australian Government to act now to protect the privacy of Australian workers from the increasing frequency and expansion of unnecessary and unreasonable employer overreach into workers privacy.

Recommendations

Recommendation 1: Amend the *Privacy Act* and *Fair Work Act* definitions and exemptions for "employee record" to:

- ensure workers (and where they choose, their unions) have standing on privacy matters under both the *Privacy Act* and the *Fair Work Act*;
- provide access for representative complaints for workers and their unions via section 38 of the *Privacy Act*; and
- limit the 'employee record' definition under the *Privacy Act* to ensure employers are only allowed to keep records consistent with the *Fair Work Regulations* and so that workers health data is protected, and
- expand the matters Entry Permit Holders are permitted to investigate, interview and request records of, to ensure they include privacy matters.

Recommendation 2: Amend the definition of 'health information' in the *Privacy Act* to limit the types of health information allowed to be accessed and retained by employers.

Recommendation 3: Recognise that the power imbalance between a worker applying for a job and an employer requesting privacy consent means that consent cannot reasonably be considered voluntary.

Recommendation 4: Introduce safeguards to ensure employers can only obtain health data for a primary purpose and that primary purposes are established via industry or sector guidelines in privacy codes. An entity should be made to outline the primary purpose for which the information is required, and the data obtained should be limited to that purpose.

Recommendation 5: Amend the *Privacy Act 1988* to require privacy codes to be developed in consultation with industry representatives similar to the manner in which safety Codes of Practice are developed. Privacy codes must clearly outline the types of health data permitted, how that information is allowed to be obtained and the minimum threshold employers are required to meet to demonstrate how a 'primary purpose' is being met.

Recommendation 6: Introduce mandatory reporting requirements for breaches of privacy that ensures workers are notified in a timely manner and provides for adequate remedies and enforcement.