



Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to
the Victorian Law Reform Commission

Inquiry into Surveillance in Public Places

July 2009

Office of the Victorian Privacy Commissioner (Privacy Victoria)

GPO Box 5057

10-16 Queen Street

Melbourne Victoria 3000

Australia

Phone: 1300-666-444

Fax: +61-3-8619-8700

Email: enquiries@privacy.vic.gov.au

Website: www.privacy.vic.gov.au

Table of Contents

1.	Introduction	1
2.	Principles to guide public place surveillance	2
3.	A new role for an independent regulator	3
4.	Specific functions of the regulator	4
5.	Voluntary best-practice standards	6
6.	Mandatory codes of practice.....	6
7.	A licensing system for some surveillance practices?.....	7
8.	Changes to clarify and strengthen the SDA (Vic)	8
9.	Creating a statutory cause of action for serious invasions of privacy.....	10

1. Introduction

The widespread use of increasingly pervasive, efficient and inexpensive surveillance threatens the privacy of all Victorians.

The level of surveillance of public spaces has increased rapidly over recent years, and continues to grow. Moreover, the development of digital surveillance technology means that the nature of surveillance has changed dramatically. Digital surveillance means that there is no barrier to storing all footage indefinitely and ever-improving means of image-searching, in tandem with developments in face and gait-recognition technologies, allows footage to be searched for individual people and matched against existing data bases.

Privacy is a fundamental human right, essential to one’s sense of self. Privacy is intrinsically important to human dignity, intimacy and the development of varied and meaningful interpersonal relationships. It needs and deserves protection, even in “public” places.

Failure to protect privacy in public places may fundamentally alter the nature of our society and community. If surveillance of public places continues unregulated and unchecked, the entire notion of a “public place” may be irretrievably lost. Instead, individuals will feel whenever they are in a public place, that they are indeed in a form of panopticon: always able to be observed by an unlimited number of unseen, unidentified “others”. This will have particularly severe impacts on certain groups – the homeless, the socio-economic disadvantaged, young people – all of those for whom private space is limited or unavailable.

For these reasons, I share the Victorian Law Reform Commission’s (the Commission) view that the time has come to reform the regulatory framework that governs surveillance in public places in Victoria. This could be done by amending the *Surveillance Devices Act 1997 (Vic)* [‘SDA (Vic)’] (perhaps renamed the *Surveillance Act*, to reflect less focus on devices and more on activities) to introduce a series of overarching principles, an independent regulator and a regulatory and complaint handling regime.

I endorse the suggested broad definition of “public place”, taken from the *Racial Discrimination Act 1975 (Cth)*. However, the suggested definition of “surveillance” is too narrow. While I endorse the exclusion of “casual observation”, the requirement that surveillance involve the “deliberate or purposive monitoring of people” would exclude any incidental capture – and subsequent use – of images or information about people. The use of images of people “incidentally” captured by CCTV which was deliberately installed for another primary purpose should still be subject to regulation.¹

¹ See *Ng v Department of Education* [2005] VCAT 1054

2. Principles to guide public place surveillance

1. *Do you agree with the draft principles proposed by the Commission to guide policy making about public place surveillance?*

I generally support and agree with the draft principles proposed by the Commission:

1. **People are entitled to some privacy when in public places**

The level of privacy which can be reasonably expected in public places will vary depending on a number of factors, including: the specific location; the nature of the activity or conversation undertaken; whether the surveillance results in a permanent record and whether and how this is disseminated; the form of surveillance used; and the identity of the individual(s) being observed. However, in almost all instances there will be at least some entitlement to, and expectation, of privacy. In this context, the right to privacy is not about having ‘something to hide’, it is about reversing the onus so that government, the media, private businesses and the rest of the community, has a legitimate reason to observe and know².

2. **Wherever practicable, public place surveillance should be transparent**

It is a fundamental component of privacy protection that, when personal information is collected about an individual, that individual has the right to know about the collection, the identity of the collector and the purpose for collection. This is universally reflected in privacy legislation, including Information Privacy Principle (IPP) 1.3 of the *Information Privacy Act 2000 (Vic)*, (‘IPA’).³ This should apply equally to public place surveillance.

I acknowledge the difficulties in achieving complete transparency, due to the inherent nature of surveillance. By definition, it does not involve a discrete transaction between the individual and the collecting organisation. Statutory rules or mandatory codes (discussed below) should reflect this, by providing for some limited exemptions. However, as an overarching, aspirational principle, public place surveillance should be transparent. A qualified expectation, reflected in the phrase “wherever practicable”, should not be used in this context.

3. **Public place surveillance conducted on a continuous basis should be carried out for a legitimate purpose that is relevant to the activities of the organisation conducting it**

Again, it is a fundamental component of privacy protection that personal information should only be collected where necessary and for a legitimate and lawful purpose (IPPs 1.1, 1.2)⁴. This should also be a fundamental principle of public place surveillance.

² See the article ‘Nothing to Hide, Nothing to Fear?’ by former Victorian Privacy Commissioner Paul Chadwick in *Privacy Aware*, Office of the Victorian Privacy Commissioner, Vol. 5, No. 2, Winter 2006 from <http://www.privacy.vic.gov.au/dir100/priweb.nsf/content/3D4B3085A784AEA9CA256C5A0081E819?OpenDocument>, last viewed 25 June 2009; see also Daniel Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy”, 44 *San Diego Law Review* 745 (2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565, last viewed 25 June 2009 ;

³ See OVPC, *Guidelines to the Information Privacy Principles*, September 2006, pp. 34-37;

⁴ *Ibid.*, pp. 28-33;

4. Public place surveillance conducted on a continuous basis should be proportional to its legitimate purpose

Proportionality is also a fundamental tenet of privacy protection (IPP 1.2). Even in the realm of public safety and crime prevention, while there will often be a public benefit to some level of CCTV surveillance (although, as reflected in the consultation paper, this is often hotly debated⁵), this needs to be balanced against other public interests affected, including privacy. In the absence of an identifiable risk of grave harm, extremely intrusive forms of surveillance are difficult to justify.

Proportionality should also be one of the fundamental principles underlying public place surveillance.

2. Should the once-off or intermittent use of surveillance practices by individuals be regulated?

It would be difficult to devise principles or rules to apply to once-off surveillance practices, especially by individuals. As noted in the consultation paper, while the current law prohibits certain of the most offensive types of surveillance practices (e.g. stalking and 'upskirting'), it would be difficult to effectively regulate less invasive and offensive forms. However, the introduction of a statutory cause of action for serious invasions of privacy, as recommended by the Australian Law Reform Commission (ALRC), would represent some protection against one-off incidents, especially where they resulted in identifiable harm or distress.

3. A new role for an independent regulator

3. Do you agree with the proposal that an independent regulator should have responsibility for monitoring the use of public place surveillance in Victoria? Who should perform this role?

I agree with the Commission's proposal that there should be an independent regulator with responsibility to monitor the use of surveillance in public places, inform people about the requirements of the law and how to comply, promote observance of best-practice standards, and report regularly to Parliament about the extent of public place surveillance and whether regulation is adequate. Giving monitoring, awareness-raising and reporting responsibilities to an independent regulator would be of significant value, as none of these activities currently form the responsibility of any specific organisation or authority. Moreover, there is significant evidence that Victorians are not currently well informed as to the extent and nature of public place surveillance.⁶

While I have no settled view as to who should perform this independent regulatory role, a number of the proposed functions are similar to those currently bestowed on the Victorian Privacy Commissioner by the IPA, which include some regulation of surveillance when undertaken by Victorian public sector agencies or contracted service providers. It may therefore make sense, in the absence of a new, specialist, independent regulator, for the functions to be added to these. In addition, in other jurisdictions, privacy or data protection commissioners have regulation of surveillance included in their functions, to varying extents.⁷

⁵ See Victorian Law Reform Commission, *Surveillance in Public Places*, Consultation Paper, pp. 82-84;

⁶ Ibid;

⁷ E.g. the Netherlands, the United Kingdom, Ireland, Canada, New Zealand, Germany, Norway, Greece

However, as outlined below, these additional functions will require substantial resources. The extension of the functions of an existing regulator should not be seen as a “cost neutral” option, otherwise neither the proposed surveillance related functions nor the existing privacy functions will be adequately fulfilled. This would effectively *reduce* the privacy protections afforded to Victorians, which would seem to be diametrically opposite to the desired outcome put forward in the consultation paper.

With respect to the potential difficulties for a State based regulator exercising regulatory functions and powers over both the State public sector and the private sector, these are not insuperable. In my view, such jurisdiction is constitutionally possible. Section 3 of the *Privacy Act 1988 (Cth)* (*‘Privacy Act’*) provides that the *Privacy Act* is not intended to affect the law of a State that makes provision with respect to the handling of personal information and is capable of operating concurrently with the *Privacy Act*. In my view, this means that a potential *Victorian Surveillance Act* could even regulate small businesses, notwithstanding the definition of “organisation” in section 6C of the *Privacy Act* which excludes “small business operators”.

4. Specific functions of the regulator

4. *Should the regulator be given the functions proposed by the Commission?*

The proposed regulator should be given all of the functions proposed by the Commission: monitoring and research; improving public and user awareness; investigatory powers (including at his or her own motion); and reporting to Parliament.

5. *Are there any other functions that should be given to the regulator?*

In my view, public place surveillance should be made subject to a scheme of statutory rules, including the capacity for individuals to make complaints for alleged breaches of these rules. The regulator should be given the functions of accepting such complaints, investigating them and attempting to conciliate them, in a similar fashion to existing complaints handling powers and functions under the IPA.

As outlined below, while non-binding, advisory guidelines could be useful, this would only be the case where they were used to assist in compliance with binding requirements under legislated rules or mandatory codes. Voluntary best practice standards would not be sufficient on their own.

6. *Would a registration scheme assist the regulator to acquire information about surveillance use? Is such a scheme practical? Should some users be exempt from registration requirements?*

While a registration scheme could be extremely labour and resource intensive (although presumably only initially), it is arguable that the proposed monitoring functions of the regulator could not be effectively carried out without it. Requiring users of continuous public place surveillance to register would provide information as to the extent, scope and nature of surveillance in Victoria, which is almost entirely lacking currently.

Compliance costs for businesses could be minimised by keeping the process simple and straightforward, in a similar fashion to the data registration procedures under the *UK Data Protection Act*⁸. However, the countervailing argument is that too many resources would be devoted to the registration function and not enough to more effective controls such as handling complaints.

While some agencies might argue the need for an exemption (e.g. law enforcement organisations), provided details of registration are not published and the registration process is simple, there should be no need for exemptions, as this would undermine the proposed monitoring function.

7. What (if any) investigatory powers should be given to the regulator?

The complaint handling function should be modelled on that currently existing under the IPA, with an initial emphasis on conciliation. If in the course of conciliating the complaint, evidence emerged of a significant breach, the regulator could move on to a formal investigation with full investigatory powers. This would mean that, at a minimum there would need to be: a power to require people to answer questions; a power to compel the production of documents (including video and audio recordings); and, given the proposed definition of “public place”, (which would include premises otherwise considered private if the public has access as of right or by invitation), the power to enter and search premises. This last power could be modified by requiring authorisation by a judge or magistrate.

8. Should the regulator have an own motion investigatory power in order to identify systemic problems with surveillance in public places?

Given the nature of mass surveillance, which may escape the attention or notice of individuals, despite its intrusive and potentially offensive nature, the regulator should have an own motion investigatory power in order to identify systemic problems. In my view, this own motion power should attract the full investigatory powers (to compel answers, documents and enter and search premises) outlined above, with a power to serve a compliance notice when investigation reveals a breach of any statutory rules (see page 7).

9. Should the regulator have the power to develop advisory guidelines which explain the law concerning surveillance in public places?

In my experience, the development and promulgation of advisory guidelines can be an effective way of promoting and encouraging compliance with legal obligations.⁹ However, as in the case of voluntary best practice standards, advisory guidelines are no replacement for binding obligations. The examples given in the consultation paper¹⁰, of compliance codes developed by the Victorian Worksafe Authority under the *Occupational Health and Safety Act 2004 (Vic)*, and codes of practice prepared by the NSW Anti-Discrimination Board under the *Anti-Discrimination Act 1977 (NSW)*, are effective only because they provide guidance in the context of binding legislative obligations.

⁸ Discussed, *ibid.*, para 6.75, p. 143;

⁹ See, for example, OVPC [Guidelines to the Information Privacy Principles, Edition 2](#), September 2006; OVPC [Responding to Privacy Breaches, Guide Edition 1](#), May 2008; OVPC [Privacy Impact Assessment Guide](#), Edition 2, May 2009

¹⁰ At para 6.80 p. 144;

5. Voluntary best-practice standards

10. *Would voluntary best-practice standards developed or approved by the regulator be useful?*

As mentioned at 5, above, voluntary best practice standards could be useful, but not in isolation. As in the case of advisory guidelines, voluntary standards cannot stand in the place of binding obligations. While the introduction of voluntary standards could be perceived to be an initial “light touch” regulatory action, to be followed if necessary by voluntary codes, in my view the rights and interests at stake are of such importance and the scope, extent and nature of public place surveillance is already so overwhelming that some form of mandatory regulation is required.

11. *Is linking voluntary best-practice standards to government procurement criteria a good strategy for encouraging responsible use of surveillance practices? Are there other strategies for encouraging compliance with the voluntary standards?*

The difficulty with linking government procurement criteria as a strategy for encouraging responsible use of surveillance practices is that one of (if not the) leading users of such practices are governments of various levels. Procurement criteria would have no effect on them. Likewise, very small businesses are unlikely to obtain government procurement contracts, thus such linkage would have little, if any, effect on them.

6. Mandatory codes of practice

12. *Should there be mandatory codes, if so, what conduct should they regulate?*

There should be statutory rules, rather than mandatory codes, to regulate the conduct of public place surveillance. These rules should be based on the fundamental principles set out in the consultation paper (see 1, above).

While both the IPA and the *Privacy Act* contain provisions for the development and approval of codes in substitution for compliance with relevant privacy principles¹¹, they have not proven especially useful. In the case of the IPA, no codes have been developed or approved. This may be because the IPA does not regulate “industries” as such – it only applies to the Victorian public sector.

In the case of the *Privacy Act*, only three have been approved and an additional one is still being considered. It would not appear that particular organisations or industries have struggled to comply with the National Privacy Principles in the absence of a specific code.

13. *If mandatory codes are introduced, should the regulator have the power to approve industry codes that operate in their place?*

As outlined above, I do not see mandatory or industry based codes as a useful model. While there may be some situations in which the nature of particular industries or practices necessitated *additional* protections, there is no reason why these could not be built into a system of statutory rules.

¹¹ IPA, s.18(3)(d), Privacy Act s.18BB(2)(a)

14. Should the regulator be empowered to investigate complaints made about potential breaches of a mandatory code? How broad should such powers be?

As outlined above, statutory rules, rather than mandatory codes should be accompanied by a complaints mechanism, allowing individuals to complain to the regulator about alleged or potential breaches. The regulator's own motion investigatory power should also apply to suspected breaches in the absence of a specific complaint. In addition, a compliance notice power could apply in the case of repeat, serious or flagrant breaches of the statutory rules.¹² If mandatory codes are introduced, the similar powers should apply.

15. What kind of sanctions should be imposed for breaches of a mandatory code?

As outlined above, my preferred model of regulation would be one based on that currently operating under the IPA, focused on conciliation and compensation, rather than "sanctions". I am extremely cautious about the concept of imposing additional criminal sanctions.

One of the possible reasons for the lack of prosecutions under the SDA (Vic) is the perception that, in many cases, criminal penalties would be disproportionate to the mischief or damage caused by the surveillance activity involved.

A preferable scheme would be one where the regulator was mandated to attempt to conciliate complaints and only where conciliation was unsuccessful or not practicable, could the regulator make a declaration that there had been a breach of the code (at his or her own motion or at the request of a party to the complaint) and that certain steps should be taken to remedy the breach.

The regulator should also have a own motion investigatory powers and the ability to serve compliance notices to remedy breach. As under Part 6 of the IPA, failure to comply with a compliance notice could result in sanctions. While rarely used, regulators need "big stick" powers as well as compliant handling and educative functions.¹³

It would only be where specific surveillance activities prohibited under the SDA (Vic) were undertaken that criminal sanctions should apply.

7. A licensing system for some surveillance practices?

16. Should users of some forms of surveillance practices be required to obtain a license from a regulator?

I am sceptical about the efficacy of a licensing regime. Certain forms of surveillance are so invasive and potentially offensive that they should be prohibited, in the absence of a warrant. These forms should include, at a minimum:

¹² See IPA, s44.

¹³ See *The Governance of Privacy: Speak softly and carry a big stick*, Speech by Dr Anthony Bendall, Deputy Privacy Commissioner, to the Australian Institute of Administrative Law Forum, Melbourne, 8 August 2008, available at <http://www.privacy.vic.gov.au/dir100/priweb.nsf/content/F776BE46B0105C42CA256C4D0019BD50?OpenDocument>, last accessed 6 July 2009;

- All covert surveillance;
- X-ray body scanners (it is unlikely Victorian legislation could affect the use of such scanners at airports, for Constitutional reasons, but any more general use should be prohibited); and
- Infra-red equipment and other equipment operating outside the visible light spectrum.

Other forms of surveillance should be regulated under the overarching principles, statutory rules and complaints mechanism outlined above.

If the Victorian Privacy Commissioner is to be the regulator, operation of a licensing scheme is a function which bears little, if any similarity to those already carried out under the IPA (except in very general terms, as it would involve a balancing of competing public interests). It would also be extremely resource intensive. In order for it be effectively achieved without detrimental effects on the functions mandated by the IPA (and other potential functions related to surveillance), it would require a substantial investment of resources.

17. *Are there any surveillance practices in Victorian public places that are particularly concerning? If so why?*

The forms of surveillance outlined in 16 above are all of particular concern, which is why they should be prohibited without warrant.

Another emerging trend which is particularly concerning is the convergence of several forms of surveillance, operated by the one agency or organisation in a given context. For example, the combination of CCTV or Automatic Number Plate Recognition (ANPR) and facial recognition technology has the potential to severely threaten personal privacy.

More fundamentally, the combination of electronic surveillance with the ever increasing demand for identity documents, particularly where these are copied or electronically scanned and retained, means that not only can individuals be observed, but also identified and potentially located, as many forms of identity documents (including drivers' licenses, the most commonly used form) include a home address.

The trend of combining various forms of surveillance strengthens the case for providing the regulator with sufficient resources to effectively monitor which organisations use various surveillance technologies.

8. Changes to clarify and strengthen the SDA (Vic)

18. *Should the SDA (Vic) expressly prohibit the use of an optical surveillance device in toilet areas, shower areas and change rooms?*

As indicated above, the SDA (Vic) should be reformed and restructured, away from its current concentration on different *types* of devices, towards more general and comprehensive regulation of surveillance.

As part of this, the SDA (Vic) should be amended to expressly prohibit the use of surveillance devices in areas with a clear and high expectation of personal privacy (e.g. toilet areas, shower areas, change areas and bathrooms), as is currently the case with respect to

work places¹⁴. This should be extended to other places where people ought to reasonably expect privacy, such as lunchrooms or rest areas.

19. Should the definition of “tracking device” in the SDA (Vic) be amended so that it includes all devices capable of determining the geographical location of a person or an object?

The present definition of “tracking device” needs to be amended, preferably as part of a wholesale reworking, away from concentration on particular devices. Including all devices capable of any form of tracking, regardless of their primary purpose, would be appropriate. This amendment would also bring the SDA (Vic) into conformity with the *Surveillance Devices Act 2007 (NSW)*¹⁵.

20. Should the SDA (Vic) be amended to include a new “catch-all” category of surveillance devices to cover those devices that do not fit within the Act’s existing listening, optical, tracking and data surveillance categories? How could this be done?

Again the SDA (Vic) should be reformed and restructured, away from its current concentration on different *types* of devices, towards more general and comprehensive regulation of surveillance. This should encompass both prohibition of certain practices and regulation of others, subject to rules and safeguards. As part of this reform, the SDA (Vic) should cover any device capable of surveillance or tracking of human movement, activity or communication.

21. Should the exemption for participant monitoring in the SDA (Vic) be removed? If so, should this be done for both listening and optical surveillance devices?

The participant monitoring provisions of the SDA (Vic) should also be reformed. The use of covert surveillance should generally be prohibited except in limited and appropriate circumstances, preferably with a warrant.

22. Should the enforcement regime of the SDA (Vic) be extended to include civil penalties?

As detailed above, regulation of surveillance activities should be according to a set of statutory rules, with a complaints mechanism initially focusing on conciliation, but also including own motion investigations and compliance notices. As indicated at 15, above, one possible explanation for the lack of prosecutions under the SDA (Vic) is the perception that, in many cases, criminal penalties are disproportionate to the mischief or damage caused by the surveillance activity involved.

However, another possible explanation is the inherent conflict involved in providing Victoria Police as the only agency capable of prosecuting offences under the SDA (Vic). On one view, it is in Victoria Police’s interest to encourage individuals and agencies to engage in surveillance, as any footage or information obtained is almost always accessible to Police and can be useful in intelligence or operational activities. For this reason, one of the functions

¹⁴ SDA (Vic), s. 9B

¹⁵ SDA (Vic), s.4

that the proposed regulator should be given is to refer appropriate matters under the SDA (Vic) to the Director of Public Prosecutions.

23. Should the regulator's proposed powers to develop guidelines be extended to clarifying the meaning of consent in the SDA (Vic)? If so, how should the meaning of consent be clarified?

Consent is generally a problematic concept in the area of surveillance. For this reason, the meaning of consent should be clarified in the SDA (Vic) itself. Even implied consent should be free, revocable and fully informed. A person who is notified of surveillance but has no real choice or opportunity to leave the relevant area or avoid the relevant activity should not be considered to have consented. It is difficult to see how guidance from the regulator could provide clarity in this area, given that in general, true "consent" will not have been obtained.

9. Creating a statutory cause of action for serious invasions of privacy

24. Should there be a statutory cause of action for serious invasions of privacy along the lines proposed by the ALRC?

As indicated in my submission to the ALRC's [*Review of Australian Privacy Law \(Discussion Paper No. 72\)*](#), I support the proposition that the law should provide for some form of cause of action for invasion of privacy.

This could be achieved either by statute, as is proposed here, or by allowing the courts to act instead. Relying on the courts to recognise a cause of action for privacy may not be the best approach, given the inherent limitations associated with the courts only being able to consider particular matters brought before them by parties resourced to access justice at the requisite level. In addition, the courts would be limited by existing remedies developed within the common law or equity.

Legislators have a better opportunity to craft a cause of action that is more precisely targeted and which takes into account competing public interests. Moreover, protection of a fundamental human right such as privacy should not be dependent on the efforts of a particularly persistent and well resourced plaintiff, to take an action all the way to the High Court of Australia in order to definitively establish the existence of a cause of action.

In my experience, a large number of individuals who contact the Office of the Victorian Privacy Commissioner and similar regulators in other jurisdictions seek redress for interferences with spatial or physical privacy for which there is currently no readily accessible remedy in Australian law, or seek to complain about interferences with personal information by other individuals, which are effectively beyond the jurisdiction of all current privacy regulators.

As indicated at 2, above, the creation of a statutory cause of action would be the best way of providing redress for one off or intermittent surveillance actions by individuals.

HELEN VERSEY
Victorian Privacy Commissioner