NEW ZEALAND COUNCIL OF TRADE UNIONS
Te Kauae Kaimahi

Submission of the

New Zealand Council of Trade Unions Te Kauae Kaimahi,

New Zealand Public Service Association Te Pūkenga Here Tikanga Mahi (PSA),

E tū

and the

New Zealand Nurses Organisation

to

the Justice Committee

on the Privacy Bill 2018

Enquiries to:

CTU, P O Box 6645Wellington

31 May 2018

Table of contents

1. Introduction and outline of submission

1.1 This submission is made on behalf of the 30 unions affiliated to the New Zealand Council of Trade Unions Te Kauae Kaimahi (CTU). With 320,000 members, the CTU is one of the largest democratic organisations in New Zealand.

1.2 The CTU acknowledges Te Tiriti o Waitangi as the founding document of Aotearoa New Zealand and formally acknowledges this through Te Rūnanga o Ngā Kaimahi Māori o Aotearoa (Te Rūnanga) the Māori arm of Te Kauae Kaimahi (CTU) which represents approximately 60,000 Māori workers.

1.1 The submission has been made in collaboration with CTU affiliates, the New Zealand Public Service Association Te Pūkenga Here Tikanga Mahi (PSA), the New Zealand Nurses Organisation Tōpūtanga Tapuhi Kaitiaki o Aotearoa (NZNO) and E tū Incorporated (E tū).

1.2 The PSA is the largest trade union in New Zealand with over 64,000 members. It is a democratic organisation representing members in the public service, the wider state sector (the district health boards, crown research institutes and other crown entities), state owned enterprises, local government, tertiary education institutions and non-governmental organisations working in the health, social services and community sectors.

1.3 The PSA has been advocating for strong, innovative and effective public and community services since our establishment in 1913. People join the PSA to negotiate their terms of employment collectively, to have a voice within their workplace and to have an independent public voice on the quality of public and community services and how they are delivered.

1.4 E tū has 54,000 members. It is the second largest union in New Zealand and the largest private sector union. E tū was formed in 2015 out of a merger of the Engineering, Printing and Manufacturing Union, the Service and Food Workers Union and the Flight Attendants Union. E tū has membership in a broad span of industries from mining, construction, manufacturing and engineering to care and support work, cleaning, catering, security and other service-related areas. E tū has a similar number of male and female members and has a larger than average percentage of Maori, Pacific and migrant workers.

1.1 NZNO has 49,000 members, and is the leading professional and union representative of nurses and Māori nurses, and also represents midwives, kaiāwhina and nursing support workers, and nursing students. NZNO is committed to the representation of members and the promotion of nursing/midwifery. NZNO embraces te Tiriti O Waitangi and works to improve the health status of all peoples of Aotearoa New Zealand through participation in health and social policy development.

1.2 The CTU, PSA, NZNO and E tū (the authors) advocate for all New Zealanders to work in conditions of dignity and fairness, including the rights to privacy of workers. Accordingly this submission will consider the rights to privacy of workers and will consider whether the reform proposal in the Privacy Bill sufficiently takes this into account.

1.3 This submission will be divided into the following sections:

a. Domestic context
b. International context
    i. International obligations
    ii. ILO Code of Practice
    iii. EU Directive on Data Management
c. Support for Aspects of the Bill
d. Analysis of Privacy Issues in the Workplace
    i. Pre-employment privacy considerations
    ii. Drug testing
    iii. Psychometric testing
    iv. Covert recordings
    v. Monitoring (wearable devices & computer monitoring), the future of work and technological advancements
    vi. Use of Algorithms
    vii. Privacy issues and triangular employment regulation
    viii. Concerns with accredited employers for the purposes of ACC
    ix. Workers' rights to privacy and free trade agreements
e. Health and privacy
f. Beneficiaries rights to privacy
g. Recommendations
    i. Clarification of 'necessary test' in principle 1
    ii. Code of Practice for Workers' Rights to Privacy
    iii. Conduct wider consultation.
h. Conclusion

a. Domestic Context

1.4 This Bill is timely and essential to address the changes in the way New Zealand manages people's personal information. In particular this Bill is long awaited because of significant technological advances since the original Privacy Act's inception in 1993. The changes and progress in technology such as the internet, social media (Facebook,

Twitter, Instagram for example) cloud based data storage and the way we manage information means Privacy Laws needed modernisation. The Law Commission recognised this following their 2011 review seven years ago. Subsequently the need for this law reform has grown more urgent year by year. The rate of technological change also means issues around information and privacy and how we manage them will continue to increase and grow in their importance in the future. There is also considerable debate about the future of work and how technology will increasingly impact the way we work and the work we do in the next 20 years and beyond. Intrusions on privacy will be among the issues raised by developments such as automated decision making and the impact of technology on workers and their jobs.

1.5 The significance of technology and its impact on the management of people's personal information and how agencies (including many employers) manage that information cannot be underestimated. A privacy breach can have a significant impact on an individual. For example a victim of a breach may have to deal with the consequences of crime resulting from identity theft or a loss of sensitive data such as bank account details, IRD numbers, address and contact details which are used in fraud (known as "blagging").

1.6 In New Zealand, there is a well-established, but often under-recognised, nexus between privacy and employment law, with overlapping legal and policy issues between the two jurisdictions.

1.7 The major overlapping issues arising in the employment / privacy law interface, such as the collection of personal information for job applicants in pre-employment, covert recording of employees, monitoring, surveillance, and physical and psychological testing of employees, will be addressed individually in this submission.

1.8 Assessment of the balance of jurisprudence in this area reveals that employers have enjoyed the upper hand in privacy rights as a result of being able to rely on overriding practical, contractual and statutory obligations. As such, employer's requirements tend to function as the default position and privacy legislation in New Zealand generally tends to reinforce this position.[1]

[1] Paul Roth, 'Privacy in the Workplace', paper delivered to PSA, unpublished.

1.9 There are both historical and emerging trends with respect to intrusion on workers' rights to privacy. Technological advancement has provided further means to encroach upon workers' rights to privacy, and predictions are for this only to increase.

1.10 Two forces are combining to heighten concerns with the rights of privacy of workers: technological advancements and blurred lines between working and private life. Traditional arguments used by employers to ignore or override workers' rights to privacy, such as managerial prerogative or the purported need to intrude based on health and safety, are cited frequently. However, basing the necessity of employee privacy invasions on the foundation of needing to protect the employer's public image is increasing.[2] Technological developments have opened up new ways workers can be monitored both within and outside the workplace.

1.11 Privacy case law in New Zealand shows that the privacy principles in the current legislation do not form an effective bar to intrusions of workers' privacy rights. Employees enjoy some protections in discrimination and employment law, but these mechanisms are not able to address the trend of increasingly intrusive undermining of workers' rights to privacy.

1.12 There are three factors accounting for the lack of active protection for workers in the privacy context. Firstly, there is an outdated understanding of the employment relationship as being entirely consensual, thereby ignoring the imbalance of power in the relationship. Secondly the Privacy Commissioner has fallen into a legitimising role in relation to new technologies facilitated by the lack of any real power to exert control over new and intrusive practices.[3]

1.13 Thirdly there is a disjuncture in the current legislation between the approach taken by the Privacy Commissioner and the Human Rights Review Tribunal. The Privacy Commissioner's duty is to expressly balance privacy against other important social interests.[4] As complaints are brought in the first instance to the Privacy Commissioner, this duty acts as a filtering mechanism. The Tribunal and other judicial institutions are not bound by the same requirement.[5] This has allowed the Commissioner to operate in a manner that is less strict on employers, a conclusion which can be gleaned from

[2] Ronald McCallum, Employer Controls over Private Life, Sydney, 2002.
[3] Paul Roth, 'Privacy Law Reform in New Zealand: Will it Touch the Workplace?' (2016) 41 (2) *New Zealand Journal of Employment Relations* 36 at 38.
[4] Privacy Act 1993, s14(a)
[5] *Harder v Proceedings Commissioner* [2000] 3 NZLR 80 per [23].

analysis of the Privacy Commissioner's treatment of workers' rights to privacy cases (outlined below).

1.14 Conversely New Zealand employment law institutions have recognised the right to privacy of employees under the Privacy Act and used them to inform decisions on whether an employer's actions have been fair and reasonable even though they don't have express jurisdiction.

1.15 As a result, we argue that it is incumbent in considering a major reform to New Zealand privacy law - as this Bill seeks to do - to ensure consideration has been given to the right to privacy of people in relation to their employment.

1.16 The changes proposed by the Bill are largely in response to significant technological changes since 1993, and in particular the rise of the Internet and the digital economy. The Privacy Act does need to evolve to both meet current realties and anticipate future changes to the ways in which personal information can be collected, stored and used.

1.17 However, the current Bill does not adequately address the significant issues these changes have created for the protection of people's personal information at work.

1.18 The current Act has been interpreted by the courts as providing employers enhanced rights to access and use workers' personal information. The Bill continues this enhanced right largely unchanged and so perpetuates dated concepts of employment based on master-servant workplace relationships, which privilege employers' rights of property over individual's right to personal privacy. To continue this is inappropriate and out of touch with individuals' expectations this this modern democracy.

1.19 In addition, the changes proposed do not adequately meet the need for greater regulation of data in New Zealand in this new and evolving technological environment. In our view, while the Privacy Act must reflect and be responsive to this context, additional and separate regulation of data is needed.

1.20 After providing information on the right to privacy of workers in employment, this submission will outline a number of recommendations to ensure the reform of privacy law captures and addresses all the relevant issues. It is noted that as part of the consultation process for reforming privacy law in New Zealand, sectors such as trade unions and not-for-profit organisations were not consulted. This is the first opportunity for the CTU and is affiliates to raise these concerns.

b. International Context

1.21 New Zealand is not alone in recognising the need for change in our privacy laws as evidenced by the fact that most privacy laws around the world have been reviewed or updated in the past three years.

1.22 Quite apart from the domestic legal context for the delivery and protection of privacy rights in New Zealand, New Zealand is bound by international obligations to uphold the right to privacy.

1.23 New Zealand is legally bound to give substance to the right to privacy, as provided for under art 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR) which says[6]:

> 1. 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.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

1.24 In addition to being bound by the ICCPR, New Zealand also has a Privacy Act:

> …to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines).[7]

1.25 There is also the International Labour Organisation (ILO) Code of Practice on the Protection of Worker's Personal Data. The Code balances the legitimate interest of agencies in relation to the protection of their property and the monitoring of workers' performance and health and safety; and the rights of workers to privacy and personal dignity. It provides a set of general principles to govern the collection, storage, security, use and communication of workers' personal data. Worker here includes not only current workers, but former workers and job applicants as well. Personal data means any information related to an identified or identifiable worker.

[6] 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976); ratified by New Zealand on 28 December 1978.
[7] Privacy Act 1993, long title.

1.26 European countries are beginning a wave of reform of data management practice following the issuing of the General Protection of Data Regulations[8] (the GPDR) by the European Union, which came into force on 25 May 2018. This document provides a base guideline of best practice for a number of organisations globally. It also throws light on New Zealand's need for our privacy laws to be updated to keep up with global changes around privacy. The regulations "give individuals greater control over their data by setting out additional and more clearly defined rights for individuals whose personal data is collected and processed by organisations. The GDPR also imposes corresponding and greatly increased obligations on organisations that collect this data"[9].

1.27 The GDPR is based on the core principles of data protection which exist under current law. Privacy principles, such as those proposed in the Bill are integral to the GDPR, including its principles. However the GDPR goes further by requiring organisations developing data systems to include privacy as a design feature of those systems.

1.28 The New Zealand government and the European Commission are about to begin negotiations for a New Zealand-European Union trade and investment agreement. Its likely provisions, including on "e-commerce", will have significant impacts on privacy and the European Union requires privacy laws in the Parties to such agreements to be consistent with the GDPR.

1.29 These instruments should be taken into account in reforming privacy law in New Zealand.

2. Support for Aspects of the Bill

2.1 Despite the CTU's submission that a 'workers' rights to privacy' lens has not been applied to the reform process so far, the CTU believes an overhaul of privacy law is well overdue and the current proposal includes some important reforms.

2.2 There are six key areas of reform in this bill:

- Strengthening cross border data flow protections;
- Mandatory data breach reporting of privacy breaches. (Currently in New Zealand there is only voluntary reporting);

[8] https://www.eugdpr.org/eugdpr.org-1.html
[9] http://gdprandyou.ie/gdpr-for-individuals/

- Compliance Notices;
- Introduction of new criminal offences – specifically it will be an offence to mislead an agency in a way that affects someone else's information and to knowingly destroy documents containing personal information where a request has been made for it;
- Access requests - Ability of the Privacy Commissioner to make binding decisions on access requests, enabling the Commissioner to make decisions on complaints relating to access to information rather than the Human Rights Review Tribunal; and,
- Strengthening the Privacy Commissioners existing investigation power by allowing him or her to shorten the timeframe within which an agency must comply and by increasing the penalty for non-compliance.

2.3 By way of general comment we support the retention of the 12 flexible privacy principles. These principles have served us well, are generally easily understood by the public assisting with access to justice where a complainant can determine if they have grounds for complaint and then feel confident to take action for redress of a breach.

2.4 The principles are also fundamental in guiding agencies about how they need to manage personal information they collect, use, store and destroy and will in many instances inform privacy management policy for agencies. They inform and guide agency and individual alike and we support their retention.

2.5 Cross Border Data Flow Protections

2.6 The more substantive changes are in Principle 11 (new subclauses 3-6 and clause 20 of the Privacy Bill) which relate to information been disclosed to agencies outside New Zealand. We consider the creation of additional obligations on agencies where they are disclosing personal information across borders is a necessary and sensible amendment given the increase of data flows outside of New Zealand borders due to technology. This has been happening for some time and the law needed updating to reflect this.

2.7 It is fundamental an agency brings to an individual's attention where their information is being shared outside of New Zealand and the individual is given the opportunity to authorise such action. This is particularly applicable in a New Zealand employment context where an employer has its payroll or human resources function based outside of New Zealand. We have members employed by companies whose payroll and in some instances human resources functions are managed from Australia. We also

have members employed by companies whose payroll is processed outside New Zealand.

2.8 Therefore New Zealand employee pay-related information and personal details are crossing borders frequently. New Zealand employees need assurance their personal data will be safe as identifying information and bank account details are transferred. In one case currently before the Employment Relations Authority, the New Zealand employees' timesheets are sent to Melbourne then on to not one but two other companies, outside Australia, for processing. The information is then sent back to Australia before the wages are paid into New Zealand bank accounts.

2.9 We therefore welcome the strengthening of principle 11 to require employer agencies to consider their obligations to employees and other individuals more carefully.

2.10 However, as is recognised in the Employment Relations Act 2000,[10] there is an inherent imbalance in the power between employee and employer; therefore, while the employer agency must seek authority from the employee concerned for the disclosure of their information to an overseas person, the employee may have no other choice than to agree, particularly if they wish to be paid. This creates an absence of mutuality in the agreement to allow information to be transferred and raises the question: does this provide enough of a safeguard or go far enough to protect employees' personal information?

2.11 We propose a Code of Practice for Workers' Rights to Privacy be developed to flesh out what steps an employer should take in these types of situations to protect New Zealand employee personal information. This is particularly important given the regular movement of personal information of New Zealand employees across borders that has increased as a result of technology such as email and payroll processing systems.

2.12 Mandatory Data Breach Reporting – Part 6 Privacy Bill

2.13 We support the introduction of mandatory reporting. The introduction of a mandatory data breach reporting requirement brings us into line with overseas legislation and regulations. It is our hope this requirement will have the impact upon agencies that they are motivated to take a proactive approach to managing the safety of personal information they collect, use and store on a daily basis and this change in the law will

[10] Employment Relations Act 2000, Part 1 Section(3)(a)(ii)

see agencies take privacy more seriously in order to avoid triggering the reporting requirement. Also this new requirement will reduce the risk of harm to individuals resulting from privacy breaches.

2.14 It is our hope the result of this new requirement will encourage agencies to have clear, documented policy and processes around privacy and information management if they currently don't and that there will be a greater focus on education of staff around privacy and what is required of them to protect the information held by their agency in their daily work.

2.15 The requirement to notify the Privacy Commissioner of a breach and then to also notify the individual will be a further motivating factor for agencies. Where it is not "reasonably practicable" to notify the individual, having to provide a public notice will also be a significant deterrent, as an employer agency would want to avoid due to potential reputational damage and economic consequences.

2.16 However, to be effective, this will require employers to invest time and money into education of their employees to manage the new reporting requirement. Awareness amongst employees and employers regarding privacy issues and agencies' obligations currently varies widely agency to agency and there is inconsistency in approach, in our experience. The ability to manage such regulation will be far more feasible for larger well-resourced employers, than smaller employer with fewer resources and less capacity to manage privacy issues. Again, a Code of Practice for Workers' Rights to Privacy could ease that burden and ensure consistent compliance.

2.17 Without such a supporting mechanism, we anticipate employees will be scapegoated if the employer agency breaches its obligations and is exposed by the mandatory notification requirements. Such an eventuality would be consistent with the punitive response to employee error following the increased liability on companies under the Health and Safety at Work Act. Care needs to be taken to avoid a similar unintended consequence in this context. We therefore urge the adoption of an express duty to educate employees tasked with implementing compliance measures. We submit that should a code of practice be developed that focuses on the unique interface between employment and privacy, mechanisms could be included to require the employing agency to meet an appropriate standard for staff education around privacy and process. This would mitigate against the unintended consequences of superficial compliance practices supplemented by punitive action against employees where there

is a privacy breach. This would also support the adoption of meaningful and effective preventative action rather than knee-jerk responses when breaches occur.

2.18 We note the ILO's Code of Practice on the Protection of Workers' Personal Data[11] at clause 5.9 promotes as a general principle that those who process data should be regularly trained to ensure they understand the process and their role in applying privacy principles. This further supports the proactive development of a Code of Practice for Workers' Rights to Privacy within the New Zealand environment.

2.19 The adoption of a Code of Practice for Workers' Rights to Privacy will benefit both employees and employers. At a recent Privacy Forum at Te Papa on 9 May 2018 in Wellington, held by the Office of the Privacy Commissioner, the Head of Digital for Spark[12] spoke of their support for a process which supported staff through breaches to create a culture where people know they can report a breach rather than acting in punitive way. This resonates with our experience: If fear surrounds the occurrence of a breach, the impetus to disclose and remedy it is undermined. The open reporting of adverse events (i.e events with negative reactions or results that are unintended, unexpected or unplanned) is integral to quality and safety systems in several sectors, including health and aviation, and are supported by robust learning programmes. Supporting compliance by employees and employers with a code that clarifies effective education and training are necessary to managing this requirement and will greatly enhance the successful implementation of the new requirements.

2.20 Mandatory Breach Notification Reporting – the legal test

2.21 There is some concern that the requirement of mandatory reporting could lead to over reporting of privacy breaches. This is because the definition in the bill of a notifiable privacy breach that would have to be reported is framed very broadly. Clause 117 defines that a notifiable privacy breach will be a breach that has caused any of the types of harm set out at clause 75(2)(b) of an affected individual or there is "a risk it will do so" . The interference with the individual's privacy has to be a breach as per clause 75 (2) it must also be an action as described at clause 75(2)(b) of the Privacy Bill which states:

The action –

[11]http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf
[12] Sarah Auva'a Head of Digital Trust, Spark New Zealand.

(i) has caused, or may cause, loss, detriment, damage, or injury to the individual; or

(ii) has adversely affected, or may adversely affect, the rights, benefits, privileges, obligations or interests of the individual; or

(iii) has resulted in, or may result in significant humiliation, significant loss of dignity, or significant injury to feelings of the individual.

2.22 The test required for a notifiable privacy breach in Australian legislation that came into effect from 22 February 2018[13] is based on a much narrower legal test relating to a reasonableness standard. In Australia a breach must be reported when there is an unauthorised access to, unauthorised disclosure of or loss of personal information held by an entity and a reasonable person concludes that unauthorised action is likely to result in serious harm to the individual, whom the information relates. Notification must occur if the agency or entity has "reasonable grounds to be believe" an eligible data breach has happened.

2.23 We are concerned the broad nature of the proposed test for a notifiable breach in this Bill will be difficult to work with and create confusion amongst agencies and for those subject to a breach and would result in inconsistent application and over reporting. We submit this test needs simplification and further examination of other jurisdictions close to our own such as Australia and Canada appears warranted.

2.24 Exceptions to obligations to notify of data breach

2.25 We accept it may be appropriate for an exception to notification to arise where there are sound medical reasons as determined by an approved health practitioner relating to physical or mental health of an individual and the other exceptions relating to the defence of New Zealand and maintenance of law enforcement.

2.26 With respect to clause 120 we submit this provision requires further consideration by the Committee. In particular clause 120(5)(b) identifies a "representative" for the purposes of this provision to include: "for an affected individual aged 16 or over, means an individual appearing to be lawfully acting on that individual's behalf or in that

[13] Privacy Amendment (Notifiable Data Breaches) Act 2017.

individual's interests." Our concern is that in an employment setting this definition of representative could be construed as including a union organiser or union delegate.

2.27 Unions are incorporated societies with a statutory duty of good faith to their members. The intentional withholding of information about a member, from that person, would impair the relationship between the union and its member and could expose the union to a claim of bad faith. Yet if there was a reasonable basis to be concerned that disclosure of a breach of privacy may compromise the employee's physical or emotional wellbeing, the union would be faced with a dilemma not of its own making. It also raises the spectre of the union taking on the role of delivering bad news to an employee arising from the employer's breach and it is not the role of unions to provide a conduit for employers to avoid their responsibility. We suggest that the definition of "representative" be amended to expressly exclude union representatives. In applying this provision in an employment context we can envisage a situation where an employer agency breaches privacy and is required to make a notifiable breach however they determine that due to the exemption at clause 120(2)(b) they won't notify the individual concerned but notify a "representative." That representative, if a union official then becomes responsible for notifying the individual of the privacy breach. That individual may be compromised due to physical or mental health concerns. It is not desirable that a union official could find themselves having to deliver that notification instead of the employer.

2.28 Compliance Notices

2.29 The Bill provides that the Privacy Commissioner will be able to issue compliance notices that require an agency to do something or stop doing something, in order to comply with the Privacy Act. The Human Rights Review Tribunal will then be able to enforce compliance notices and hear appeals. We support this change in the law giving the Privacy Commissioner a stronger ability to respond to Privacy breaches and consider this change will serve to better encourage compliance and have the desired effect of reducing the risk of privacy breaches. Currently the Privacy Commissioner is only able to make recommendations, the incentive to pursue those recommendations is weighed against other business interests and potential costs which then undermines the aims of the Privacy Commission to protect individual's personal information and undermines confidence in a system that is supposed to address privacy breaches.

2.30 The current system aims to seek voluntary compliance; however, if an agency is unmotivated to change their privacy practices they will continue to mismanage privacy

and their practice and process will not be fit for purpose and potentially cause harm. Therefore strengthening the ability of the regulator to manage behaviour that compromises privacy of individual's information has to be supported as it will improve outcomes by compelling agencies to act or face the potential of a compliance order. There was comment in a Law Commission paper[14] that this change may assist to address systemic failures that contribute to a breach causing harm. Therefore changing behaviours is behind these proposed amendments and that should be supported. However in the employment context it also provides further support for a Privacy Employment Code to be implemented as well as these changes to support a platform for a change of behaviour amongst employer agencies with a code that sets out clear expectations for employers on various matters impacting employees and their privacy within employment.

2.31 Allowing the Privacy Commissioner to make these orders rather than the Human Rights Review Tribunal also means the process can help an individual more quickly reducing bureaucracy and potentially reducing the risk of more harm to individual's privacy as the Commissioner can make the agency act in specified time frames. The Commissioner will be involved at the complaint stage and also at the compliance stage rather than the matter moving to the Human Rights Review Tribunal.

2.32 Sometimes speedy action is required to stop abuse of rights, and a compliance process provides that option. The Law Commission's report also noted that the current processes involving the Office of the Privacy Commissioner and the Human Rights Review Tribunal when managing a complaint was "clunky" and resulted in duplication of investigations by two bodies, which meant longer time frames and greater expense. Therefore we support this change as it will be more streamlined, reduce delays for complainants and should be more efficient and cost-effective. However we also think it is important to continue the focus of the Privacy Commissioner's process on conciliation as the first option for resolution with compliance orders only where such process is unsuccessful.

2.33 New Criminal Offences

2.34 In line with other parts of this Bill which strengthen the need to comply, increased financial penalties for serious offences such as destroying documents and digital files

[14] Review of the Privacy Act, Review of the Law of Privacy Stage 4, Law Commission, June 2011, Report 123 http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R123.pdf.

requested seems appropriate. Current financial penalties of $2000 are simply too low and the proposed $10,000 will support an approach of encouraging compliance.

2.35 Access Determinations

2.36 Currently over half the complaints received by the Office of the Privacy Commissioner relate to access issues.[15] Access to information is an important right underpinning an entitlement to fairness and having an even playing field. An employee cannot challenge if they don't have all the information or facts. This is particularly true within an employment context where there is already a power imbalance between the employer and the employee which is well recognised by the Employment Relations Act.

2.37 Currently only the Human Rights Review Tribunal can make determinations about access. Information is power and the ability to access information addresses imbalances created by not having all the necessary information.

2.38 In terms of access to justice, a quicker response would create greater satisfaction to individuals when attempting to address their complaints and also give greater confidence in the system.

2.39 Therefore we support the inclusion of powers in the Privacy Bill allowing the Privacy Commissioner to make binding decisions on access rather than the matter having to be referred onto the Human Rights Review Tribunal. As a result of clause 96 of the Bill upon investigating a privacy complaint the Commissioner will now have the power to make various determinations on access to information sought by a complainant, whereas currently the matter would have had to be referred to the Human Rights Review Tribunal after investigation by the Commissioner. This will undoubtedly speed up the outcome of a complaint process.

2.40 As well as improving access to justice and the above reasons there are other significant benefits for these changes. For example it will take pressure off the Human Rights Review Tribunal which is currently facing significant delays in working through cases. We have some concerns about how the new work load will be managed by the Office of the Privacy Commissioner; however, we take note of the Law Commission

[15] Regulatory Impact Statements at: https://treasury.govt.nz/sites/default/files/2014-08/ris-justice-sgr-aug14.pdf

Report which stated it believed significant efficiencies will be gained by the introduction of these new powers.[16]

2.41 The Commissioner's power to determine complaints about access to personal information is likely to lead to quicker responses and could include voluntary releases occurring more frequently by agencies rather than awaiting a determination. Having a system that enables shorter time periods is ultimately better when seeking access. The right of appeal period under clause 11 of the Bill requiring an agency to lodge the appeal within 20 days ensures if an agency wants to appeal it will have to make its decision in a timely way. These elements are important to ensure the individual subject to the breach is not further disadvantaged by delays in legal processes and that these are reduced as much as is possible while trying to balance fairness to both parties. Delay can be used as a tactic to wear opponents down; therefore a 20 day right of appeal balances all parties' interests. The ability to move through the process without too much delay is at the heart of a good process the public can have confidence in. This is also further supported by the retention of continuing The Commissioner's initial focus on problem resolution through conciliation of a privacy complaint.

2.42 Access determinations won't be published, however as there may be public benefit in publishing case notes as a matter of education on what is an appropriate request etc we support publishing of case notes on access determinations. This will also assist in education about access determinations and when they may be granted, which may provide guidance to parties in dispute.

3. Analysis of Privacy Issues in the Workplace

3.1 This section of the submission will consider the following:

a. Pre-employment privacy considerations
b. Drug testing
c. Psychometric testing
d. Covert recordings
e. Monitoring (wearable devices & computer monitoring), future of work and technological advances
f. Use of Algorithms
g. Privacy issues and triangular employment regulation

[16] Review of the Privacy Act, Review of the Law of Privacy Stage 4, Law Commission, June 2011, Report 123.

h. Concerns with accredited employers for the purposes of ACC

a. Pre-employment

3.2 There are concerns regarding the protection of the privacy of job applicants in the pre-employment environment. Like most jurisdictions, employment, discrimination and human rights law provide some remedies for discriminatory hiring practices. However, without more explicit legal protection, job applicants are ordinarily not in a position to refuse to disclose information requested by an employer or employment agency.

3.3 For instance, in case No 2418, the Privacy Commissioner found that personality testing of job applicants was permissible under the Privacy Act.[17] In coming to this finding, the Commissioner did not address the intrusiveness of the test or its relevance to the particular position sought by the applicant.

3.4 Requests for medical information and ACC history of job applicants is a further area of concern. Employers are permitted to seek such information to be compliant with their health and safety obligations, or to establish employee's ability to perform the role, but are not entitled to request information beyond those boundaries.

3.5 However the boundaries between and understanding of the rules that apply to personal and health information are routinely misapplied and/or misunderstood.

3.6 The Health Information Privacy Code 1994 ("the Code") sits within the Privacy legislation, and sets specific rules for agencies in the health sector. It covers health information collected, used, held and disclosed by health agencies and takes the place of the information privacy principles for the health sector.

3.7 Health practitioners registered under the Health Practitioners Competence Assurance Act 2003 must comply with the Code, as well as professional obligations of confidentiality and trust. (There are some exceptions to this disclosure, such as, for example with a school nurse when a health condition affects learning or when there are accidents and incidents that need to be investigated to lessen the threat of harm to others.) However the different privacy protocols that apply to health, as opposed to personal information, are poorly understood and can interfere with both employees' and health consumers' rights.

[17] Privacy Commissioner *Case Note 2418* [1999] NZPrivCmr 6.

3.8 For instance, NZNO is aware of instances where employees have been asked for, and in some cases have agreed to, full disclosure of health information (eg in relation to ACC), without being aware of the distinct protections for the privacy of this information and their right to restrict access.

3.9 Similarly, despite the Commissioner's excellent publication *Privacy in Schools,* there needs to be more awareness in schools of the difference between academic/ educational information on a student and health information. School nurses are occasionally pressured for student's health information, as some schools consider they have both a right and a duty to be informed about health matters, and some school IT systems make it difficult to separate access to health information (which should not be available to teachers or the principal) and record to the academic/ educational information.

3.10 Strengthening the role of the Commissioner, as this Bill does, should enable more opportunities for public education about privacy rights and responsibilities.

3.11 A specific issue has also arisen in relation to the mandatory pre-employment and subsequent three yearly safety check process under the Vulnerable Children Act 2014. These go beyond a check on criminal convictions, and may include anything documented by the police, regardless of the relevance or involvement of the person being checked. There have been instances where a domestic violence issue, neighbour dispute, etc. has come up as part of the screening process which employees have not been aware of and have not 'self reported'. The process has also been problematic for employers who have to decide what to do with the information sent, especially if an employee's privacy has been breached.

3.12 Natural justice demands that employees and prospective employees have full and timely access to any personal information disclosed to a third party. However, it is likely that a statutory framework for the Policy Vetting Service (which the government has been proposed) will be necessary to address the issues around poorly conceived and burdensome requirement for constant screening and vetting of children's workers.

b. <u>Drug testing</u>

3.13 The permissibility of drug and alcohol testing has tended to be determined by employment law rather than privacy law in New Zealand, with the focus being an employer's statutory and common law obligations in terms of health and safety.

3.14 However, drug and alcohol testing involves the collection, storage, and use of what is very sensitive personal information from employees, and the Privacy Principles are therefore engaged and highly relevant. For example, the Privacy Act should be able to protect employees from drug and alcohol testing that was unreasonably intrusive under Principle 4, or that is unnecessary or not for a lawful purpose, under Principle 1.

3.15 Whether an employer's drug and alcohol testing regime can be challenged will depend very much on the facts of the case. However, there is limited guidance available to assist employers in fairly and reasonably deciding whether or not a drug and alcohol testing regime can be justified in the first place, let alone what to test for, the proper procedure to follow, how the results should be interpreted, or who are appropriate persons to carry out the testing and to see the results. This lack of guidance was noted by the Employment Court in the seminal *NZ Amalgamated Engineering, Printing & Manufacturing Union Inc v Air New Zealand Ltd* case, when it stated that it was unsatisfactory that there was no legislation that "specifies any limitations upon this power or any safeguards as to the use to which the evidence obtained with the co-operation of employees may be put."

3.16 As drug and alcohol testing requires the taking of a bodily sample, it is a serious and highly intrusive process. It also affects an employee's choices outside the workplace, as tests can detect further than current impairment. As such, it should be subject to appropriate constraints that reflect this significance. With drug and alcohol testing now becoming the norm amongst New Zealand employers, we would support the joint development of a code of practice in this area, which could address issues relating to justification, necessity, testing procedures, analysis, disclosure and use of results.

c. <u>Psychometric testing</u>

3.17 We also have significant concerns about the use of psychometric testing in the workplace and its impact on privacy.

3.18 Our experience is that psychometric testing is used by many public service and other employers in both the recruitment and restructuring processes. For example, responses to a 2013 Official Information Act request by the PSA indicated that over the previous year all government departments had used psychometric testing in recruitment, with several also using it on existing employees when selecting for jobs or promotion. Just last year Inland Revenue undertook a large scale restructuring of

its staff and required 900 employees who sought to retain employment to undergo psychometric testing.

3.19 Several aspects of psychometric testing are at odds with the Privacy Principles.

3.20 Principle 4 requires that the collection of personal information must be obtained by fair and lawful means. However, psychometric testing has been criticised as being "pseudoscientific" and of questionable substance, reliability and validity.[18] It has also been found to discriminate against workers with disabilities such as Autistic Spectrum Condition.[19] To the extent that this is true of any particular psychometric testing regime, it is neither fair nor lawful.

3.21 The nature of the questions asked are often such that the individual being tested may be unsure exactly what information they are disclosing about themselves, risking a breach of Principle 3, which requires an individual to be made aware of the fact that the information is being collected. Questions such as "If I wanted to I could disguise myself as someone else" and "Sometimes I feel a kind of power around me" are illustrative,[20] and may well lead applicants to divulge information that they did not intend to divulge, or are at best unaware that they are divulging.

3.22 When used in any selection process, it is necessary to ensure that what the test is designed to measure is directly related to a specific job requirement, or the information gathered will not be necessary for the purpose, and the employer will be in breach of Principle 1. As we have noted elsewhere, we support the strengthening/stricter interpretation of the "necessary to collect" test of Principle 1 to better protect employees from unnecessarily intrusive and unreasonable information gathering by employers.

3.23 Further, the confidentiality agreements that psychometric testing companies require employer clients to sign mean that Principle 6 is breached, as employees are unable to gain access to the results of their tests to ensure their accuracy. This is also a breach of natural justice, and of the duty of good faith under section 4(1A) of the Employment Relations Act 2000 as employers are unable to comply with their

[18] Annie Murphy Paul, *The Cult of Personality: How Personality Tests are Leading Us to Miseducate Our Children, Mismanage Our Companies , and Misunderstand Ourselves* (Free Press, New York, 2004);
[19] For example: *The Government Legal Service v T Brookes*, UK Employment Appeal Tribunal, UKEAT/0302/16/RN.
[20] Example questions from psychometric tests carried out by the Ministry of Business, Innovation and Employment on its health and safety inspectors in 2013.

obligation to provide all relevant information, a point which has been stressed by our Employment Court.[21]

3.24 Once collected, the personal information of employees is commonly retained by the testing company and used for its own commercial purposes and benefit. Employees must be made aware of this and consent to it, otherwise a breach of multiple Principles will occur.

3.25 The current Act and/or its interpretation by the Privacy Commissioner have seen breaches of privacy through psychometric testing go unchallenged. In one case, a woman who applied for a sales representative role was asked to complete a form containing 200 questions, some of which were personality and attitude questions unrelated to, and too personal for, the role. The Privacy Commissioner did not address the intrusiveness of the test or its relevance to the particular position applied for, and instead focused on a technical failure to comply with procedure.[22] In another, which dealt with the situation later criticised by the Employment Court in the Gilbert case above, an employer's refusal to provide an employee with their psychometric test results was held not to breach Principle 6 on the basis that its agreement with the testing company required this.[23]

3.26 We consider that many of our above concerns about psychometric testing could be addressed by having accepted standards expressed clearly in a code of practice on the protection of worker's personal information. We also consider that clauses 53 and 55 of the Bill should be amended to eliminate the ability for psychometric test results to be withheld from individuals on the grounds that they are subject to a confidentiality agreement or trade secret interest between the employer and another entity.

d. <u>Covert recordings</u>

3.27 There have been cases involving workplace surveillance considered by the Privacy Commissioner which have found workplace surveillance to be a permissible practice. In New Zealand, there are few legal controls on surreptitious video or audio recording in the workplace.

[21] *Derek Wayne Gilbert v Transfield Services (New Zealand) Ltd* [2013] NZEmpC 71.
[22] Case Note 2418 [1999] NZ PrivCmr 6.
[23] Case Note 88333 [2007] NZ PrivCmr 4.

e. Monitoring (wearable devices & computer monitoring), future of work and technological advances

3.28 More and more people are using digital devices and applications in their work, generating growing quantities of personal data, which can be collected, stored and analysed. Electronic monitoring through devices placed in the workplace or worn or used by workers is increasingly commonplace. The embedding of identifying and recording devices within an employee's body (such as under the skin) is even being contemplated by some employers overseas according to media reports.[24]

3.29 Workers have always been watched at work, and using technology to do this, such as clocking out, is not new. What is new is the level of intrusiveness that digital technologies enable and the intimacy of the information that is collected. Surveillance through keystroke monitoring and CCTV are common in New Zealand workplaces. Workers can be fitted with badges that track not only their location but also monitor their tone of voice, how often they speak, to who they speak and for how long. Devices can capture information about heart rate, health and how long a worker spends in the toilet.

3.30 The question is, does the benefit to employers from increased performance informed by this kind of personal information justify the level of intrusion into individual people's privacy?

3.31 Research indicates that while electronic surveillance may give employers a lot of personal information about a worker, it may not achieve the aim of increasing productivity but instead, in a kind of "transparency paradox", reduce performance by inducing those observed to conceal their activity through codes and other costly behaviours. In our view these kinds of practices treat workers as somehow less than human and are a low road approach to productivity that should not be further enabled by the Bill, which is at its heart is concerned with a civil liberty

f. Use of Algorithms

3.32 The creation of algorithms is a critical element of automated decision making. Algorithms and the rise of artificial intelligence is to become an increasing feature of

[24] E.g. "Cyborgs at work: Employees getting implanted with microchips", by James Brooks, 4 April 2017, https://www.stuff.co.nz/technology/digital-living/91175604/cyborgs-at-work-employees-getting-implanted-with-microchips; "American company installing microchips into employees", 24 July 2017, http://www.newshub.co.nz/home/world/2017/07/american-company-installing-microchips-into-employees.html

our future world. However the significant resourcing benefits technology such as automated decision making brings to employer agencies must not outweigh the caution with which this technology must be managed to ensure the rights of employees are not undermined.[25]

3.33 This technology has the potential to impact significantly on decisions affecting many individuals including thousands of employees into the future. We do not profess to be experts upon the subject of algorithms and expect the Committee will receive feedback from those better qualified to comment and we are aware there is research being carried out on algorithms and artificial intelligence at Otago University[26] and commentary by the Office of the Privacy Commissioner. However due to their likely impact upon employees and privacy, we wish to make some comment within this submission to say the use of such technology requires careful consideration and controls. It may be that within a Code of Employment Privacy which has been proposed by this submission further work will need to be done to investigate and better understand all of the issues and their potential to impact on employment decisions and privacy.

3.34 Generally what we already know from recent evidence of New Zealand case law and overseas cases such as the *State and Loomis*[27], caution is needed when using information produced by automated systems, particularly as it relates to employees. In the case of *Gilbert*[28] the judge was highly critical of the use of a psychometric testing tool to evaluate employees for redundancy selection. The owners of the testing system wanted to keep the ingredients and results of their system secret, the judge commented this "illustrated the inappropriateness of its use in a process that requires openness and information exchange", the companies' refusal to provide the actual test scores and inability to access the proprietorial intellectual property of the testing organisation, including the questions asked and the actual questions given, was found by the judge not to be consistent with the requirements of the Employment Relations Act to share information, disclosure and objective rationality.[29]

[25] In mathematics and computer science, an **algorithm** (/ˈælgərɪðəm/ (listen) *AL-gə-ridh-əm*) is an unambiguous specification of how to solve a class of problems. Algorithms can perform calculation, data processing and automated reasoning tasks. (https://en.wikipedia.org/wiki/Algorithm)

[26] See further research by Associate Professor Colin Gavaghan, Otago University and others on artificial intelligence issues around ethics, law and policy https://www.otago.ac.nz/news/news/otago633498.html

[27] https://harvardlawreview.org/2017/03/state-v-loomis/

[28] Derek Wayne Gilbert v Transfield Services (New Zealand) Ltd [2013] NZEmpC 71.

[29] Derek Wayne Gilbert v Transfield Services (New Zealand) Ltd [2013] NZEmpC 71. Para [111]

3.35 We also take note of the ILO's Code of Practice on the Protection of Workers' Personal Data which provides us with some guidance about how to manage automated systems and employees information. The code includes within its scope at clause 4.1(b) the application of manual and automatic processing of all data. At clause 5.5 of its general principles it states decisions concerning a worker should not be based solely on the automated processing of that worker's personal data and at 5.6 Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance. The principles on individual rights at 11.2 regarding access to all data relevant to the employee including data created by automated systems and 12.2 regarding collective rights requires employees and their representatives should know about the introduction and modification of automated systems that process employees' data. These provisions highlight important rights that require consideration in this context and provide support for the submission that there be a Privacy and Employment Code that also considers the impact of automated decision making upon employees and what rights need to be identified for employees to protect them.

3.36 We also submit there needs to be a combined approach when dealing with decision making based on commercially created algorithms that involves principles including (not intended to be exhaustive):

- human oversight from the beginning;
- greater transparency about what information and data is drawn into algorithmic programs that are developed for software that will impact on decisions involving employees;
- that it be recognised there are limitations with automated decision making such as the potential for bias and perpetuation of bias and discrimination;
- disclosure to the affected employees of the algorithms used; and
- a weighing of the benefit vs the risks of their use.

g. Privacy issues and triangular employment regulation

3.37 Recently the CTU and PSA have submitted on the member's Bill before the Select Committee, the Employment Relations (Triangular Employment) Amendment Bill.

3.38 In this submission serious concerns were raised about the misuse of personal information by host employers in triangular employment relationships.

3.39 Presently, as the CTU understands it, host employers can access a range of information from the labour hire agency in order to choose workers. This information relates to protected attributes of age, sex etc. This information can be used by host employers for discriminatory purposes. The Bill must also seek to address this phenomenon.

h. Concerns with accredited employers for the purposes of ACC

3.40 The ACC systems in New Zealand establishes a regime of 'accredited employers' for the purposes of self-insurance. Under this regime, there is significant potential for, and many known instances, of the privacy rights of workers being breached by the unlawful sharing of workers' information between the employer as employer and the employer as the accredited employer carrying out its responsibility to provide accident compensation and rehabilitation on behalf of ACC. This is particularly the case with respect to medical information of employees, which can be used to disadvantage workers in their employment, such as dismissing them on medical grounds. It is a serious deficit in the protection of workers' rights to privacy not adequately addressed or considered in the current Bill.

i. Workers' rights to privacy and free trade agreements

3.41 New Zealand is seeking to conclude further free trade and investment agreements. Currently the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) is close to ratification; as noted above negotiations are about to begin for an agreement with the European Union, and negotiations are active with the Pacific Alliance. These agreements contain provisions with respect to labour rights and also impact on privacy rights such as through their E-Commerce provisions. Consistent with reform of privacy law in New Zealand, consideration needs to be given to ensuring both labour and privacy-related provisions in trade and investment agreements are informed by New Zealand privacy law.

4. Health and privacy

4.1 The impact of the collection and use of personal data by companies afforded by new technologies extends well beyond individuals. There is significant concern about the potential to amplify harmful health behaviours, especially in relation to tobacco and

alcohol use. For instance, tobacco giant Philip Morris is currently seeking regulatory approval for a new smoking device that the iQOS smoking device is built with circuitry that enables it to collect personal data about users' smoking habits and utilise it for marketing purposes.[30] The alcohol industry already uses a range of social media to identify and target customers. Public health and wellbeing must be considered in relation to privacy law and corporations' collection and use of personal information.

4.2 We welcome and support Clause 52 which ensures that "in any case where an agency is proposing to refuse an access request because disclosure of the information would be likely to prejudice the physical or mental health of the requestor, the agency may consult with the requestor's health practitioner (and is not limited to consulting with the requestor's medical practitioner as currently)". This is a necessary amendment, consistent with the Health Practitioners Competence Assurance Act 2003, and recognises that there are other registered health practitioners besides medical practitioners whom it may be relevant to consult with.

5. Beneficiaries' rights to privacy

5.1 In addition to the workers' rights to privacy dimension of privacy law, there is an additional framework of analysis relating to beneficiaries' rights to privacy which should be undertaken to ensure the completeness of the privacy law reform in New Zealand.

5.2 The CTU is aware that the Ministry of Social Development uses data tracking for the purposes of fraud detection. The human rights implications of this data gathering should be considered within this reform process.

5.3 Whilst the CTU does not consider itself to be the content expert in this area, the CTU urges the Select Committee to ensure sufficient consultation has taken place with advocacy groups within this and related health, tamarki ora, social and housing sectors.

6. Recommendations

6.1 Having regard to the content of our submissions, we recommend as follows:

a. <u>Reform of necessary test in principle 1</u>

[30] https://www.reuters.com/investigates/special-report/tobacco-iqos-device/

6.2 Taking into account case law in the form of Privacy Commissioner case comments, we recommend that the test of 'necessary' outlined in principle 1, as reflected in both the current Privacy Act and replicated in the Privacy Bill, be tightened to confirm a high threshold for the meaning 'necessary'. Case law on this provision under the current law has been too lax. The views of the Privacy Commissioner on a number of complaints indicate that, non-derogable or not, the "necessary to collect" test in principle 1 involves a low threshold that is not difficult for an employer to satisfy.[31]

6.3 The employer ought to bear the burden of proving that a test is indeed "necessary".

b. Code of Practice for Workers' Rights to Privacy

6.4 The current Privacy Act at s 46 and s 35 of the Privacy Bill 2018 both contain provision for the Privacy Commissioner to establish a Codes of Practice. In addition to requiring the Bill to ensure it captures issues regarding workers' right to privacy, we recommend that the Privacy Commissioner be tasked with developing a Code of Practice for Workers' Rights Privacy.

6.5 We recommend that the Committee refer the Bill back to officials to enable work on a code of practice on the protection of workers' personal information, based on the International Labour Organisation's Code of Practice on the Protection of Workers' Personal Data[32] and drawing on the European General Protection of Data Regulations.

c. Conduct wider consultation.

Consistent with our submission on the dimension of beneficiaries' rights to privacy, we are aware that widespread consultation other than through the Law Commission process, has not taken place and should take place to ensure all views are taken into account. Essentially New Zealand cannot purport to undertake comprehensive reform of privacy law without undertaking widespread consultation with affected groups of interests.

7. Conclusion

[31] Paul Roth, 'Privacy Law Reform in New Zealand: Will it Touch the Workplace?' (2016) 41 (2) *New Zealand Journal of Employment Relations* 36 at 42.
[32] http://www.ilo.org/safework/info/standards-and-instruments/codes/WCMS_107797/lang--en/index.htm

7.1 We support aspects of the improvements in the Privacy Bill, but consider that the dimension of workers' rights to privacy, and beneficiaries' rights to privacy, have not been given sufficient consideration.

7.2 Privacy legislation is most important for providing employment law with a source of accepted standards of what society regards as fair and reasonable in relation to the handling of worker's personal information and their expectations of privacy.[33] As technology advances, lawmakers must seek to strengthen and enforce people's rights to privacy as it relates to their employment.

7.3 As a result, we consider that the Bill should not proceed in its current form. In the alternative, there should be an undertaking that the Privacy Commissioner engage with the union movement regarding the development of a Code of Practice for Workers' Rights to Privacy.

7.4 The CTU, accompanied by affiliates, wish to make an oral submission to the Select Committee.

[33] Paul Roth, 'Privacy Law Reform in New Zealand: Will it Touch the Workplace?' (2016) 41 (2) *New Zealand Journal of Employment Relations* 36 at 57.