THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: P&DL:RHap1966131

31 August 2020

The Hon Daniel Mookhey MLC
Committee Chair
Select Committee on the impact of technological and other change on the future of work and workers in New South Wales
Legislative Council
Parliament House, Macquarie Street
Sydney NSW 2000

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

Dear Mr Mookhey,

Inquiry into the impact of technological and other change on the future of work and workers in New South Wales

The Law Society of New South Wales welcomes the opportunity to provide 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 (Select Committee) as part of its current inquiry. The Law Society's Privacy and Data Law Committee has contributed to this submission.

While acknowledging the broad terms of reference for the Select Committee's inquiry, this submission focuses exclusively on issues around workplace surveillance, per term of reference h:

> Whether current laws and workplace protections are fit for purpose in the 21st century, including workplace surveillance laws and provisions dealing with workplace change obligations and consequences.

Workplace surveillance during COVID-19

There has been dramatic growth[1] in the range of potential surveillance by employers and collection of data about employees' activities, both in employer-provided workplaces and elsewhere.[2] Those means are increasingly automated and remote from the employee: unobserved by the employee and potentially covert.

The COVID-19 pandemic and associated lockdown has accelerated this growth. For security and other reasons, many employees use laptops, smartphones and online (cloud) resources. Services are made available or paid for by employers, but are also often permitted to be used for personal, social and family activities. These devices and services may be used anywhere

[1]Patrick Wood, "Employee monitoring software surges as companies send staff home", *the ABC*, 22 May 2020.

[2] See further Peter Leonard, 'Data Ownership and the Regulation of Data Driven Businesses', Scitech Lawyer (American Bar Association), 16/2, Winter 2020.

and anytime, and during COVID-19 lockdown, are usually used at home, including for permitted private purposes.

Many employers initially scrambled to enable remote working under COVID-19 restrictions without first evaluating whether associated monitoring was reasonable and proportionate. Upon the re-opening of workplaces, some employers are implementing new technologies to monitor workplace activities to address COVID-19 related health and safety concerns. As employer-provided workplaces reopen, COVID-19 risk management and monitoring provide an opportunity for employers to expand surveillance activities and the collection of data about employee activities and movements.

Many employers may carefully consider the use of such activities, and those activities may be reasonable and proportionate to address real public health or security risks. For some business activities, for example, monitoring is becoming commonplace for quality control or assurance, for risk management (for example, driver fatigue[3]) or as a regulatory requirement. Cyberthreats and data exfiltrations have rightly led to employer concerns about the management of confidential and commercially sensitive information on employee devices and through online resources that employees access and use. Moreover, humans are fallible. Work-related data is as accessible as the weakest vulnerability point in the work data ecosystem allows it to be found. The employee who is rogue or careless with data can create large financial and reputational exposures for employers, through data breach liability (see for example, Morrisons Supermarkets[4]) or damage from other data exfiltrations.

While there may be legitimate reasons for employers to undertake surveillance over employees, the Law Society considers that the current workplace surveillance framework should be reviewed and revised. This is particularly important at a time when the use of surveillance and tracking in workplaces and elsewhere is rapidly proliferating.

Current workplace surveillance laws

NSW is one of the few Australian jurisdictions with specific legislation to regulate the surveillance of employees in the workplace. As the Select Committee is aware, the *Workplace Surveillance Act 2005* (NSW) (WSA) sets out the circumstances in which an employer may lawfully undertake surveillance of employees.

The WSA defines 'surveillance' as meaning camera, computer and tracking surveillance.[5] The WSA does not apply to surveillance by means of a listening device.[6] Camera surveillance regulated by the WSA will also be regulated by the *Surveillance Devices Act 2007* (SDA) if the camera is used to record the audio of a private conversation.

The provisions of the WSA apply whenever employees are 'at work', which is defined broadly to mean any time an employee is at the workplace, whether or not the employee is performing

---

[3] For example, http://www.smartcaptech.com/ and case studies at http://www.smartcaptech.com/case-study/ and https://www.nhvr.gov.au/news/2018/12/14/new-smartcap-fatigue-technology-trial-kicks-off-to-improve-heavy-vehicle-safety-around-port-of.

[4] *WM Morrison Supermarkets plc (Appellant) v Various Claimants* (Respondents) [2020] UKSC 12 (on appeal from [2018] EWCA Civ 2339); compare NSW Informational Privacy Rights: Legislative Scope and Interpretation - Employer, Employee, and Agent Responsibilities - A Special Report under Section 61C Privacy and *Personal Information Protection Act 1998;* Anna Johnston, Salinger Privacy, Training is key to avoiding liability for rogue employees, blog post of 1 October 2019, https://www.salingerprivacy.com.au/2019/10/01/training-is-key/; *Director General, Department of Education and Training v MT* [2006] NSWCA 270; *DGL v Illawarra Shoalhaven Local Health District* [2018] NSWCATAD 296.

[5] *Workplace Surveillance Act 2005* (NSW) s 3.

[6] *Workplace Surveillance Act 2005* (NSW) s 3.

work, or any time the employee is performing work, even if they are not at the workplace (for example, employees working from home).[7]

Generally, surveillance of an employee must not commence without prior notice in writing to the employee.[8] Notice must be given at least 14 days prior to the surveillance commencing, unless the employee agrees to a lesser period of notice.[9] The WSA contains specific requirements for notices to be present on vehicles that are the subject of tracking, for computer monitoring policies, notices identifying that cameras are operating in the workplace and for cameras to be visible in the workplace. The WSA also regulates the disclosure and use of surveillance records.

Surveillance of change rooms and bathrooms, even with notice, is prohibited.[10] An employer is also prohibited from undertaking covert surveillance of an employee while the employee is at work for the employer unless the surveillance is authorised by a covert surveillance authority.[11] The WSA sets out the procedure to obtain such an authority.[12]

The WSA creates summary offences for non-compliance with various provisions of that Act, including in relation to surveillance in changerooms and bathrooms and while an employee is not at work; restrictions on the use and disclosure of surveillance records; and the use of covert surveillance authorities.

Organisational accountability

Surveillance technologies and activities now commonly include listening or audio surveillance; data surveillance (including surveillance of email communications, computer usage and internet activities); optical or visual surveillance; tracking or location surveillance and biometric surveillance (including fingerprints, cheek swabs, iris scans and blood).

The Law Society notes that reasonable and proportionate surveillance in a workplace can benefit both employers and employees in many ways, including by improving the safety and security of property and personnel; ensuring that the employer is providing a safe system of work; increasing business efficiency and performance; enabling employee performance management, and assisting in reducing adverse consequences of fatigue.

However, expansion of surveillance activities and the collection of data about employee activities and movements often creates tension between an employer and employees. This tension is often exacerbated where expansions of such activities are not fully transparent or properly explained to employees; or because the expansion is not limited to such activities as are reasonable, necessary and proportionate to address an identified need; or because the activities are not conducted with proper risk assessment and the mitigation of associated risks by implementation of reasonable controls and safeguards.

Moreover, there is currently no legal protection to ensure that surveillance activities and the collection of data about employee activities and movements are properly evaluated by each employer, applying a standard of reasonableness or fairness. Nor is there any requirement for an employer to apply any test as to the necessity or proportionality of a relevant privacy-affecting act or practice of surveillance and collection of data about employees' activities.

---

[7] *Workplace Surveillance Act 2005* (NSW) s 5.
[8] *Workplace Surveillance Act 2005* (NSW) s 10(1).
[9] *Workplace Surveillance Act 2005* (NSW) s 10(2).
[10] *Workplace Surveillance Act 2005* (NSW) s 15.
[11] *Workplace Surveillance Act 2005* (NSW) s 19.
[12] *Workplace Surveillance Act 2005* (NSW) Part 4, Division 2.

In our view, human dignity requires that an individual be able to go about their life without unreasonable or covert intrusions into what they do, why they do what they do, with whom and where. This includes a right to go about in public (including online and in workplaces) without unreasonable intrusions upon an individual's ability to be a private self in public (including online and in workplaces). This is not an absolute right, and should not prevail over other basic human rights, such as a right to protection of health and safety, or the legitimate requirements of an employer to ensure an efficient, safe, and secure working environment.

Our existing data privacy and surveillance laws are intended to empower individuals by informing them how data about them may be being collected and used, and thereby enable them to exercise a choice. This is the 'notice and choice', or 'notice and consent', framework for data privacy and surveillance regulation. However, the capacity to choose, or withhold consent, is significantly constrained for employees, particularly as unemployment rates rise.

In our view, 'notice and choice', or 'notice and consent' should be supplemented with an additional requirement of demonstrated organisational accountability of an entity (such as an employer) that is collecting, handling or disclosing personal information about the affected individual (such as an employee), or conducting surveillance in a workplace context. An appropriate framework would ensure that an employee is not only provided with a description of the reason and extent of surveillance and data collection by an employer, but would also make an employer accountable to ensure that a proposed activity of surveillance or data collection is necessary and proportionate to achieving a reasonable outcome, with reasonableness judged by consideration of the degree and extent of impact upon legitimate expectations of privacy, societal interests (such as the health and safety of other individuals), and the interests of the employer in conducting its operations in a safe and efficient workplace.

There is a range of international examples for the adoption of such an approach. For example, we note subsection 5(3) (appropriate purposes) of the Personal Information Protection and Electronic Documents Act of Canada (PIPEA),[13] relevantly provides: 'An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances'. In applying subsection 5(3), Canadian courts have generally taken into consideration whether the collection, use or disclosure of personal information is directed to a bona fide business interest, and whether the loss of privacy is proportional to any benefit gained.[14] The following factors have been stated to be relevant in determining whether an organisation's purpose complies with subsection 5(3):

- the degree of sensitivity of the personal information at issue;
- whether the organisation's purpose represents a legitimate need / bona fide business interest;
- whether the collection, use and disclosure would be effective in meeting the organisation's need;
- whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and
- whether the loss of privacy is proportional to the benefits.[15]

[13] Available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/.
[14] Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)", May 2018, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/, under heading "Evaluating an organization's purposes under 5(3)"; *A.T. v. Globe24h.com* [2017] FC 114.
[15] *A.T. v. Globe24h.com*, [2017] FC 114 at [74]; Ibid; also, *Turner v. Telus Communications Inc* [2005] FC 1601 at [39], aff'd [2007] FCA 21, at [48].

While relevant in relation to general surveillance, the Law Society considers this change in regulatory framework is particularly required in relation to workplace surveillance. There is currently no effective regulatory oversight or control of workplace surveillance activities, which appears to be a significant legal gap, particularly noting that the collection and use of personal information about employees is regulated by data privacy statutes and Federal and State privacy commissioners.

Interaction with the SDA

As noted above, the WSA does not regulate audio surveillance or the recording of private conversations. Surveillance by means of a listening device is regulated by the SDA. This includes listening devices attached to a camera in the workplace. Therefore, optical and audio surveillance of employees while at work will fall under the regulation of both the WSA and SDA.

The Law Society considers that having two separate pieces of legislation can create confusion and dissonance. While the provisions of the WSA, particularly in relation to the notice requirements and prohibitions around recording in changerooms and bathrooms, are important and should be retained, we suggest a review of the legislative framework in this area, and consideration of whether the WSA should be retained as a standalone piece of legislation, or possibly incorporated, as a separate Division, into the SDA.

Review of the SDA framework

The Law Society notes that the SDA regulates the making and use of audio recordings in NSW generally, beyond the regulation of workplace audio surveillance.

If feasible, we suggest the Select Committee consider the current framework under the SDA as part of this inquiry.

We draw the Select Committee's attention to the Queensland Law Reform Commission's (QLRC) recently published review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies.[16] The review provides a comprehensive analysis of current surveillance device laws in Queensland and recommends the adoption of a new framework for protecting an individual's privacy from unjustified interference from the use, or the communication or publication of information obtained from the use, of surveillance devices. The report provides draft legislation for the proposed regulation of the use of surveillance devices in Queensland (covering listening devices, optical surveillance devices, tracking device and data surveillance devices). The QLRC is currently undertaking a separate review of workplace surveillance laws.

The Law Society would support the adoption of many of the recommendations made in the QLRC's report, particularly in relation to the exceptions attached to the prohibitions against use of surveillance devices or disclosure of information obtained from use of those devices.

However, the QLRC's report proposes continuation of a notice and consent basis for surveillance laws. For reasons outlined above, the Law Society considers that notice and consent should be supplemented with, or replaced by, an additional requirement of demonstrated organisational accountability. Organisational accountability requires the creation of a legal obligation for an employer to ensure that workplace surveillance is reasonable, necessary, and proportionate.

[16] Queensland Law Reform Commission, "Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies", Report No 77, February 2020.

Harmonisation of surveillance device laws

We note the surveillance law provisions across Australian states and territories are inconsistent and consider this creates confusion for individuals. It also creates difficulties for businesses operating across jurisdictions, for example, in relation to telephone call recording.

The Australian Law Reform Commission has previously noted that the inconsistencies in the provisions between jurisdictions results in 'uncertainty and complexity, reducing privacy protection for individuals and increasing the compliance burdens for organisations'.[17]

The Law Society has previously supported a uniform approach to surveillance regulation to ensure consistency of protections across Australia.[18] We continue to support this position.

We therefore invite the Select Committee to consider the significant work undertaken by the QLRC, and to recommend a similar approach to surveillance device regulation in NSW, but supplemented with an additional legal obligation for an employer to ensure that workplace surveillance is reasonable, necessary, and proportionate.

Civil remedies framework

While the WSA creates various offences for the breach of relevant provisions of that Act, the Law Society is concerned about the practical difficulties of holding employers to account under the current framework.

The maximum penalty for an offence under the WSA is 50 penalty units (currently $5,500), with offences dealt with summarily. While these offences may serve as a deterrent from wrongdoing in some instances, we query whether they are operating as intended. The Law Society is not aware of any prosecutions made under the WSA to date and notes the difficulty, from an evidentiary and resourcing perspective, with prosecuting such minor offences.

In these circumstances, the Law Society considers that in addition to the criminal offences prescribed in the WSA, civil remedies should also be made available to individuals for breaches of employers' obligations under the WSA provisions. We would also support the inclusion of a civil remedies regime under the SDA to supplement the existing criminal offence regime.

We note that in its recent report, the QLRC recognised that 'a significant shortcoming of the current model of surveillance devices legislation in Queensland and the other jurisdictions is the reliance on criminal prohibitions alone'.[19] The QLRC recommended the adoption of a civil remedies regime for breaches of surveillance devices legislation in Queensland, noting 'civil remedies provide an additional safeguard for privacy by giving affected individuals an avenue for personal redress'.[20]

We note that the NSW Law Reform Commission (NSWLRC) has previously recommended that complaints about contraventions of surveillance devices legislation should be made to the NSW Privacy Commissioner for conciliation and, if unable to be resolved in that way, referred

[17] Australian Law Reform Commission, "Serious invasions of privacy in the digital era", 3 September 2014, 295-296, 276.
[18] Law Society of NSW, Submission No 122 to the Australian Law Reform Commission's Inquiry into Serious Invasions of Privacy in the Digital Era, dated 12 May 2014, 4.
[19] Queensland Law Reform Commission, "Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies", Report No 77, February 2020, 207.
[20] Queensland Law Reform Commission, "Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies", Report No 77, February 2020, 239.

to the (now) NSW Civil and Administrative Tribunal for decision.[21] The NSWLRC recommended that standing be given to a person affected by the conduct of the surveillance; and where the surveillance has taken place in the workplace, an industrial organisation on behalf of the employee(s) who have been affected by the conduct of surveillance.[22]

The NSWLRC noted that the benefits of providing access to conciliation in the first instance, and determination by a division of the (now) NCAT in the second instance, are several. The conciliation process is:

- readily accessible by complainants;
- relatively inexpensive;
- not intimidating; and
- can bring flexibility and informality to bear on the resolution of complaints.[23]

The NSWLRC further recommended that the NSW Privacy Commissioner be given the power to conduct inquiries and initiate investigations into surveillance-related matters, including breaches, or threatened breaches, of the relevant legislation.[24]

The Law Society supports the introduction of a civil remedies framework to supplement the existing criminal offence frameworks under both the specific workplace surveillance provisions under the WSA, and more generally, the SDA provisions. We consider this would provide a more appropriate framework for recognising the effect of infringements on individual privacy and for holding employers to account, particularly noting there is currently no statutory cause of action in NSW for serious invasions of privacy.

Independent oversight and monitoring

In addition to the adoption of a civil remedies framework, the Law Society supports enhanced oversight and monitoring mechanisms over both the workplace surveillance and general surveillance device regulation frameworks in NSW.

In its recent report, the QLRC recognised that the 'ubiquity and intrusive nature of surveillance device technologies, their potential to infringe and intrude upon individuals' privacy and the growing significance of these issues in people's lives require an appropriate regulatory response'.[25] The QLRC recommended the establishment of an independent regulatory body to 'help the community understand and give effect to their responsibilities and rights under the legislation'.[26] The QLRC recommended the independent regulator's primary functions should be to 'provide education and best practice guidance, and to monitor the operation of and compliance with the legislation and developments in surveillance devices technology, together with a complaints receiving, management and mediation function'.[27]

We note that in NSW, the office of the Surveillance Devices Commissioner has been established under the SDA. We understand the focus of that office is on holding law enforcement agencies to account over their application for, and use of, surveillance device warrants (for the use of covert surveillance). In the first instance, we suggest the Select

[21] New South Wales Law Reform Commission, Interim Report No 98 (2001), see recommendations 91 to 102, 105.
[22] New South Wales Law Reform Commission, Interim Report No 98 (2001), recommendation 92.
[23] New South Wales Law Reform Commission, Interim Report No 98 (2001), 425.
[24] Ibid.
[25] Queensland Law Reform Commission, "Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies", Report No 77, February 2020, 287.
[26] Ibid.
[27] Queensland Law Reform Commission, "Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies", Report No 77, February 2020, 293.

Committee consider the feasibility of expanding the NSW Surveillance Devices Commissioner's jurisdiction over applications for covert surveillance authorities under the WSA.

We further suggest that a broader oversight, complaints handling, guidance, and regulatory function, in line with the office of independent regulator recommended by the QLRC, should be conferred on an independent NSW office.

In our view, the NSW Privacy Commissioner would be best placed to receive additional regulatory and monitoring functions under both the WSA and SDA, as well as enhanced functions to issue education and guidance about the use of surveillance devices in the workplace context to help employers understand their obligations. In addition to experience and expertise in the area of privacy law and regulation, the NSW Information and Privacy Commission is established as an independent statutory authority. In contrast, the NSW Surveillance Devices Commissioner is a public service employee appointed by the Secretary of the Department of Communities and Justice.[28]

Focus on, and guidance as to, risk assessment, mitigation, and management of residual privacy risk is already a core function of the NSW Privacy Commissioner. We consider the Commissioner's work in relation to privacy management plans and privacy impact assessments can readily be adapted and applied to surveillance activities, as has already been demonstrated by the NSW Privacy Commissioner's work in relation to use of CCTV by local government authorities.

Subject to the introduction of a civil remedies framework, we would also support the Privacy Commissioner taking on a complaints handling function to address possible infringements of surveillance laws (in line with the approach the NSWLRC has previously recommended). We consider the Privacy Commissioner should also be given the power to conduct inquiries and initiate investigations of their own accord.

We note that the NSW Privacy Commissioner would require substantial additional funding to be able to properly discharge these important additional functions.

Thank you again for the opportunity to contribute to this consultation. Should you require any further information, please contact Adi Prigan, policy lawyer on 9926 0285 or adi.prigan@lawsociety.com.au.

Yours sincerely,

Richard Harvey
President

[28] *Surveillance Devices Act 2007* s 51A.