NEW SOUTH WALES SOCIETY OF
LABOR LAWYERS

E: info@nswlaborlawyers.com
W: www.nswlaborlawyers.com

7 September 2020

Mr Daniel Mookhey MLC
Chair, Workplace Technology Inquiry
Parliament House
Macquarie Street
Sydney NSW 2000

By email: *futureofwork@parliament.nsw.gov.au*

Dear Chair,

Submission to the Select Committee on the impact of technological and other change on the future of work and workers in New South Wales

The New South Wales Society of Labor Lawyers ('the Society') welcomes the opportunity to make a submission to the Select Committee on the impact of technological and other change on the future of work and workers in New South Wales ('the Committee').

By way of background, the Society, originally established in 1977, aims to promote changes in the substantive and procedural law, the administration of justice, the legal profession, legal services, legal aid and legal education to help bring about a more just and equitable society. The Society provides a meeting ground for people involved in the law who believe in Labor principles of fairness, social justice, equal opportunity, compassion and community. The Society's membership and supporters include barristers, solicitors and trade union industrial officers working across the legal field.

The Society submits in relation to term of reference 1(h) which asks whether current laws and workplace protections are fit for purpose in the 21st century, including, amongst other things, workplace surveillance laws. In particular, the Society makes submissions in relation to the *Workplace Surveillance Act 2005* (NSW) ('WSA').

The timing of this inquiry could not be more significant. As the COVID-19 pandemic displaces employees around Australia and the world, novel work arrangements have arisen. Many employees have been forced through no fault of their own to conduct their day-to-day roles from their private homes. It is likely, even after the COVID-19 pandemic subsides, that workplaces in Australia will not be the same as they were prior to the pandemic, and that many practices established during the pandemic will continue. The transition to working from home in particular raises complicated issues in relation to the surveillance of employees by employers outside of the workplace, an issue which, in our view, necessitates a rethink of existing workplace surveillance legislation in NSW to achieve protection of privacy in the workplace. For example, monitoring software is increasingly being used in Australia to record the behaviour of employees at their place at work, whether that be a work premises or their personal home. Recent reports indicate that since the COVID-19 pandemic began there has been a significant uptake of these types of technologies by employers across the country[1]. Such technologies include software that tracks keystrokes, computer idle time and screen activity. This rise is not

[1] Some companies offering this software have reported an increase of 300 percent in sales in the months leading into May 2020: see Patrick Wood, 'Employee monitoring software surges as companies send staff home', *Australian Broadcasting Corporation* (online, 22 May 2020).

unexpected; employers have a legitimate need to monitor the performance of their employees, especially when one of the primary methods of monitoring, by proximity, has been disrupted. However, it calls into question the adequacy of our workplace surveillance laws, which are currently not adapted to deal with the rise in these types of technologies.

Background to workplace surveillance legislation

Workplace surveillance is governed by the WSA. For overt surveillance, the WSA requires that an employer provide at least 14 days' notice to an employee if the employer plans to conduct surveillance of an employee[2]. The notice must include particulars around, *inter alia*, the kind of surveillance to be carried out, how it will be carried out and when it will commence[3]. The notice period required for overt surveillance may be commenced by means of a policy[4]. This has meant that the notice requirements of the provision may be met by putting in place an encompassing policy which sets out the notice requirements. For covert surveillance, the WSA provides that an employer can only conduct covert surveillance of an employee if the employer has obtained a covert surveillance authority[5], and that can only be granted for the purpose of establishing whether an employee is involved in unlawful activity (being an offence under NSW or Commonwealth law)[6].

Both overt and covert surveillance include surveillance conducted through the means of a camera or tracking device, or by software or other equipment that monitors or records the information input or output, or other use, of a computer[7]. In relation to computer surveillance, the WSA provides that this type of surveillance must be carried out in accordance with a policy of the employer on computer surveillance of employees of work, and the employee must be notified in advance of that policy 'in such a way that is reasonable to assume that the employee is aware of and understands the policy'.[8] In relation to camera surveillance, the WSA requires that any cameras be clearly visible and that there be signs at the entrance to each surveilled place notifying employees that they are subject to camera surveillance[9]. There is also an outright prohibition on all forms of surveillance in a change room, toilet, shower or bath facility in the workplace[10].

To a lesser extent, the *Surveillance Devices Act 2007* (NSW) ('SDA') also regulates the use of surveillance devices (within and outside of NSW workplaces) by prohibiting the use and installation of surveillance devices. In particular, the SDA prohibits the use of a listening device to record a private conversation without the consent of the parties to the conversation[11], including the use of a camera surveillance device to monitor a private conversation[12].

The Society's general approach to workplace surveillance legislation

Our Society's view is that workplace surveillance laws in Australia are unnecessarily complex. The regulatory framework is different in each state and territory in the country, with some states (including NSW) having multiple statutes governing the use of surveillance in the workplace. The legal requirements as between states are different, in some cases substantially different. For example, NSW, Victoria and the ACT have specific workplace surveillance legislation (and corresponding notice and policy requirements for employers) whereas other states and territories regulate workplace surveillance

[2] WSA, s 10.
[3] WSA, s 10.
[4] WSA, s 13(5).
[5] WSA, s 19.
[6] WSA, s 23.
[7] WSA, s 3.
[8] WSA, s 12.
[9] WSA, s 11.
[10] WSA, s 15.
[11] SDA, s 7.
[12] WSA, s 3 – see notes to definition of 'surveillance'.

through their general privacy and surveillance laws. The inconsistency across jurisdictions creates regulatory confusion for employees, employers and industrial associations. It also creates unequal privacy rights as between employees in different states and within the same companies. The result is confusion over legal rights and unnecessary costs to the employer for compliance in different states. Like the Australian Law Reform Commission[13], our Society supports a uniform national law governing workplace surveillance in Australia. The NSW Government should continuously make representations at a federal level in support of this uniform legislation.

Proposals for reform

In the absence of uniform laws at a federal level, we consider this Committee is well placed to proactively update NSW workplace surveillance laws for a contemporary context. We recommend the following changes be made to the WSA to provide greater protection for the privacy of employees in NSW workplaces:

A. Create Additional Privacy Protections

In our view, the widescale uptake in monitoring software in Australia is cause for alarm. This is because the WSA contains limited protections against misuse of monitoring software. 'Computer surveillance', which extends to 'surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer', is couched in broad terms and likely covers such software. To introduce such surveillance in the form of monitoring software, an employer need only provide 14 days' notice to the employee[14] and have a policy which governs the surveillance which is brought to the attention of the employee[15].

We consider the WSA is lacking in protections against misuse and overuse of surveillance technology, particularly monitoring software. A new provision should be inserted into the WSA to the effect that any surveillance conducted in accordance with the WSA be conducted solely for a 'legitimate purpose' and not breach an employee's 'reasonable expectation of privacy'. The latter of these requirements is intended to, amongst other things, protect employees from surveillance that may monitor private activities conducted on a work device, for example, screen capturing of private email accounts or keylogging of private passwords. An onus should be placed on the employer to establish that such surveillance has met both these requirements. Contravention of the provision would, like for other provisions of the WSA, carry a maximum penalty, and would factor into the Fair Work Commission's approach to the admissibility of evidence obtained in breach of workplace surveillance laws[16].

At least in relation to continuous monitoring software, being software that continuously or at regular intervals monitors the input and output of a computer, we recommend that the Committee go further and consider amending the WSA such that an employer is required to consider less intrusive means of surveillance before implementing such technology. There are usually less intrusive methods of measuring metrics such as employee performance than software that constantly tracks computer activity. Employers should be required to consider these options before taking steps to constantly monitor their employees.

In addition to data access rights (discussed below), we also consider it important that the WSA be amended to ensure that any data collected on employees is collected in accordance with, or by a

[13] ALRC, *Serious Invasions of Privacy in the Digital Era*, (Report 123, June 2014), Recommendation 14-6.
[14] WSA, s 10.
[15] WSA, s 12.
[16] See the recent decision in *Krav Maga Defence Institute Pty Ltd t/a KMDI v Saar Markovitch* [2019] FWCFB 263 which found that unlawfully obtained surveillance evidence was admissible, after giving weight to the discretions in s 138 of the *Evidence Act 1995* (Cth), which the Commission is not bound by but should give regard to in its consideration of admissibility.

similar process to, the guidelines contained in the *Privacy Act 1998* (Cth). For example, an employer should not collect the personal information of an employee unless it be 'reasonably necessary' or 'directly related' to the employer's activities.[17] Further, any sensitive information regarding an employee (for example, race, sex, gender etc.) should not be collected by an employer unless the employee consents to the collection of this data and the collection of sensitive information is 'reasonably necessary' or 'directly related' to the employer's activities.[18]

B. Introduce Data Access Rights

In order for the protections afforded in the WSA (and the changes recommended in this submission) to be effective, we consider that employees should have the right to obtain, on request, the product of any surveillance activity, as it relates to them. Such access rights would enable employees and their industrial organisations to assess the intrusiveness of any surveillance activity, address any concerns that the surveillance activity may be in breach of the WSA or any workplace policy, and create an equal footing in internal performance management or misconduct investigations. Proper access rights in the WSA are essential given the increasing prevalence of monitoring software in the workplace.

C. Introduce Consultation Rights

The WSA does not require an employer to consult with employees prior to the introduction of surveillance, nor establish if there is any legitimate need for surveillance. In the ACT, employers are required to consult with employees for the minimum notice period specified in their workplace surveillance law (14 days) and they are required to do so in good faith (meaning the employee is given a genuine opportunity to influence the conduct of the surveillance)[19]. We recommend that a similar provision be inserted into the WSA to require mandatory consultation periods with employees prior to the introduction of workplace surveillance as well as disclosure of the purpose of the surveillance. The purpose of a consultation provision would be to promote good faith arrangements between employers and employees, and promote open dialogue on issues to do with surveillance.

D. Prohibit Surveillance at Additional Locations

The WSA prohibits the carrying out of surveillance in a change room, toilet, shower or bath facility in the workplace[20]. This prohibition lags behind interstate counterparts: see s 7, *Surveillance Devices Act 1999* (Vic) and s 41, *Workplace Privacy Act 2011* (ACT). In line with these interstate equivalents, we recommend that the WSA be amended to include nursing, sick, first aid, prayer and breastfeeding rooms to expand the prohibition on surveillance and promote privacy in these facilities.

E. Clarify the Definition of 'Surveillance'

While we consider that the definition of 'surveillance' in s 3 of the WSA addresses most forms of workplace surveillance technology currently in the market, the definition could be amended to include the following, for the avoidance of doubt. Firstly, we suggest amending the definition of 'camera surveillance' to include cameras installed on workplace devices such as laptops and smart phones. Secondly, we suggest amending the definition of 'tracking surveillance' to include heat and motion sensors that are used for the purpose of monitoring an employee's activities. Thirdly, we suggest removing the 'primary purpose' requirement from the definition of 'tracking surveillance' such that the definition unequivocally applies to devices that record geographical location and movement regardless

[17] *Privacy Act 1988* s Sch 1.
[18] Ibid.
[19] *Workplace Privacy Act 2011* (ACT), s 14.
[20] WSA, s 15.

of whether this function is the primary purpose of the device. Where a device performs a surveillance or tracking function (as most phones and tablets now do), employees should be informed before this feature is activated and used by the employer, and such use should be subject to the consultation provisions proposed earlier in this submission.

F. Extend Protections to Independent Contractors

The WSA currently adopts the definition of employee in s 5 of the *Industrial Relations Act 1996* (NSW) ('IRA'), which broadly includes 'a person employed in any industry' and also employees under Chapter 6 of the IRA and persons performing voluntary work. Schedule 1 of the IRA states that 'employee' also includes certain categories of work, some of which could include the roles performed by independent contractors. However, there is no encompassing inclusion of independent contractors within the WSA. We consider the definition in s 3 of the WSA should be amended to extend protections in the WSA to any independent contractors who enter into a contract for services with a company, to ensure that independent contractors in NSW are subject to the same workplace surveillance regime.

G. Consolidated Surveillance Legislation

The Society also recommends that the Committee consider rationalising the WSA and SDA into one consolidated statute that governs the use of surveillance devices in NSW. In our view, a unified regime in NSW would improve the simplicity and efficiency of the system and ultimately lead to improved privacy outcomes.

We thank you for your consideration of this submission. Please contact the undersigned at info@nswlaborlawyers.com if the Committee requires any further submissions.

Yours faithfully,

NSW Society of Labor Lawyers