Electrical Trades Union of Australia
Proud to be Union

31st March 2022

Australian Attorney-General's Department

By email: privacyactreview@ag.gov.au

ETU Submission to the Attorney General's Department Review of the Privacy Act 1998

The Electrical Trades Union of Australia ('the ETU') is a division of the Communications, Electrical and Plumbing Union ('the CEPU').[1] The ETU is the principal union for electrical and electrotechnology tradespeople and apprentices in Australia, representing well over sixty thousand workers around the country. The CEPU represents over one hundred thousand workers nationally, making us amongst the largest trade unions in Australia.

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 Nation peoples today.

The ETU welcomes the opportunity to provide feedback to the Attorney General's Department (AGD) review of *the Privacy Act 1988 (Cth)* (Privacy Act). The ETU is aware of the ACTU submission to this review and support the content contained therein. This submission seeks to briefly expand on the issues in that submission and provide the perspective of electrotechnology workers with regard to privacy as well as providing some additional recommendations to improve workers privacy.

The Union's focus is on the growing encroachment upon workers' rights by employers. This encroachment is occurring during pre-employment processes, throughout the employment period, and also with regard to post employment practices. This submission is concerned with practical steps that 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 reforms need to address the following:

1. arbitrated privacy codes: developed, implemented, monitored, and reviewed on an industry basis;
2. improved standing rights for workers and unions in privacy disputes, breaches, consultations, and complaints;
3. mandatory, positive obligations on employers for the timely reporting of breaches of worker privacy, with penalties for non-compliance;
4. 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

[1] CEPU is a registered organisation under the *Fair Work (Registered Organisations) Act 2009* (Cth).

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 and includes information which, if collected in another context (such as a customer/supplier relationship), would be subject to the utmost protections.

The ETU routinely represents members in relation to concerns, disputes and breaches of their privacy. Electrotechnology workers, and no doubt many others, are increasingly facing employers with ever expanding demands to accede to requests to invade their privacy. This is occurring prior to employment, during employment and even post-employment.

There is an overwhelming urgency to establish a framework, similar to that adopted for safety codes of practice, that develops, through arbitration or equivalent if necessary, industry or sector based privacy codes.

By way of example, one employer, SNC Lavalin, entered into a services contract previously held by a company Broadspectrum and, in doing so, all transferring employees (predominantly electrical and mechanical tradespersons) of Broadspectrum were required to apply for employment with SNC Lavalin in order to continue performing the jobs they were already doing. SNC Lavalin required all such employees to undertake medical screening which included a blood test as part of the 'recruitment' process.

SNC Lavalin disclosed that the purpose of the blood testing was to identify a risk profile for cardiac arrest. The risk profile, at best, would indicate whether the applicant had a 0% to 15% increase in risk of a cardiac event at some point in the subsequent three years. SNC Lavalin also required the job applicants to sign a very broad consent form which required them to consent to SNC Lavalin disclosing their medical information to its related bodies corporate which are not located in Australia, permitted the offshoring of blood samples, and agree that SNC Lavalin was not required to ensure that those entities complied with Australia's privacy laws, including the Privacy Act. The ETU filed proceedings against SNC Lavalin in the Federal Court in 2019, which promptly resolved by way of settlement.

While, *prima facie*, it appears these matters were resolved sensibly, the reality is that extraordinary resources were required to stop the employer from overreaching. Hundreds of person hours were expended by the Union, thousands of dollars of members money in legal fee's and hours and hours of the courts valuable time were used up when they should not have been. Further, it is wholly unclear what the Union's prospects were had the matter progressed to hearing, particularly with respect to standing. And despite this outcome, there has been no change of practice in the industry.

The ETU is aware that this practice is being adopted by many other employers. For example, the practice is being used by Primero (at the direction of FMG) at the Eliwana mine site in WA. FMG has refused to disclose the purpose of the blood testing, other than by quoting its health and safety obligations and asserting that blood tests may be necessary for high-risk roles in challenging working environments.

In addition, 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 personal in a practice shockingly referred to as 'view stream'.

As a final example, the ETU recently dealt with privacy concerns relating to vaccinations.

In the recent decision of *CFMEU v BHP Coal Pty Ltd [2022] FWC 81*, the Union parties argued against BHP's vaccination site-access requirement on the basis of the Privacy Act and the common law right to bodily integrity. In October 2021 BHP Coal implemented a mandatory vaccination policy, requiring all persons entering their 14 mine sites in Queensland, as a condition of entry, to provide evidence of their vaccination by 31 January 2022.

Whilst the outcome of that case was ultimately that the Deputy President Asbury determined that, yes, the Site Access Requirement is a lawful and reasonable direction having regard to the Privacy Act and the right to bodily integrity. This is actually a confirmation of the failure of the regulatory framework to protect workers privacy and establish community acceptable thresholds. But further to this, what was revealed during the case, was that BHP not only wanted evidentiary proof of vaccines beyond what should be considered reasonable, they had also at times wanted an unusual level of detail and access and control of workers private information, including:

- the 'brand' of each vaccine received, and
- copies of detailed medical records to prove it

In addition, BHP failed to adequately clarify:

- the extent and limitations to which they would share and or disclose this medical information, and
- where they would store this data, what security would apply to that data and for how long they would store it.

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.*

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.

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

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* 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.