28 November 2011

The Executive Director
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001
Email: privacy@alrc.gov.au

Dear Ms Wynn,

Issues Paper: Serious Invasions of Privacy in the Digital Era

Thank you for the opportunity to comment on the Issues Paper. In relation to the issues relating to the question of a statutory cause of action I would reiterate the comments made in my submission in respect of the *DPC's Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy* (attached below).

This submission focuses on some of the issues raised in Questions 26 and 27.

Question 26

As is the case elsewhere, privacy in Australia is regulated via a range of different mechanisms, including information privacy and health records laws, telecommunications laws, surveillance devices laws and various aspects of the general criminal law. While a statutory cause of action would have a valuable role to play for addressing more serious privacy invasions which fall within the gaps, it is arguably that there remains considerable scope to improve existing regimes so as to further narrow those gaps.

Information privacy laws have the potential to regulate both the publication of personal information and privacy intrusive information collection activities. However, the *Privacy Act 1988* (Cth) fails to do so in part due to the limited nature of the principles on which it is based and in part due to significant gaps in its coverage. As a consequence, there is a need for other laws to address significant breaches of privacy arising from the publication of personal information and privacy intrusive information gathering practices.

The key mechanism currently available in relation to publication is the common law action for breach of confidence. While there has been some doubt concerning the ability of plaintiffs to obtain compensation for non-economic harm, the decision of the Victorian Supreme Court in *Giller v Procopets* [2008] VSCA 236 seems to have resolved that problem in Victoria and will arguably carry considerable weight in other jurisdictions. Should that transpire not to be the case, there would be merit in legislating to this effect as suggested in the Issues Paper.

Publication is also subject to criminal prohibitions in the *Telecommunications (Interception and Access) Act* 1979 (Cth) and state and territory surveillance device laws (eg the *Surveillance Devices Act* 1999 (Vic),s 11), to the extent he information published has been collected illegally. It may also in some instances be subject to criminal sanctions in general criminal laws (child pornography laws).

The key mechanisms which currently regulate intrusive information gathering are the federal *Telecommunications (interception and Access) Act 1979* and state and territory surveillance device laws. The former provides protection for the content of communications as they pass through the telecommunications network, while the latter to varying extents limit uses of surveillance devices to gather personal information. The TIAA provides for robust protection but is limited in its scope; the surveillance devices laws vary considerably but are all subject to gaps which limit the extent to which they regulate privacy invasive surveillance activities. Also they provide only for criminal sanctions and are not generally neither well understood nor well enforced. These two sets of laws are supplemented by criminal laws which prohibit specific forms of information gathering (eg laws which criminalise hacking into computers).

(a) Gaps in the coverage of the *Privacy Act 1988* (Cth)

I would strongly endorse all of the recommendations concerning gaps in the coverage of the Act which were made in *For Your Information: Australian Privacy Law and Practice* and would further add the following comments:

- Despite the many exceptions to the small business operator exemption, it remains problematic given the high proportion of businesses which fall within it. The fact that they are not required to comply with the Act means that there is no incentive for them to learn about privacy or to implement privacy protective information handling practices. It is unclear why small businesses require this exemption in Australia when they are not similarly exempt in other countries with private sector data protection regimes. However, if the exemption is to be retained, it would be preferable to require small business operators to comply with a less onerous set of principles, rather than excluding them altogether.

- The employee records exemption also constitutes a major gap. It is clear that privacy is not being dealt with in enterprise agreements and that employers are both able to, and do in practice, gather considerable quantities of personal information in circumstances where they are not held to account for how that information is secured or used. The fact that public sector employers have been able to maintain effective HR functions while not enjoying similar protection (FOI regimes have been in place in many jurisdictions since the early 1980s) suggests that such protection is unnecessary. If it is felt that the existing exceptions to right of access are insufficient then it would preferable to amend these to further strengthen then. It is difficult to see why employers should be exempt from security obligations or obligations to use and disclose personal information consistently with the purpose for which it was collected.

- The issue of media regulation will always be controversial due to the competing public interest in freedom of the media. However, it is difficult to see why there can be any valid basis for failing to implement changes to the media exemption to ensure that media organisations are exempt only to the extent that they are subject to regulation by via enforceable code which compliance with privacy standards. This is an important issue to the extent that there are media organisations which are not subject to any code

and given that with the advent of the blogger and citizen journalist, journalism is no longer the domain only of "media organisations".

- The other exception which requires active consideration is the one for individuals engaged in non-commercial activities. While it is inappropriate for the APPs to apply to individuals generally, it is clear that there is scope for individuals to inflict serious harm on the others via the posting of personal information on the Internet, including on social media sites. I would suggest that a possible solution to this issue would be to include within the Act a Code of Conduct which governs problematic activities to the extent that those who engage in them fall within the jurisdictions of the Privacy Act.

(b) Lack of uniformity in laws which address surveillance

Surveillance laws form an important element of the patchwork of laws which regulate privacy in Australia. However, in addition to lacking in uniformity, they are subject to major gaps and are generally neither well understood nor well enforced. Chapter 6 of the VLRC's *Surveillance in Public Places Report* (2010) provides a useful analysis of the gaps in *Surveillance Devices Act 1999* (Vic) and specific recommendations for its reform.

The Acts which regulate uses of surveillance implement national model legislation developed by a joint working group of the Standing Committee of Attorneys-General and the Australasian Police Ministers' Council on National Investigation Powers. However, this uniformity is confined to the provisions within them which relates to the governance of uses of surveillance devices for law enforcement purposes; the provisions which regulate surveillance in general differ considerable in their scope.[1] It is unclear that it is strictly necessary to regulate general uses of surveillance devices at the state level, but to the extent that it remains so, there would be merit in considering a uniform regime based on the recommendations of the VLRC.

Surveillance in public places has assumed additional importance in the light of technological developments that have taken place since the publication of the VLRC's report in 2010. Furthermore, it is now increasingly possible to identify people directly, via the use of face recognition technology,[2] and indirectly, via automatic number plate recognition and radio frequency identification[3] technologies which link people to objects that allow individuals to be identified. Further issues arise from the increasing prevalence of geo-location surveillance based on tracking devices that provide information about the location over time of a person or an object associated with an individual person. This technology is now commonly used in a range of contexts and products, including the ubiquitous mobile phone and the many devices that make

---

[1] See note on the Victorian Surveillance Devices Act appended to this submission.

[2] See D. Svantesson, 'Face-to-data – the Ultimate Privacy Violation?' (2012) 118 *Privacy Laws & Business* 21, 21-24; B. Buckley and M. Hunter, 'Say Cheese! Privacy and Facial Recognition' (2011) 27 *Computer Law & Security Review* 637; A. Senior and S. Pankanti, 'Privacy Protection and Face Recognition' in S. Li and A. Jain (eds.), *Handbook of Face Recognitions*, 2nd ed. (London: Springer-Verlag, 2011).

[3] See M. Ohkubo, K. Suzuki, and S. Kinoshita, 'RFID Privacy Issues and Technical Challenges' (2005) 48 *Communications of the ACM* 66.

use of global positional system ('GPS') and RFID technologies.[4] Additionally, as noted in the Issue Paper, there are issues arising from the increasing use of drones to conduct aerial surveillance.

(c) Telecommunications privacy

Telecommunications privacy is regulated via the *Telecommunications (interception and Access Act) 1979*, which regulates surveillance involving the content of telecommunications while they are passing over, or stored within, a telecommunications system. It prohibits: intercepting a 'real-time' communication passing over the telecommunications system;[5] accessing a communication such as an email, SMS and voicemail message while it is stored on a telecommunications carrier's (including an Internet Service Provider's) equipment;[6] and communicating or otherwise dealing with illegally intercepted information.[7] Major gaps are that it does not apply to any interceptions that take place either before or after a communication passes over a telecommunications system and is less protective of transactional data. The latter is significant due to the extent that transactional data can be very revealing not only of a person's relationship network but also (in the case of mobile phone data) of their geographical location at specific points in time.

Question 27

Arguably further measures are required to address specific issues, including the following.

Harassment

There can be a close interrelationship between privacy and harassment. For example, there is evidence of the use of surveillance devices to harass individuals (either deliberately in the context of the use of cameras outside abortion clinics, or incidentally, as in the case of sustained paparazzi activities). Likewise, there is potential for stalkers to use surveillance to further their stalking. There is also evidence of publication of personal data as a means of harassment, for example in the context of failed relationships or bullying or where incidents involving bullying are filmed and publicised as a means of further demeaning a victim. While there are laws in some jurisdictions which can be used in some situations, there is arguably merit in considering more general Australia-wide laws along the lines of the UK Protection from *Harassment Act 1997* and the *Malicious Communications Act 1998*.

The issue of (lack of) consent

Our privacy protection is premised on the assumption that privacy protection is generally unavailable where the individual affected has been notified of specific matters, or at least where she or has consented to specific activities. Notification and consent mechanisms provide an important means for ensuring that these laws work in a common sense way. However they are problematic there individuals have no real choice in the matter. This not something that lends itself to simple or easy solutions. However, it is arguably that the concept of proportionality provides a useful starting

---

[4] See, for example, the discussion of location position in S. Nouwt, 'Reasonable Expectations of Geo-privacy?' (2008) 5 *ScriptEd* 376, 380-2.

[5] *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIAA*') ss. 7(1) and 105.

[6] This prohibition applies in circumstances where that message cannot be accessed on that equipment by a person who is not a party to the communication, without the assistance of an employee of the carrier. *TIAA*, , ss. 5(1) ('stored communication') and 108.

[7] *TIAA*, ss. 63 and 108(1).

point. In other words, there must be some legitimate purpose served by the information gathering/surveillance and the nature and quantity or the information gathered/intrusiveness of the surveillance must be proportional in the circumstances.

Coerced access

A related issue concerns he potential for coerced access to personal information that would otherwise be protected and kept secret (for example, because the person who holds it is subject to legal obligations to protect it or because it is password protected). As noted in the Issues Paper, a current issue of concern in the US relates to the growing trend for employers to require access to password-protected Facebook sites of prospective employees. Arguably this practice encroaches unreasonably on individual's freedom of expression and their relationships with friends and family. There is also a danger in the future that employers may require employees to obtain and provide them with copies of the information contained on PCEHRs, thereby undermining the protection currently available for them and potentially undermining the patient-doctor relationship. It is arguable therefore that approach suggested at [180] warrants attention both in the specific context of employer requests to access social media accounts and also in relation to other situations where there are strong public interest grounds for prohibiting the coerced access.

Big data and the issue of re-identification

The Privacy Act currently operates on the premise that information ceases to be "personal information" and therefore subject its operation once it has been deidentified. This aspect of the Act needs to be reconsidered in the light of the issues raised by "big data" and constantly improving techniques for data mining. It is important that deidentification is no longer viewed as a "once and for all process" and that organisations should have ongoing responsibility to reassess deidentified data to ensure that it remains incapable of reidentification.

A right to be forgotten

A problem with the Internet is that it facilitates agglomeration and indiscriminate retrieval of a plethora of information, of varying degrees of accuracy and relevance to an individual's circumstances, including information published by them at different times in their lives and information published by others with or without permission, including information that may have been gathered surreptitiously or via intrusive surveillance practices. The so-called "right to be forgotten" contained in the proposed EU General Data Protection Regulation provides a useful template for a partial solution based on a qualified right to request the deletion of personal information which is worth of consideration for Australia.

Associate Professor Moira Paterson,
Faculty of Law, Monash University

4 November 2011

Privacy and FOI Policy Branch
Department of the Prime Minister and Cabinet
1 National Circuit
BARTON ACT 2600

Dear Sir/Madam,

Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy

Thank you for the opportunity to comment on this legislation. My comments in relation to some of the questions raised are as follows.

1. *Do recent developments in technology mean that additional ways of protecting individuals' privacy should be considered in Australia?*

Yes, recent developments pose new privacy threats which arguably required new measures to protect privacy. The new technologies which pose new privacy threats are not confined to those identified in the paper. They also, for example, include the issues which are dealt with by the Victorian Law Reform Commission in its Report, *Surveillance in Public Places.*[8]

The impact of modern technologies and the practices which they have facilitated has been to undermine privacy in public places by making it easier to observe, record and publish information about individuals' activities and, by removing the randomness of such observations, reducing the extent of anonymity available to them.

As pointed out by in the VLRC's report, public place surveillance impacts disproportionately on marginalised and vulnerable members of society who may rely on public places as "social, living and cultural spaces" and may in fact operate to exclude them from certain public areas. More broadly, however, the specific harm that it causes is its chilling effect which erodes freedom of expression.

2. *Is there a need for a cause of action for serious invasion of privacy in Australia?*

Yes, there is arguably a need for such an action to provide a remedy (and disincentive) for more egregious privacy breaches.

The existing regulatory framework consist of patchworks of information privacy and surveillance devices laws which do not provide adequate protection for important aspects of privacy.

By way of example, the existing private sector principles in the *Privacy Act 1988* (Cth) do not require consent for collection of personal information unless it also qualifies as "sensitive information". In addition, they do not apply to individuals or to the majority of businesses or to the handling by a business of personal information about current or past employees.

[8] VLRC, *Final Report* 18, 2010.

Similarly the restrictions in surveillance device laws are subject to significant limitations that vary from state to state. For example, the current restrictions in Victoria do not restrict the use of surveillance devices in any outdoor location, irrespective of the circumstances.

At the same time, and despite the positive indications provided by the High Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd,*[9], none of the higher courts in Australia have yet been prepared to recognise a privacy tort or to extend the action for breach of confidence so that it provides a de facto cause of action for breach of privacy as has occurred in the UK in the context of the *Human Rights Act 1998* (UK). As noted, in the Issues Paper, existing common law causes of action provide only some limited incidental protection for privacy, although the decision of the Victorian Court of Appeal in *Giller v Procopets*[10] removed an important obstacle to the use of the breach of confidence action for privacy-related actions *by* holding that damages for breach of confidence can be awarded for mental distress falling short of a recognisable psychiatric injury. (The court did not, however, expand the traditional boundaries of that cause of action as it was able to find in favour of the plaintiff on the basis of the breach of the confidential relationship between sexual partners.)

3. *Should any cause of action for serious invasion of privacy be created by statute or be left to development at common law?*

The creation of a statutory tort is arguably preferable because it provides scope to craft a law which clearly addresses the complex policy issues involved (for example, by providing guidance concerning the balancing of privacy with competing interests such as freedom of expression). It also provides an opportunity to provide detailed guidance concerning the operation of the new law.

4. *Is 'highly offensive' an appropriate standard for a cause of action relating to serious invasions of privacy?*

The "highly offensive" test, which was first developed in the United States and more recently adopted in New Zealand,[11] arguably imposes an overly high threshold and tilts the balance too far in favour of freedom of expression. That approach is explicable in the US on the basis of the strong emphasis given to the First Amendment and the lack of any equivalent protection for privacy as a separate right.[12] It is also explicable in NZ due to the similar emphasis on freedom of expression in the New Zealand *Bill of Rights Act 1990.*[13] The high threshold which it imposes is illustrated by a New Zealand case where a couple

---

[9] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

[10] *Giller v Procopets* [2008] VSCA 236.

[11] See *Hosking v Runting* [2005] 1 *NZLR* 1 (CA).

[12] It should be noted, however, that a privacy interest is said to underlie a number of specific articulated rights including Fourth Amendment right to be free from unwarranted search and seizure and the Fourteenth Amendment due process right.

[13] Section 14 protects freedom of expression but there is no direct equivalent protection for general privacy although a privacy interest is said to underlie a number of specific articulated rights, such as freedom from unreasonable search and seizure (s 21), freedom of association (s 17), the right not to be subject to medical or scientific experimentation (s 10) and the right to refuse to undergo medical treatment (s 11)..

unsuccessfully sued in respect of the broadcasting of television footage taken without their knowledge or permission when they were trapped in their car following an accident.[14] While Allan J was satisfied that the couple had a reasonable expectation of privacy in respect of their conversations while trapped in the car, he was not convinced that any parts of the material broadcast qualified as highly offensive. As noted by New Zealand academic, "[t]his was largely because the Andrews were not able to show they were humiliated or embarrassed by the broadcast".[15]

The constitutional position in the US and NZ contrasts with approach taken in the ICCPR which offers direct protection for privacy as well as for freedom of expression. Article 17 provides that a person is entitled to legal protection against arbitrary or unlawful attacks on his or her privacy, family, home or correspondence while Articles 19 protects freedom of expression including the right to seek, receive and impart information and ideas. Australia is a signatory to the ICCPR and does not have any equivalent any Bill of Rights legislation, although the Victoria and ACT Human Rights Charters contain rights of privacy and freedom of expression which are based on those in the ICCPR.

A similar approach to that in ICCPR is found in the European Human Rights Convention which contains similarly worded protection for both privacy and freedom of expression. It should be noted that the expanded breach of confidence action developed by the UK courts since the enactment of the UK *Human Rights Act 1998* to give effect to the UK's obligations under the ECHR does not contain any threshold test of unreasonableness. It instead requires a reasonable expectation of privacy and the absence of any competing public interest which justified the privacy intrusion.[16] The latter provides scope for an explicit balancing of the right to privacy against any competing public interest such as freedom of expression. That approach has been explained as follows by Justice Eady in *Mosley v News Group Newspapers Limited:*[17]

> In order to determine which should take precedence, *in the particular circumstances*, it is necessary to examine the facts closely as revealed in the evidence at trial and to decide whether (assuming a reasonable expectation of privacy to have been established) some countervailing consideration of public interest may be said to justify any intrusion which has taken place.

The requirement that a publication or intrusion must be highly offensive serves would seem to serve three specific aims: to provide an element of objectivity into what is a very subjective subject area, to ensure that the action is not available in cases where the nature of privacy invasion is trivial in nature (thereby avoiding floodgates) and to ensure that the action does not impinge unnecessarily on freedom of expression. It is arguable however, that

---

[14] *Andrews v TVNZ* HC Auckland ,CIV 2004-404-3536, 15 December 2006. This case is discussed in Ursula Cheer, "The Tort of Privacy" (2008 Privacy Issues Forum, Office of the Privacy Commissioner, Wellington, 27 August 2008) < www.privacy.org.nz/assets/Files/PAW/7.-Speaker-Ursula-Cheer.doc>.

[15] Ursula Cheer, "The Tort of Privacy" (2008 Privacy Issues Forum, Office of the Privacy Commissioner, Wellington, 27 August 2008) < www.privacy.org.nz/assets/Files/PAW/7.-Speaker-Ursula-Cheer.doc> at 7.

[16] There is a useful discussion of the current state of the law in the UK in Justice Eady's judgment in *Max Mosley v News Group Newspapers Limited* [2008] EWHC 1777, [2008] WLR (D) 259.

[17] Ibid, at [11].

these can be achieved in ways which allow for more nuanced protection in relation to serious privacy breaches.

There are 3 specific problems with the test suggested:

Offensiveness: what should be in issue is the extent of the privacy invasiveness/harm to privacy The concept of offensiveness is not precisely the same and has different connotations and meanings – ranging from causing to moral outrage to wounding of feeling.

The use of the word "highly": what is required is some qualifier which excludes trivial claims. It is arguable that the word "highly" raises the bar too high especially when judged from the purely objective standpoint of an average person of ordinary sensibilities. To the extent that it is desirable to include some qualifying term which excludes more trivial forms of invasion, a word such "seriously" is arguably preferable.

The nature of the objective test: an objective test serves a useful role in providing some element of certainty and protecting defendants from litigation by plaintiffs who are unusually or excessively sensitive. However, an objective test based on an average person fails to take into account the context or circumstances of a plaintiff and is arguably inappropriate in a society where there are many differing legitimate views about appropriate levels of disclosure of personal information. To the extent that an objective test is appropriate, sensibilities should be judged having regard to the specific context of the individual. For example, older people who have not been part of the social networking community are likely to be more offended by many disclosures than younger people. The appropriate standard in these circumstances in one relating to a person who falls in that category but who is is not usually sensitive.

5. *Should the balancing of interests in any proposed cause of action be integrated into the cause of action (ALRC or NSWLRC) or constitute a separate defence (VLRC)?*

As noted by the VLRC, this is an issue of significance in terms of onus of proof. The approach suggested by the VLC is preferable in that the plaintiff already has the onus of establishing that he or she had a reasonable expectation of privacy which was breached in a serious way. The requirement that a privacy breach needs to be serious to justify litigation itself acknowledges that there is a competing interest in transparency that should always trump where the privacy breach is trivial in nature. In those circumstances it is not unreasonable to require the defendant to prove that a serious breach was nevertheless in the public interest because of the strong public interest in freedom of expression (or some other competing interest).

Irrespective of which approach is taken, it would be worthwhile considering the approach which is now used in the *Freedom of Information Act 1992* (Cth) of including specific guidance as to the factors which may be or may not be taken into account in assessing public interest.[18] See the discussion below in relation to question 8.

[18] Freedom of Information Act 1982 (Cth), s 11B.

6. *How best could a statutory cause of action recognise the public interest in freedom of expression?*

See comments in relation to question 5 above.

7. *Is the inclusion of 'intentional' or 'reckless' as fault elements for any proposed cause of action appropriate, or should it contain different requirements as to fault?*

The VLRC's approach is preferable for the reasons outlined in the extracted quote. There have been many examples of serious privacy breaches arising from conduct which is negligent as opposed to reckless. It would be inappropriate to deprive victims of remedies in those circumstances.

8. *Should any legislation allow for the consideration of other relevant matters, and, if so, is the list of matters proposed by the NSWLRC necessary and sufficient?*

As discussed above, it would be useful to follow the approach taken in the amended *Freedom of Information Act 1982* (Cth) in providing some guidance as to factors relevant to the assessment of public interest.

In my view, factors that should be relevant would include the extent to which an individual has a public profile (but while making clear that public figures are still entitled to appropriate privacy protection), the extent to which the public has a legitimate interest in acquiring that information, whether disclosure of the information contravenes a statutory provision designed to protect privacy interests. The fact that public are merely curious or interested in the information should not be a relevant factor.

Associate Professor Moira Paterson,
Faculty of Law, Monash University

Note on Victorian Surveillance Devices legislation (2008)

The first surveillance device legislation in Victoria, the *Listening Devices Act* 1969 (Vic) was enacted to protect the privacy of private conversations.[19] The Act prohibited the non-consensual use of listening devices to record "private conversations"[20] (those which could not reasonably be expected to be overheard by others)[21] and also prohibited the communication or publication of records or reports of private conversations, except in limited circumstances, including where this was no more than reasonably necessary in the public interest or in the course of a person's duty or for the protection of his or her lawful interests.[22]

The *Surveillance Devices Act* 1999 (Vic) (SDA) was enacted to repeal and replace the *Listening Devices Act* primarily due to concerns about the use of video cameras. An incident which preceded it which was referred to in the Shadow Attorney-General's speech involved the non-consensual taping of sexual activity on the part of a well-known Australian personality and its sale by her ex-boyfriend.[23]

The new legislation was described in the Attorney-General's Second Reading speech as designed "to bring the regulation of optical surveillance devices into line with the regulation of listening devices and to provide "stringent safeguards for the protection of privacy". It built of the existing protection of listening devices and extended protection to three additional types of surveillance devices – optical surveillance devices, tracking devices and data surveillance devices. Protection in respect of data surveillance devices was limited to their use by law enforcement officers and did not extend to the use of software for spying. In commenting in relation to these limitations the Shadow Attorney-General, Rob Hulls commented that this might be an issue that needed to be revisited although he understood the difficulties in introducing legislation aimed at regulating such material.[24]

The extension to tracking devices was explained on the basis that tracking devices were virtually unknown in 1969 but were now commonly used by law enforcement agencies and other persons and organisations in the community.[25] Nevertheless, these were regarded as less intrusive than other categories of surveillance devices as explained in relation to the decision to allow a warrant to track a person or object to be issued by the Magistrates' Court.[26]

The prohibition on the use of optical surveillance devices follows a similar pattern to that for listening devices[27] in that it is confined to "private activities"[28] (those which could not reasonably

---

[19] It was described as "primarily actuated by the desire that the individual man or woman should be protected against persons who spy on his or her private conversations": see Hansard, Legislative Assembly, 22 April 1999 p 546 (Mr Hulls).
[20] *Listening Devices Act 1969* (Vic), s 4(1).
[21] *Listening Devices Act 1969* (Vic), s 3 (definition of private conversation).
[22] *Listening Devices Act 1969* (Vic), s 4(2).
[23] Hansard, Legislative Assembly, 22 April 1999 p 548 (Mr Perton).
[24] Hansard, Legislative Assembly, 22 April 1999 p 547 (Mr Hulls).
[25] Hansard, Legislative Council, 11 May 1999, p 525 (Hon Mr Bowden).
[26] Hansard, Legislative Assembly, 25 March 1999, p 192 (Mrs Wade (Attorney-General)).
[27] *Surveillance Devices Act* 1999 (Vic), s 6(1).
[28] *Surveillance Devices Act* 1999 (Vic), s 7 (1).

be expected to be observed by others)[29]. The Parliamentary Debates suggests awareness of the limitations of the definition of private activity with some discussion of the lack of protection in respect of outdoor places such as backyards and on beaches.[30]

As was the case with the *Listening Devices Act*, the SDA permits participant recording (in relation to optical surveillance as well as listening devices) but imposes restrictions on the dissemination of that information without the consent of the all the parties involved[31] except in limited circumstances.[32]

Like Victoria, other states criminalise very problematic forms of surveillance in public places, and surveillance incidental to other problematic behaviours. For example, other states have sanctions for stalking behaviour[33] and prohibit 'up-skirting',[34] and criminalise misuses of communications and computers.[35]

As might be expected, the issue of surveillance has attracted legislative action in other parts of Australia also. All Australian states and territories have some form of surveillance device legislation, although most of these apply only to listening devices (as was originally the case with Victoria).

There are four jurisdictions with first generation listening device legislation. [36] While these laws are more limited in scope than the SDA, it is noted that the prohibitions in respect of listening devices in the Australian Capital Territory and South Australia Acts[37] prohibit the recording of a private conversation even when an individual is a party to the conversation.

---

[29] *Surveillance Devices Act* 1999 (Vic), s 3(1) (definitions of private conversation and private activity).

[30] Hansard, Legislative Assembly, 22 April 1999, p 559 (Mr Lupton) and p 555 (Mr Perton).

[31] *Surveillance Devices Act* 1999 (Vic), s 11(1).

[32] *Surveillance Devices Act* 1999 (Vic), s 11(2).

[33] See, eg, the *Crimes Act 1900* (ACT) s 35; *Crimes Act 1900* (NSW) s 545AB; *Criminal Code Act 1983* (NT) s 189, *Criminal Code 1899* (Qld) ch 33A; *Criminal Law Consolidation Act 1935* (SA) s 19AA; *Criminal Code Act Compilation Act 1913* (WA) s 338E.

[34] *Criminal Code Act 1899* (Qld) ss 227A – 227C. New South Wales makes it an offensive to film or attempt to film a person for indecent purposes (ie, for a sexual purpose or sexual gratification, without that person's consent, where that person was in a state of undress, or was engaged in a private act, or was in circumstances in which a reasonable person would reasonably expect to be afforded privacy). *Summary Offences Act 1988* (NSW) s 21G

[35] See, eg, *Crimes Act 1900 (*NSW) pt 6; *Criminal Code 1983* (NT) div 10; *Criminal Code 1899* (Qld) s 408E; *Criminal Law Consolidation Act 1935* (SA) pt 4A. Some differences from the Victorian model include: 1) The South Australian legislation makes it an offence to possess a computer virus or equivalent with intent to commit serious computer offence 86I; and 2) The Queensland Act contains a general offence of using a restricted computer without the consent of the computer's controller. That offence carries a penalty of up to 2 years imprisonment. However, that penalty for that offence increases to 5 years imprisonment if the offender causes or intends to cause detriment or damage, or gains or intends to gain a benefit and to 10 years imprisonment if they cause a detriment or damage or obtain a benefit to the value of more than $5000, or intend to commit an indictable offence.

[36] See *Listening Devices Act 1992 (*ACT); *Listening Devices Act 1984* (NSW); *Invasion of Privacy Act 1971* (Qld); *Listening Devices Act 1991* (Tas).

[37] See *Listening Devices Act 1992 (*ACT) s 4(1); *Listening and Surveillance Devices Act 1972* (SA) s 4.

Apart from Victoria, only New South Wales, the Northern Territory, and Western Australia have acts which cover devices other than listening devices.[38] The earliest of these surveillance device law, the *Surveillance Devices Act 1998* (WA) (the WA SDA) uses a model very similar to the one in the SDA but subject to an important key difference in respect of the observations and recording of activities which take place outside buildings. It prohibits the use of an optical surveillance device to monitor a private activity even if it occurs outdoors, provided it is not of an activity the parties ought reasonably to expect may be observed.

The *Surveillance Devices Act 2000* (NT) is likewise broadly similar but again subject to important differences in the scope of its prohibitions of listening and optical surveillance. It prohibits surveillance via the use of listening and optical surveillance devices even if the conversation[39] or activity[40] is not private. The *Surveillance Devices Act 2007* (NSW) (NSW SDA) is worthy of closer scrutiny due its recent enactment and the extent of differences in its structure. It again regulates the same categories of surveillance devices as the SDA. However, there are number of key differences in the scope of the prohibitions.

Its prohibition in respect of listening devices is essentially similar to the equivalent Victorian provision except that it also forbids the non-consensual recording of a conversation to which the person making the recording is a party. [41] It also extends more broadly to conversations intended to be heard by authorised persons who are not parties to the conversation (although again subject to the proviso that the parties ought not reasonably to expect that they will be overheard by other people).[42]

In contrast, the prohibition in respect of optical surveillance devices has a very different focus from its Victorian equivalent. It applies to uses of an optical surveillance device to observe or record any activity (not just private activity) but only if the installation or use of the device involves entry onto or into a building or vehicle or interference with a vehicle or other object without the express or implied consent of the person having lawful possession or control.[43] (The expression "premises" includes land and building both in and outside New South Wales.[44]).

The prohibition against tracking devices is broadly similar[45] but extends more broadly not devices not primarily intended for tracking[46] and is also subject to an additional exception in respect of uses for "lawful purposes".[47]

---

[38] *Surveillance Devices Act 1998* (WA); *Surveillance Devices Act 2000* (NT); *Surveillance Devices Act 2007* (NSW).

[39] See *Surveillance Devices Act 2000* (NT) s 5.

[40] See *Surveillance Devices Act 2000* (NT) s 5. It should be noted, however, that the Long Title to Act refers to the recording, monitoring or observation of persons' "private activities").

[41] *Surveillance Devices Act 2007* (NSW) s 7.

[42] *Surveillance Devices Act 2007* (NSW) s 4(10 (definition of "private conversation").

[43] *Surveillance Devices Act 2007* (NSW) s 8.

[44] *Surveillance Devices Act 2007* (NSW) s 4(1).

[45] See *Surveillance Devices Act 2007* (NSW) s 9.

[46] See *Surveillance Devices Act 2007* (NSW) s 4(1) (definition of "tracking device")..

[47] *Surveillance Devices Act 2007* (NSW) s 9(2)(c).

Finally, the prohibition in relation to data surveillance devices applies to any person (rather than only to a law enforcement officer) where the activity involves entry onto or into premises without the consent of the owner or occupier or interference with a computer or a computer network without the consent of the he person having lawful possession or lawful control of it.[48] Two key differences from the Victorian provision is that a "computer" includes an electronic device for transferring information (not just one for storing and processing information) and a "data surveillance device" includes programs (not just a physical device).[49]

There are also important differences in the scope the provisions which restrict dealings with information obtained from illegal uses of surveillance devices. An important difference in the case of the data obtained illegally via the use of devices other than data surveillance devices is that the NSW Act contains an additional offence in respect of possession[50] (in addition to a separate offence in respect of communication and publication[51]). In addition, the exceptions to the prohibition address the issue of uses by third parties such as the media, quite differently. Instead of having an exception based on a public interest as in Victoria, both offences contain blanket exclusions in respect of persons who have acquired information in a manner that does not involve a contravention of the Act.[52] The prohibition in respect data obtained via the illegal use of data surveillance devices is confined to communication and publication[53] and is again subject to an exception in respect of persons who have acquired information without themselves contravening the data surveillance device prohibition.[54]

A final important difference is that the NSW SDA outlaws the manufacture, supply or possession of surveillance devices for unlawful use.

---

48 *Surveillance Devices Act 2007* (NSW) s 10.

49 See definitions in *Surveillance Devices Act 2007* (NSW) s 4(1).

50 *Surveillance Devices Act 2007* (NSW) s 12 – Possession of record of private conversation or activity.

51 *Surveillance Devices Act 2007* (NSW) s 11 - Prohibition on communication or publication of private conversations or recordings of activities.

52 See *Surveillance Devices Act 2007* (NSW) ss 11(3) and 12(2)(c).

53 *Surveillance Devices Act 2007* (NSW) s 14(3).

54 *Surveillance Devices Act 2007* (NSW) s 13.