Eye Spy to Spyware: Working Within the Confines of the NSW Surveillance Devices Act 2007

The New South Wales Surveillance Devices Act 2007 significantly expands the regulation of overt and covert surveillance in New South Wales. Sophie Dawson and Helen Gill take a look.

The New South Wales *Surveillance Devices Act 2007* (the **Act**) received assent from the Governor-General on 23 November 2007 and replaces the *Listening Devices Act 1984* (NSW). It is set to commence on a date to be appointed by proclamation, tentatively set for July 2008, and will apply in conjunction with other New South Wales State and Federal legislation that regulate surveillance devices, including the *Workplace Surveillance Act 2005* (NSW) and the *Telecommunications (Interception) Act 1979* (Cth).

Compared to its predecessor, the Act is broader both in application and effect. In addition to regulating listening devices, its operation extends to optical surveillance, tracking and data surveillance devices.

Listening Devices

Subject to exceptions, the Act prohibits the installation, use or maintenance of a 'listening device' where the device is intended to be used to monitor, record or listen to a private conversation while it is taking place. The prohibition applies regardless of whether the person using the device is a party to the conversation.

'Listening device' is defined broadly under the Act to mean 'any device capable of being used to overhear, record, monitor or listen to a conversation or words being spoken',[1] and is likely to include tape recorders, recording functions on mobile telephones and answering machines, intercoms, baby monitors, parabolic microphones, electronic stethoscopes and telephone wire taps. Hearing aids and similar devices used by persons with impaired hearing to overcome the disability are specifically excluded from the definition.[2] This is consistent with the position under the *Listening Devices Act 1984* (NSW).

Consent and 'lawful interests' exceptions

Two of the exceptions provided under the Act may be of assistance to media organisations. They arise where a party to a private conversation (a person by or to whom words are spoken during the course of the conversation or a person who records or listens to those words with the consent, express or implied, of such a person), uses a listening device to record, monitor or listen to a private conversation and:

- the express or implied consent of all principal parties to the conversation, being persons by or to whom words are spoken during the course of that conversation, is obtained in relation to use of the listening device(s); or
- the consent of one principal party is obtained to use of the listening device(s); and
  - as a matter of objective judgment,[3] the recording of the conversation is reasonably necessary in order to protect the 'lawful interests' of that principal party, being actual 'lawful interests' that are in existence at the time of use of the listening device;[4] or
  - the recording is not made for the purpose of communicating or publishing the conversation (or a report of it) to persons who were not parties to the conversation.

The 'lawful interests' exception is an important one. Over the years a plethora of case law has developed to assist in determining what is encompassed by this phrase, which is not defined in the Act, and was not defined in the *Listening Devices Act 1984* (NSW). The decisions in *R v Zubrecky*,[5] *Violi v Berrivale*[6] and *R v Le*[7] have established that 'lawful interests', synonymous with 'legitimate interests' or 'interests conforming to law' are much broader in scope than mere 'legal interests' in the sense of legal rights, titles, duties or liabilities. The recording of a conversation by a principal party so as to protect him or her from malicious allegations of fabrication as regards the true content of the conversation[8] or the exact terms of an oral contract, where the said terms were outlined during the conversation,[9] have, for example, been found to fall within the scope of 'lawful interests' in particular circumstances. Similarly, the audio-visual recording of one parent's access visits to his or her child for the purpose of protection against allegations of misconduct or impropriety was considered to be a protected 'lawful interest' in a particular case.[10]

However, as noted by Adams J in *R v Le*, this does not mean that:

> the mere intention of making an irrefutable record of a conversation to which one is a party will, without more, satisfy the defence: the circumstances in which the recording occurs will always be relevant to the determination of whether there is, indeed, a 'reasonable necessity' for doing so.[11]

For example, the covert recording of a 'without prejudice' private conversation by a party to that conversation 'for her own private use to assist her comprehension and to give herself an opportunity to revisit what had taken place',[12] while in her lawful interests, has not been found to be reasonably necessary where the interests of that party could have been protected in other ways and without concealment, such as through the taking of handwritten notes.[13]

The 'lawful interests' exception has proved useful in a media context as regards the act of recording; however it does not, of itself, permit publication. In *Channel Seven Perth Pty Ltd v 'S' (A Company)*,[14] for example, Le Miere J found it to be reasonably necessary in the circumstances for 'M', a casual employee of 'S', to protect her 'lawful interests' by using a hidden listening device, at the behest of Channel Seven Perth Pty Ltd, to covertly record a 'private conversation' between herself and the general manager of 'S', in which it was explained that she was to be 'let go' because her pregnancy posed an 'occupational health and safety risk'. Le Miere J explained that while the video did not 'record' unlawful conduct, it 'is or may be evidence from which it may be inferred that the company acted unlawfully'[15] by discriminating against 'M' on the grounds of her pregnancy. However, while Le Miere J found the recording to be lawful, he ultimately refused Channel Seven Perth Pty Ltd's application[16] for an order allowing *publication* of the record of private conversation as, having weighed the competing

interests, he was not satisfied that the publication would further or protect the public interest (the test in Western Australia).

On appeal to the Supreme Court of Western Australia, McLure JA (with whom Pullin and Buss JJA agreed) held that Le Miere J had erred in going outside the scope and purpose of the Act in weighing up the competing interests and considering the public interest in protecting the privacy of the general manager's conversation, and the likely damage to the general manager and 'S' by publication of the interview.

The Supreme Court of Western Australia set aside Le Miere J's decision and determined the matter afresh, finding that as the recording did not record unlawful conduct and Channel Seven Perth Pty Ltd could broadcast the story without the covertly recorded interview, 'the evidence falls well short of providing a proper foundation for a conclusion that the proposed publication should be made to protect or further the public interest.'[17] The appeal was dismissed, as was Channel Seven Perth Pty Ltd's further appeal to the High Court of Australia.[18]

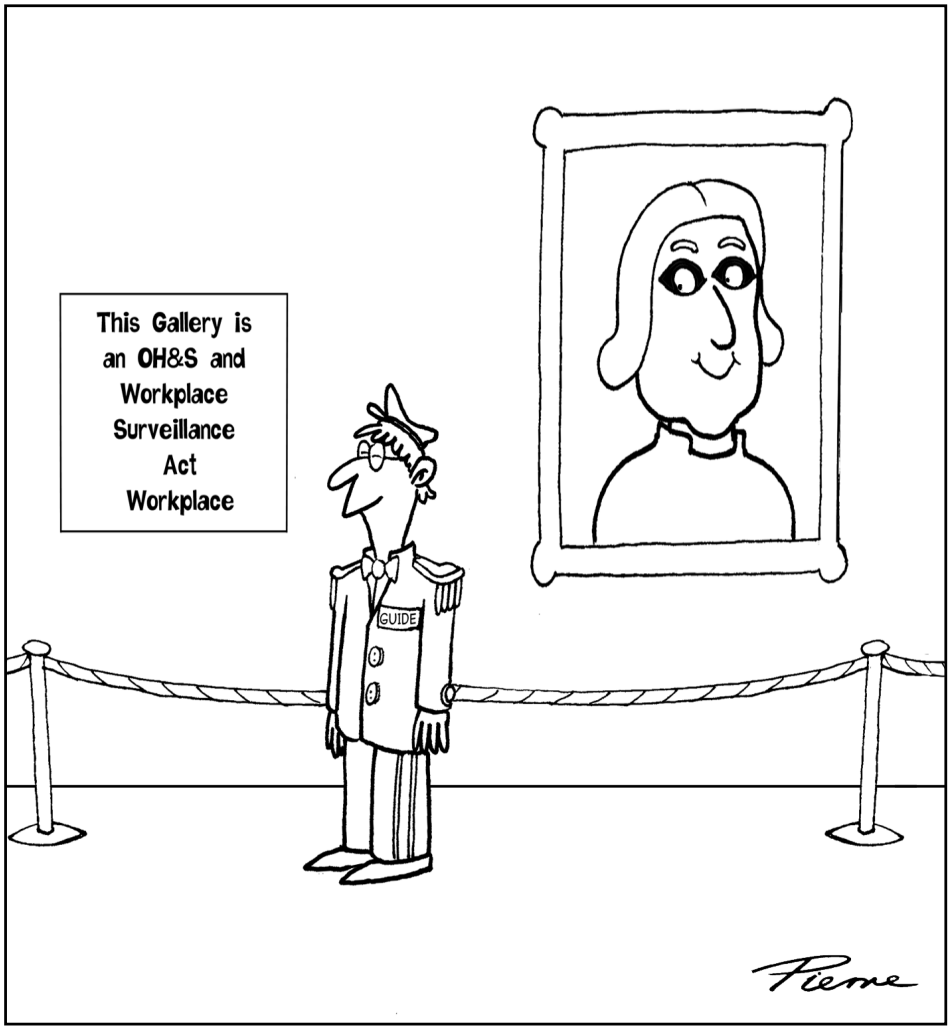
While there is no equivalent to section 31 in the NSW Act, publication by the media of a record of private conversation made by a listening device will generally only be permitted with the express or implied consent of all principal parties to the private conversation.

The practical effect of the Act for journalists, private investigators, parents and other individuals who wish to use a listening device to listen to, record or monitor a private conversation to which they are not a party, is substantially the same as under the *Listening Devices Act*. That is, unless the consent of one or more principal parties to the conversation is obtained or the 'lawful interests' exception applies, then use of a listening device to record a private conversation will constitute an indictable offence. Under the Act, the maximum penalty is two years imprisonment and/or an $11,000 fine for an individual, and a $22,000 fine in respect of a body corporate.

Further, recordings or reports of 'private conversations' recorded in contravention of the Act may be inadmissible in evidence in civil or criminal proceedings by virtue of section 138 of the *Evidence Act 1995* (NSW). This is an important consideration for journalists, since this could make recordings of no use as a defence in defamation proceedings.

Optical Surveillance Devices

The Act also prohibits the installation, use or maintenance of optical surveillance devices on or within premises, a vehicle, or any other object for the purpose of observing or recording the carrying on of an activity, where the installation, use or maintenance involves entry onto premises or entry into or interference[19] with a vehicle or object without the express or implied consent of the owner or occupier of the premises or the individual having lawful possession or control of the vehicle or object.



'Optical surveillance device' is defined broadly in the Act to mean 'any device capable of being used to record visually or observe an activity',[20] and is likely to include binoculars, telescopes, cameras, video cameras, security cameras, closed-circuit television (CCTV) and webcams. However, glasses, monocles, contact lenses and similar devices used by persons with impaired sight to overcome the disability are specifically excluded from the definition.[21]

Through limiting the application of the prohibition to activities that involve a non-consensual entry onto premises or into vehicles or interference with objects, the Act effectively constrains but does not prevent the use of optical surveillance devices for the purpose of investigative journalism. Nor does it stop private investigators from surveying and recording the movements of their quarry, provided that they work within the limitations of the Act.

Cases concerning the law of trespass will be very important in understanding when use of a camera is likely to be lawful under the Act. In *TCN Channel Nine Pty Ltd v Anning*,[22] for example, a television news crew entered a residential property with the intention of filming a police raid on the premises and conducting interviews with a view to broadcasting. At first instance, District Court Judge English found that TCN Channel Nine Pty Ltd, by its servants and agents, did not have any express or implied licence to enter and remain on the property to film. Thus, in so doing, it had committed the tort of trespass to land and caused the occupier (Anning) personal injury including mental trauma. The occupier was awarded damages in the amount of $100,000 (being general, aggravated and exemplary damages) plus interest. On appeal, the New South Wales Court of Appeal (Spigelman CJ, Mason P and Grove J) unanimously upheld the decision of English DCJ as regards the finding of trespass to land, but allowed the appeal insofar as exemplary damages and damages for mental trauma were awarded, and the interest calculated. Ultimately Anning was awarded damages in the amount of $50,000 (being general and aggravated damages) plus interest.

While the courts do recognise an implied licence to enter a property to approach the

occupier to request permission to film,[23] an implied licence was not found to exist in *TCN Channel Nine Pty Ltd v Anning*. This was because the Court found that TCN Channel Nine Pty Ltd, by its servants and agents, had entered the property with the intention of filming the police raid as distinct from requesting permission to film.

The use of non-malicious Trojan horse programs creates an interesting scenario. These are programs that are typically installed to manage systems, detect suspicious data, deploy and patch software, and conduct surveillance and forensics. They may be installed directly, remotely via an email attachment, or through exploiting common operating system vulnerabilities and bypassing security measures.

The question arises as to whether the covert use of a non-malicious Trojan horse program, installed remotely via an email attachment or by exploitation of common operating system vulnerabilities, that intercepts or even initiates a webcam feed, will constitute a breach of the Act.

While it is arguable that such an activity would constitute interference with a computer (an object) and that it would contravene the Act on that basis, the position is not free from doubt. There are, of course, also other laws which would need to be taken into account in relation to any such activity, including any right of action for breach of privacy,[24] Federal, State and Territory computer crimes legislation (where relevant) and, depending on the person using the software in question, workplace surveillance and/or privacy legislation.

Such activities, if carried out with an intention to commit an indictable offence, would be likely to contravene section 308C of the *Crimes Act 1900* (NSW).

Tracking Devices

The Act prohibits installation, use or maintenance of a 'tracking device' for the purpose of ascertaining the geographical location of a person or object without the express or implied consent of that person or the person having lawful possession or control of the object, unless it is for a lawful purpose.

The breadth of the definition of 'tracking device' provided in the Act, and the fact that it includes 'any electronic device *capable* of being used'[25] for such a purpose, means that it is likely to include such devices as global positioning system chips found in vehicles and mobile telephones, as well as terrestrial-based automatic vehicle location systems (such as LoJack and LORAN) and other devices capable of determining the geographical location of a person or object.

The phrase 'lawful purpose' is not defined in the Act. However in *Taikato v R*[26], it was determined that 'lawful purpose' is not synonymous with 'lawful authority', but is a purpose that is authorised in a positive rule of law 'as opposed to not forbidden by law.'[27] Similarly, *The Macquarie Dictionary*, the dictionary of reference for Australian courts, defines 'lawful' to mean 'allowed or permitted by law', 'legally … entitled' and 'recognised or sanctioned by law'.[28]

In determining the practical effect of this prohibition, consideration must be given to section 275A of the *Telecommunications Act 1997* (Cth). Section 275A deems information about the location of a mobile telephone handset or other mobile communications device to be information relating to the affairs of the customer responsible for the handset or device. Section 276 of that Act prohibits use and disclosure of such information by carriers, carriage service providers and telecommunications contractors, subject to exceptions. The key exception, in section 289, is where the person to whom the information relates consents to the use or disclosure, or is reasonably likely to be aware that information is used or disclosed in the circumstances in question.

Data Surveillance

The final prohibition in the Act concerns the installation, use or maintenance of a data surveillance device(s) for the purpose of recording or monitoring the input and/or output of information from a computer where such an act entails the entry onto premises or interference[29] with a computer or network in the absence of the express or implied consent of the owner or occupier of the premises or the individual having lawful possession or control of the computer or computer network.

'Data surveillance device' is defined broadly in the Act to mean 'any device or program capable of being used to record or monitor the input of information into or output of information from a computer'[30] other than an optical surveillance device. 'Computer' is also defined broadly to mean 'any electronic device for storing, processing or transferring information',[31] and is likely to include Blackberrys, Blackjacks, Palm Pilots and similar hand-held devices.

As the prohibition is limited to acts that entail entry onto premises or interference with a computer or computer network without consent, employers retain the capacity under the Act to utilise non-malicious Trojan horse programs, such as Microsoft's soon to be patented Anti-slacking software, to overtly monitor internet usage, employee productivity, competence and physical well-being,[32] and to log keystrokes. Such surveillance is also regulated by the *Workplace Surveillance Act 2005* (NSW), and employers must comply with notice requirements regarding such surveillance.

The question arises as to whether non-malicious Trojan horse programs that are used to covertly spy on a computer user, log keystrokes to steal information such as passwords and credit card numbers, and report data by sending it to a fixed email or IP address, would involve 'interference' with a computer or network given that it would not interfere with or delay normal computer operations. A recent example of such a program, according to media reports, is the specially crafted Excel file that, if downloaded from an email attachment by an individual with a pre-2007 version of Microsoft Excel, permits the sender to obtain access to the target computer for malicious purposes.[33]

The question of what constitutes 'interference with a computer or computer network' was considered in *The Queen v Steven George Hourmouzis*[34] in which the defendant pleaded guilty to interfering with, interrupting or obstructing the lawful use of a computer contrary to section 76E of the *Crimes Act 1914* (Cth). Mr Hourmouzis had sent more than three million spam email messages to addresses in Australia and overseas fraudulently extolling a predicted 'plus 900 per cent rise in Rentech stock over the next few months', that were relayed through third party servers to minimise the risk of detection. The utilisation of these servers, while not causing any physical damage, did require the servers to be shut down and time to be lost so that the offending messages could be cleared. Further, the trading of Rentech shares on the NASDAQ had to be halted pending an announcement by the company, financial and personal resources had to be expended to investigate the spam problem, anti-spam defences had to be implemented and complaints dealt with, and certain internet addresses had to be blocked for a period, all of which affected the ability of those businesses to communicate.

Such repercussions would likely constitute interference with a computer or computer network under the Act. They may also contravene section 308C of the *Crimes Act 1900* (NSW) (referred to above) if there is the requisite intention to commit, or facilitate the commission of, a serious indictable offence within the jurisdiction of New South Wales.

Prohibition on Disclosure and Possession of Records and Recordings

The Act prohibits natural persons and bodies corporate from publishing or communicating to any person, any record, recording or information that has come to their knowledge as a direct or indirect result of the use of a surveillance device in contra-

vention of Part 2 of the Act,[35] *unless* the publication or communication is made:

- to a party to the private conversation or activity;
- with the express or implied consent of all principal parties to the conversation or activity;
- to the person in lawful possession or control of the computer or computer network, or with their express or implied consent; or
- some other exception applies.

Further, the mere possession of a record of a private conversation or activity will constitute an offence under the Act where the individual or body corporate with possession has knowledge (as distinct from a mere suspicion) that the record was obtained through the direct or indirect use of a listening device, optical surveillance device or tracking device in contravention of the Act,[36] *unless* such possession is:

- in connection with proceedings for an offence against the Act or its regulations (if and when they are enacted);
- with the consent of all parties involved in the conversation or activity; or
- the result of communication or publication of the record in circumstances that do not constitute a breach of the Act.

The latter prohibition is of particular significance for journalists as an offence will be committed regardless of whether the journalist actually uses or discloses the record. This prohibition is consistent with section 8 of the *Listening Devices Act 1984* (NSW), although its application is extended to activities recorded using optical surveillance devices. Journalists should, therefore, promptly obtain advice if they receive a record which may fall into this category.

It is notable that none of these prohibitions contain any exception for circumstances in which there is a strong public interest in publication, such as where surveillance exposes corruption. This is a significant matter for journalists, as it may, in some cases, prevent or limit the media's ability to expose such matters.

Conclusion

The Act significantly expands the regulation of overt and covert surveillance in New South Wales. Interesting questions arise as to whether it strikes the balance between privacy interests and the public interest in effective investigative journalism, and how it will operate in relation to new technologies. The second of these issues will, no doubt, be resolved by courts over time.

Sophie Dawson is a Partner and Helen Gill a Graduate Lawyer in the Sydney office of Blake Dawson.

(Endnotes)

1 Section 4 of the Act.

2 Section 4 of the Act.

3 *Violi v Berrivale Orchards Ltd* (2000) 99 FCR 580 at 585-86 (Branson J).

4 *Amalgamated Television Services Pty Ltd v John Marsden* [2000] NSWCA 167; BC200003896 at [21], citing Levine J.

5 (unreported, NSWDC, Graham J, 22 February 1991) at p 14.

6 (2000) 99 FCR 580 at 587 (Branson J).

7 (2004) 60 NSWLR 108

8 *R v Zubrecky* (unreported, NSWDC, Graham J, 22 February 1991) at p 14.

9 *Violi v Berrivale* (2000) 99 FCR 580 at 587 (Branson J).

10 *Director of Public Prosecutions v Nakhla* [2006] NSWSC 781; BC200605999.

11 (2004) 60 NSWLR 108 at [84] (Adams J).

12 *See v Hardman* [2002] NSWSC 234; BC200201585 at [21] (Bryson J).

13 *R v Le* (2004) 60 NSWLR 108 at [84] (Adams J).

14 (2005) 30 WAR 494; [2005] WASC 175; BC200505885

15 *Channel Seven Perth Pty Ltd v 'S' (a company)*, as above at [36] (Le Miere J).

16 Section 31(1) of the *Surveillance Devices Act 1998* (WA) provides that:

> … a judge may make an order that a person may publish or communicate a private conversation or a report or record of a private conversation, or a record of a private activity that has come to the person's knowledge as a direct or indirect result of the use of a listening device or an optical surveillance device under Division 2 or 3, if the judge is satisfied, upon application being made in accordance with section 32, that the publication or communication should be made to protect or further the public interest.

17 *Channel Seven Perth Pty Ltd v 'S'* at [41] (McLure JA).

18 *Channel Seven Perth Pty Ltd v 'S' (a company)* [2007] HCATrans 628.

19 The word 'interfere' is not defined in section 4 of the Act. *The Macquarie Dictionary* (3rd edn, 1998) defines interfere to mean 'to come into opposition, as one thing with another, especially with the effect of hampering action or procedure'. Similarly, in *Fitzpatrick v Day* (1990) 54 SASR 186, Duggan J held (at 189) that the interference in question does not have to be such as to cause 'damage or some sort of alteration to the character or nature of the item in question', there need only be 'the interruption of a regular or intended course of events: a "coming between"'.

20 Section 4 of the Act.

21 Ibid.

22 (2002) 54 NSWLR 333.

23 *Robson v Hallett* [1967] 2 QB 939.

24 See, for example, *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, *Jane Doe v Australian Broadcasting Commission* [2007] VCC 281, *Grosse v Purvis* [2003] Aust Torts Reports ¶81-706, *Kalaba v Commonwealth* [2004] FCAFC 326; BC200408581 and *Kalaba v Commonwealth* [2005] HCATrans 478.

25 Section 4 of the Act.

26 (1996) 186 CLR 454

27 *Taikato v R* [1996] 186 CLR 454 at 460 and 463 (Brennan CJ, Toohey, McHugh and Gummow JJ).

28 *The Macquarie Dictionary* (3rd edn, 1998).

29 See above n 16.

30 Section 4 of the Act.

31 Ibid.

32 'Anti-slacking software at work' *Sydney Morning Herald*, 17 January 2008; 'Microsoft files "Big Brother" patent in the US' *Intellectual Property Newsletter*, February 2008.

33 'Hackers exploit security hole in Excel' *Sydney Morning Herald*, 17 January 2008.

34 (Victorian County Court, 30 October 2000 (Unreported))

35 Sections 11 and 14 of the Act.

36 Section 12 of the *Listening Devices Act*.