Surveillance of workplace communications: What are the rules?

Peter Leonard GILBERT + TOBIN

Workplace monitoring and surveillance is becoming increasingly common. Take-up is stimulated by decline in the cost of pervasive surveillance across multiple communications modes and devices and increasing convenience of “out of the box” technological solutions for employers.

The ability to undertake surveillance of employee communications is often a significant benefit to employers. In addition to maintaining records of business transactions and client or customer relationships, surveillance of employee emails can assist employers in monitoring the performance of its workforce; in detecting and investigating any employee misconduct (such as, fraud, sexual harassment, theft of confidential information and diversion of business opportunities) and ensuring the safety of employees. However, in order to avoid liability or criminal sanctions, employers engaging in surveillance of workplace communications need to know the legal restrictions and prohibitions which relevantly apply.

Workplace monitoring has also been complicated by increasing prevalence in the workplace of personal devices such as smartphones, working from home and “bring your own device” (BYOD) policies. These changes bring their own challenges and risks for employers.

The new mobile and remote workplace

Personal and home devices used for work purposes may have a higher probability of being infected with viruses or other bad software, because the owner of the device may be more likely to share it with others, and to visit the kinds of websites and receive the kinds of emails that interaction with which can more likely lead to infection. An infection of a personal device, if the device connects to corporate systems, is a threat to corporate data and systems. A personal device may not have updated patches and fixes applied as rapidly as company-owned devices, unless there is a BYOD policy that requires the personal device to be loaded with company software and connected to the corporate network in such a way that patches, and such, get applied.

A personal device that is used to record corporate information may be inadequately partitioned on the device itself to separate the company information from the individual’s personal information. It then becomes significantly harder to access easily the company-owned information if there were a need to do so, for example, in the context of litigation or investigation.

From a security perspective, it makes it harder to appropriately secure the company information if it is intermingled with personal files. A personal device may more easily get lost or stolen, just by the nature of how it may be used (and shared). A personal device may not have the type of encryption or authentication measures that a company-owned device has. Employees may be reluctant to agree to the implementation of a remote-wipe function in the event of a lost or stolen device. A personal device may not support the same monitoring and logging capabilities that company-owned devices have in place, unless the company policy requires the personal device to be loaded with company software and connected to the corporate network in such a way that supports such monitoring and logging.

Monitoring and logging of personal devices may capture additional personal information, for example geo-location information, that may not be expected by users of personal devices.

Workplace monitoring and surveillance is also complicated by a patchwork of national laws. Australia does not have uniform laws governing surveillance in the workplace by private sector employers. As a consequence, the rules which apply to email surveillance in the workplace depend upon the Australian state or territory in which the employer is operating.

A patchwork of national laws

Australia does not have uniform laws governing the surveillance of employees by private sector employers. Consequently, the rules that apply to workplace surveillance depend upon the Australian state or territory in which the employer is operating. Currently only two jurisdictions in Australia (New South Wales and the Australian Capital Territory) have specific legislation regulating surveillance of electronic communications by
employers. These laws apply to surveillance of employees, volunteers and contractors undertaken by a company and its related corporations. In these jurisdictions, employers must conduct surveillance in accordance with a company policy and subject to the statutorily prescribed notification requirements.

Various federal, state and territory laws regulate unauthorised access to computer systems or data on computer systems that is protected by some form of access control. Although the laws take a variety of forms and need to be considered on an individual basis, in general access control technologies may only be bypassed by agreement with the controller of a computer system. In practice, this makes it prudent, if not mandatory, for employers to publish and implement a company surveillance policy that makes it clear that as a condition of provision of internet access to employees the employer is conferred the right to conduct reasonable computer surveillance.

Workplace surveillance in most Australian jurisdictions is regulated by general surveillance statutes which prohibit the use of listening, optical or tracking devices except in specified circumstances, but which do not expressly apply to email monitoring.

The rules applicable in each jurisdiction are summarised below.

There is currently no political momentum which is likely to see the advent of a national approach to regulation of workplace surveillance in the near future. However, it is expected that the final report of the Australian Law Reform Commission (ALRC) in response to the former Federal Government’s reference on the elements of a statutory cause of action for serious invasions of privacy in the digital age will repeat recommendations in the draft report for a national coordinated approach to electronic surveillance laws. As noted in that ALRC Inquiry’s Discussion Paper:

These surveillance device and workplace surveillance laws contain a number of significant inconsistencies across jurisdictions. These inconsistencies fall broadly into three categories. There are inconsistencies with respect to: the type of the devices regulated; the nature of the offences; and the nature of the defences and exceptions. Consistency and uniformity in the surveillance device laws and workplace surveillance laws is desirable. Inconsistency means that privacy protections vary depending on which state or territory a person is located in. It also makes it more difficult for a person who finds themselves under surveillance to determine their legal position. Inconsistency also means that organisations with legitimate uses for surveillance devices face increased uncertainty and regulatory burden.

The ALRC continued:

Establishing uniform workplace surveillance laws in each of the states and territories would provide greater privacy protections for employees and greater certainty for employers operating in multiple jurisdictions. These laws could be contained in specific workplace surveillance laws, as they are in the ACT and NSW, or integrated into the more general surveillance device laws, as they are in Victoria.

That ALRC Inquiry, led by Commissioner Professor Barbara McDonald, reported in June 2014 to the Federal Attorney-General. Release of the final report and the Federal Government’s response is pending.

In addition, general privacy laws, and in particular the Privacy Act 1988 (Cth) and communications interception laws may also be relevant to employers when conducting workplace electronic surveillance. However, the limited application of these laws to electronic surveillance generally presents limited obstacles for employers when conducting reasonable surveillance.

New South Wales and the Australian Capital Territory are the only jurisdictions which specifically regulate the monitoring of workplace email and computer usage.

New South Wales

General

The Workplace Surveillance Act 2005 (NSW) (NSW Act) restricts the circumstances in which an employer may lawfully engage in “surveillance” of its employees. An “employee” includes a person employed by the employer and its related corporations. However, the employer’s obligations under the NSW Act also apply in respect of employees of an unrelated third party who perform work for the employer, such as the employees of a labour hire company and volunteers.

The NSW Act applies when the employees under surveillance are “at work”, irrespective of whether they are at their employer’s premises or any other place (including if they are working from home). The legislation makes clear that an employee is “at work” whether or not the employee is actually performing work at the time and regardless of working hours. This means that an employer may (subject to compliance with the notice requirements) carry out surveillance of communications sent or received using the employer’s information technology resources and systems, including emails sent or received outside business hours or using a private email account such as Hotmail, and potentially also including an employee’s own devices, such as “bring your own” smartphones or tablets.

The NSW Act also contains provisions dealing with blocking delivery of communications sent to or by an employee, internet access by employee and the use of records made of such surveillance, other than in accordance with the Act. It is arguable that an employer’s obligations apply regardless of whether the surveillance takes place in New South Wales, provided that the employees who are under surveillance are located within the jurisdiction.
Overt surveillance

“Computer surveillance” means “surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites)”.

With the exception of covert surveillance, computer surveillance by employers of employees in New South Wales is prohibited unless the employee has been given 14 days prior written notice by her/his employer (or a lesser period by agreement) and the surveillance is conducted in accordance with the employer’s policy for computer surveillance. The written notice to the employee must specify:

- the kind of surveillance to be carried out, in this case computer surveillance;
- how the surveillance will be carried out;
- when the surveillance will start;
- whether the surveillance will be continuous or intermittent; and
- whether the surveillance will be for a specified limited period or ongoing. The employee must also be notified of the employer’s computer surveillance policy in such a way that it is reasonable to assume that the employee is aware of and understands the policy.

Surveillance relevantly includes “tracking surveillance”, which is surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement (such as a global positioning system tracking device).

The Act also imposes a general prohibition on the blocking of emails or internet access by an employer unless:

- the employer is acting in accordance with a policy on email and internet access that has been notified in advance to the employee in such a way that it is reasonable to assume that the employee is aware of and understands the policy; and
- in addition, in the case of blocking emails, the employee is given notice as soon as practicable by the employer, by email or otherwise, that the delivery of the email has been prevented, unless the email or attachment is spam, would interfere or damage the operation of the computer network, program or data, or the would be regarded by reasonable persons as being, in all the circumstances, menacing, harassing or offensive.

The policy must not permit blocking of communications or access to an internet website merely because the communication was sent by or on behalf of a union, or the website or email contains information relating industrial matters.

Covert surveillance

Where an employer suspects that one or more of its employees are engaged in unlawful activity, it may apply to a magistrate for an authority authorising covert surveillance of its employees. Covert surveillance occurs where the employer does not comply with the notification requirements set out above. The application must include, among other things:

- the grounds for the employee’s suspicion;
- the names of the employees who will be the subject of the surveillance;
- the kind of surveillance; and
- the dates on which it will be undertaken.

The application will not be granted unless the magistrate is satisfied that there are reasonable grounds to justify the issue of the authority, having regard to the seriousness of the unlawful activity with which the application is concerned. Where an authority is granted, the surveillance must be confined to surveillance for the purpose of establishing whether or not the employees are involved in an unlawful activity and cannot be used for monitoring an employee’s work performance. Penalties of up to $5500 apply where an employer conducts covert surveillance of an employee at work without first obtaining a covert surveillance authority. A corporation’s directors who knowingly authorise or permit a contravention may also be prosecuted.

Australian Capital Territory

In 2011, the Australian Capital Territory enacted the Workplace Privacy Act 2011 (ACT) (ACT Act) which regulates the collection and use of workplace surveillance information and the surveillance of workers. “Workers” includes employees, independent contractors, outworkers, persons doing work experience and volunteers. A workplace is any place where work is, has been or is to be carried out for someone conducting a business or undertaking.

While using slightly different terminology, the ACT Act establishes a regulatory framework for employee email surveillance which is almost identical to that of the NSW Act. “Surveillance” is defined to include
surveillance using a “data surveillance device” being “a device or program capable of being used to record or monitor the input of information into or the output of information from a computer”. 9

**Overt surveillance**

Like the NSW Act, the ACT Act prohibits surveillance of workers in the workplace except where the employer has given the worker written notice and, in the case of “data surveillance”, the surveillance is in accordance with an applicable employer policy. However, unlike the NSW Act, the ACT Act prescribes the form of the policy, which must state:

- how the employer’s computer resources may, and must not, be used;
- what information about the use of the employer’s computer resources is logged and who may access the logged information; and
- how the employer may monitor and audit a worker’s compliance with the policy.

An employer who conducts surveillance of a worker’s emails otherwise than in accordance with these requirements commits an offence under the ACT Act, and will be liable in respect of each infringement for a fine of up to $2200 for an individual or $11,000 for a corporation.

**Covert surveillance**

The ACT Act also provides for the authorisation and regulation of covert surveillance of workers in similar terms to the NSW Act.

**Other Australian jurisdictions**

None of the other states or the Northern Territory has followed New South Wales’ lead of specifically regulating surveillance of employee communications. Victoria is the only other jurisdiction which has legislation dealing specifically with workplace surveillance (but not surveillance) of electronic communications, by amendments to the Surveillance Devices Act 1999 (Vic) (Victorian Act) made by the Surveillance Devices (Workplace Privacy) Act 2006 (Vic). Section 9B of the Victorian Act provides an offence for the use of an optical device or listening device to carry out surveillance of the conversations or activities of workers in workplace toilets, washrooms, change rooms or lactation rooms. Workplace surveillance in Victoria is otherwise subject to the same restrictions as general surveillance devices. A 2004 Bill before the South Australian parliament (the Workplace Privacy Bill 2004 (SA)) by the Hon Ian Gilfillan MLC to regulate the monitoring, interception, storage or retrieval of email messages, was never enacted.

Western Australia (Surveillance Devices Act 1998 (WA)), South Australia (Listening and Surveillance Devices Act 1972 (SA)), Tasmania (Listening Devices Act 1991 (Tas)) and the Northern Territory (Surveillance Devices Act 2000 (NT)) all have more conventional listening devices statutes which at a minimum regulate the monitoring or recording of conversations. Western Australia, South Australia and the Northern Territory also regulate visual and tracking (or location) surveillance. The Northern Territory legislation regulates data surveillance (which encompasses surveillance of electronic communications) by law enforcement agencies, but it does not apply to data surveillance by private sector employers.

**Communication interception laws**

An employer will commit an offence under the Telecommunications (Interception and Access) Act 1979 (Cth) if it intercepts or permits another person to intercept (among other matters) to intercept a communication “passing over a telecommunications system” “without the knowledge of the person making the communication”. 10

This restriction has consistently been interpreted as applying only to the content of a communication, not information about the communication (such as, called number or email addressee, duration or other metadata). The requirement of “knowledge of the person making the communication” may be critical in the case of incoming emails, SMS or other two-way communications where the person making the communication may be a person who has not been put on notice as to the interception, where a workplace surveillance policy is disseminated in the workplace but not made known to persons dealing with that workplace. This is why phone callers to financial institutions are informed that their communication with the institution’s employees may be monitored, for instance “for security, quality assurance or training purposes”. The question of when a communication is taken to be passing over is the critical one for any liability under the legislation. Section 5F defines a communication as passing over a system when it is:

- sent or transmitted by the person sending the communication; and
- taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.

This clearly prohibits an employer from monitoring the content of an electronic communication while it is in transit from the sender to the recipient. However, the temporal nature of when interception may not occur
provides limited protection for employees as surveillance will not breach the Telecommunications (Interception and Access) Act once a communication has come to rest and becomes a stored communication, unless the prohibition (in s 108) upon “access to stored communications” in that Act applies. In general, that prohibition only applies where the access is to a stored communication that is stored on equipment that is operated by, and in the possession of, a carrier or a carriage service provider within the meaning of the Telecommunications Act 1997.11 Accordingly, most employer owned or operated communications databases will not be within this prohibition. Where the prohibition does apply — as it may to some telecommunications service provider cloud based offerings — the prohibition will not operate where the access is with the knowledge of either the intended recipient of the communication or the sender of the communication.

An employer will prudently notify its employees of any surveillance of electronic communications to avoid any risk that its surveillance may breach this legislation, even in those Australian jurisdictions where a company policy is not required under specific workplace surveillance legislation.

Various Commonwealth, state and territory laws regulate unauthorised access to computer systems or data on computer systems that is protected by password or other form of access control. Particular caution needs to be exercised in relation to app, browser or cookie based data analytics technologies which might be said to permit of facilitate unauthorised access to any device or data on any device that is protected by password or other form of access control technologies. This is particularly the case where the device is an employee owned device such as a “bring your own” smartphone or a home computer. Although the laws take a variety of forms and need to be considered on an individual basis, in general access control technologies may only be bypassed by agreement with the controller of a computer system. Accordingly, there needs to be clarity as to who is that controller and agreement by that controller to the relevant access.

Privacy legislation

The Australian Privacy Principles (APPs), set out in the Privacy Act 1988 (Cth) (Privacy Act), regulate the collection, use and storage (among other things) of personal information. However, the Privacy Act includes a broad exemption for the handling of employee records by an employer. The exemption in practice has limited application because of numerous exceptions and in particular because the exception does not allow collection and handling of personal emails or the personal information of non-employees such as contractors or volunteers. Accordingly, employers must comply with the notification requirements in the Privacy Act (APP 5 in particular) and ideally, obtain the consent of employees/contractors to the collection and handling of this information through prominent publication of the electronic communications policy.

The “employee records exemption” applies to an act or practice of an organisation which is directly related to:

- a current or former employment relationship between the organisation and its employee; and
- an employee record held by the organisation and relating to the employee.

An email which contains an employee’s personal information and relates to the employee’s employment meets the definition of an employee record. “Employee record” is broadly defined and arguably covers many matters of interest to an employer when conducting email surveillance, so as to exclude such emails that relate to the employee’s employment from any protection under the legislation. The examples of an employee record in the Privacy Act include records as to terms and conditions of employment, disciplining of the employee, leave entitlements, and union membership. However, the ever present risk is that surveillance will capture communications which do not meet the definition of an employee record.

Practical implications for employers

In practical terms, an employer’s Acceptable Use Policy should seek to achieve the following:

- Explaining the purposes for which any monitoring is conducted, the extent of the monitoring and the means used.
- Informing employees of the extent to which information about their internet access and emails and other communications is retained in the system and for how long.
- Setting out clearly the circumstances in which employees may or may not use the employer’s communications systems, including telephone systems (and mobile phones) and internet access for private communications.
- Making clear the extent and type of private use that is allowed.
- In the case of internet access, specifying clearly any restrictions on material that can be viewed or copied.
- Advising employees about the general need to exercise care, about any relevant rules, and about what personal information they are allowed to include in particular types of communication.
• Laying down clear rules for private use of the employer’s communication equipment when used from home or away from the workplace (for example, the use of facilities that enable external dialling into company networks).
• Outlining how the policy is enforced and penalties which exist for a breach of policy.

As already noted, national private sector employers currently face a disjointed approach to Australian regulation of surveillance of electronic communications. The comprehensive approach to regulation in New South Wales and the Australian Capital Territory has not been followed in other jurisdictions. Employers operating in various jurisdictions are able to take a different approach to informing employees about email surveillance. The cumulative practical outcome of the statutory requirements described above is that a private sector employer seeking to apply a consistent national approach should publish an Acceptable Use Policy and provide that policy to employees at least 14 days prior notice of the surveillance occurring (unless a lesser period of notice is agreed).

At a minimum, the Acceptable Use Policy must address the following matters:
• the kind of surveillance to be carried out, in this case, computer and telephone surveillance (including whether surveillance of emails in transit will occur);
• how the surveillance will be carried out;
• when the surveillance will start;
• whether the surveillance will be continuous or intermittent; and
• whether the surveillance will be for a specified limited period or ongoing.

To ensure compliance with the notification requirements in the Privacy Act (APP 5), the employer must also provide notice of the following in the Acceptable Use Policy:
• The employer collects and stores the content of communications (other than listening to voice communications, except of course where this is the case — and in that case express consent of employees and active steps to inform call counterparties are also prudent), including personal emails, and other data for the purpose of ensuring compliance with, for example, relevant company policies and laws.
• The main consequences (if any) for the individual if all or some of the personal information is not collected by the employer.
• Any other entity or person, or the types of entities or persons to which the employer usually discloses the information collected.
• That the privacy policy of the employer contains information about how an individual may access and correct the personal information the employer holds about that individual (at least in relation to the information that falls outside the scope of the employee records exemption, such as, personal emails).
• The privacy policy of the employer contains information about how an individual may complain about a breach of the APPs in relation to his/her personal information.
• Whether the employer is likely to disclose the personal information to persons or entities outside Australia, including to related entities, and, if so, the location in which those recipients are located.
• The circumstances in which communications may be stopped or otherwise captured or reviewed. For example, that communications may be blocked if they are suspected to be unsolicited electronic commercial messages (that is, spam) within the meaning of the Spam Act 2003 (Cth) or would or might have resulted in unauthorised interference with, damage to or operation of a computer or computer network operated by the employer or any program run by or data stored on a computer or computer network.
• Where optical monitoring devices are deployed, that these devices may be used at all access points and sensitive areas (but noting restrictions as to use in personal spaces such as bathrooms and washrooms). In addition, to comply with the NSW Act if cameras or other optical monitoring devices are used for surveillance, they must be clearly visible in the place where the surveillance is taking place and there must be clearly visible signs posted at the entrance to the workplace notifying people that they may be under surveillance at that place.

Peter Leonard
Partner
Gilbert + Tobin
PLEonard@gtlaw.com.au

Footnotes
1. The author acknowledges the assistance of his colleagues Di Banks, Kim McGuren and James Pomeroy with an earlier version of this article.
3. For example, the Surveillance Devices Act 1998 (WA); Surveillance Devices Act 2007 (NSW); Invasion of Privacy Act 1971 (Qld); Listening and Surveillance Devices Act 1972 (SA); Listening Devices Act 1991 (Tas); Surveillance Devices Act 1999 (Vic); Surveillance Devices Act 1998 (WA); Listening Devices Act 1992 (ACT); and Surveillance Devices Act 2000 (NT).
5. Above n 4, at [13.9] and [13.10].
6. Above, n 4, at [13.52].
7. See Workplace Surveillance Act 2005 (NSW), s 3.
8. Above, n 7, s 10.
9. Workplace Privacy Act 2011 (ACT), s 8. As to surveillance other than by “devices”, such as data surveillance by software installed on a person’s computer, see *R v Gittany (No 5)* [2014] NSWSC 49; BC201400465 (11 February 2014). See also, Surveillance Devices Act 2007 (NSW) s 4(1) (definition of “tracking device”), and Surveillance Devices Act 2007 (NSW) s 4(1) (definition of “tracking device”).
10. Telecommunications (Interception and Access) Act 1979 (Cth), s 7(1).
11. Paragraph (b) of the definition of “stored communication” in s 5 of the Act.