



Australian Government

Office of the Privacy Commissioner

**Consultation Paper 7 -
*Surveillance in public places***

**Submission to the Victorian Law
Reform Commission**

July 2009

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988 (Cth)* (the Privacy Act), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT Government agencies, and personal information held by all large private sector organisations, private health service providers and some small businesses. In addition, the Office has regulatory functions under other Acts, such as the *Telecommunications Act 1997* and the *Crimes Act 1914*.

Background

2. The Privacy Act assists in protecting individual privacy by fostering an individual's control over their personal information, through the application of privacy principles to the information handling practices of Commonwealth and ACT government agencies and many private sector organisations. The Information Privacy Principles (IPPs) cover the public sector while the National Privacy Principles (NPPs) cover private sector organisations.
3. The Office appreciates the opportunity to provide comment to the Victorian Law Reform Commission (the Commission) on its Consultation Paper 7, '*Surveillance in Public Places*'. The Office understands this Consultation Paper forms part of the second phase of the Commission's privacy project¹ in which the Commission has been asked to consider whether any regulatory models proposed in relation to surveillance of workers, could be applied in other surveillance contexts, such as surveillance in places of public resort, to provide for a uniform approach to the regulation of surveillance².
4. The rapid emergence in recent years of new surveillance technologies, illustrates the way in which personal information about individuals is now more easily captured, aggregated and widely distributed than ever before. For example, the use of optical surveillance measures, such as closed circuit television (CCTV), and location tracking devices, such as global positioning systems, means that much of the day to day life of an individual is now potentially open to scrutiny.
5. The Office recognises that the right to privacy is not absolute. It is necessary to balance privacy with other important social interests, such as the safety and security of the community. This should not diminish the role

¹ The first phase related to workplace privacy and was completed with the Commission making 65 recommendations which would have the effect of opening up privacy practices to more scrutiny. Further details can be found on the Commission's website:
<http://www.lawreform.vic.gov.au/wps/wcm/connect/Law+Reform/Home/Completed+Projects/Workplace+Privacy/>

² Commission's terms of reference for the privacy review -
<http://www.lawreform.vic.gov.au/wps/wcm/connect/Law+Reform/Home/Current+Projects/Surveillance+in+Public+Places/LAWREFORM+-+Surveillance+in+Public+Places+-+Terms+of+Reference>

played by privacy in democratic societies in according individuals the freedom to pursue their daily lives with appropriate respect, dignity and anonymity. Rather, the challenge is to how to achieve an appropriate balance with the protection of important human rights and social interests that may sometimes compete with privacy.

6. The Office has a number of comments about certain aspects of the Commission's 'Surveillance in Public Places' Consultation Paper. These are discussed in more detail below.

Public Surveillance Principles

7. The Office notes the Commission's proposal to develop broad public surveillance principles to inform and guide any changes to the way in which surveillance in public places is regulated in Victoria.
8. The Office supports the development of broad nationally consistent principles that enhance good privacy practice and is pleased to note that the Public Surveillance Principles are consistent with the privacy principles in the Privacy Act. A simple practical set of principles is an effective way to encourage users of surveillance to build privacy compliant practices into a surveillance system prior to its implementation and to encourage national consistency in the handling of surveillance information.
9. Currently, NPP 8 in the Privacy Act provides a limited right for an individual to transact anonymously with organisations. The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 states:

Anonymity is an important dimension of privacy...Unless there is a good practical or legal reason to require identification, organisations should give people the option to operate anonymously.

10. The Australian Law Reform Commission (ALRC) in its review of privacy recommended that an anonymity principle should be included in the model Unified Privacy Principles (UPPs) that it has proposed. As noted by this Office and supported by the ALRC, an anonymity principle encourages agencies and organisations to consider the fundamental question of whether they need to collect personal information at all and if so, the nature of the personal information it requires.
11. The Office welcomes that one of the Public Surveillance Principles requires organisations and agencies to consider whether '*People are entitled to some privacy when in public places*'. This principle should encourage organisations to consider the use of surveillance to ensure that it is only used where, and to the extent, necessary for the particular purpose envisaged.
12. Considering whether cameras may be installed in sensitive areas such as in or near toilets, shower rooms or change rooms, or sensitive situations such as where medical services are provided, is in the Office's view an important initial consideration. The Office notes that if surveillance

systems are to be considered in such areas, there should be strict conditions on their deployment.

13. Some guidance regarding the Public Surveillance Principles, ensuring that surveillance is only carried out for a legitimate purpose and that it is proportional to its legitimate purpose, can be found in the Council of Australian Government's *National Code of Practice for CCTV Systems for Mass Passenger Transport Sector for Counter Terrorism* (the COAG CCTV Code)³ and the UK Information Commissioner's CCTV Code of Practice⁴ which are both referred to in the Consultation Paper.
14. The COAG Code distinguishes between different levels of transport security risks and for each level of risk identifies the CCTV operational objectives for people, objects or vehicles. The operational objectives include:
- Observe: generally observe/monitor behaviour within a broad area
 - Detect: verify an incident after an alarm or report
 - Recognise: monitor/track an individual person, object or vehicle
 - Identify: capture enough detail to identify a person, object or vehicle.

For each operational objective the Code recommends that certain performance criteria (including that relating to image capture rates, image resolution, storage, camera positioning) for CCTV systems be met.

15. The UK Information Commissioner's CCTV Code of Practice uses four categories to determine the required quality of images:
- Monitoring: watching the flow of traffic or the movement of people where you do not need to pick out individual figures
 - Detecting: to detect the presence of a person in the image without needing to see their face
 - Recognising: to recognise somebody you know or determine that somebody is not known to you
 - Identifying: to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

³ The Code is voluntary and was approved by the Council of Australian Governments in 2006 – see http://www.coag.gov.au/coag_meeting_outcomes/2006-07-14/docs/cctv_code_practice.rtf

⁴ Information Commissioner's Office, CCTV Code of Practice revised 2008, p9, www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

16. Organisations and agencies should be encouraged to ensure that no record is made of images unless this is necessary for a legitimate and particular purpose for which the cameras have been employed, and that such recording, and any copies of the recording, are destroyed once they are no longer needed for that purpose.
17. Considering whether images can be anonymised, for example, whether faces and other identifying features could be blanked out if the images are to be used or disclosed for secondary purposes, is another option that users of surveillance should be invited to explore.
18. One of the foundations of privacy is that individuals control the use of their personal information to the greatest extent possible. The Office is supportive of the development of principles which provide individuals with greater control over the manner in which information about them is to be handled.
19. One of the key mechanisms to achieve a level of control over personal information is to encourage transparency regarding information handling. National Privacy Principle 1 in the Privacy Act requires that organisations subject to the Privacy Act provide individuals with notice regarding the purpose for which information is to be collected, how it is to be used or disclosed and how an individual may gain access to this information⁵. Ensuring that individuals have access to information about themselves where that is practicable, and the opportunity to correct any inaccuracies or discrepancies identified, also provide individuals with control over their information.

Options for Reform

20. The Consultation Paper has suggested several alternatives to address the regulation of surveillance in Victoria:
 - Establishing an Independent Regulator
 - Best Practice Standards
 - Mandatory Codes
 - A Licensing Regime
 - Changes to the Surveillance Devices Act
 - Development of a statutory cause of action
21. The Office is supportive of the options put forward by the Commission where these options will promote national consistency in the regulation of surveillance and enhance good privacy practice in sectors currently unregulated by privacy legislation.
22. The Office also suggests that the changes proposed in relation to the regulation of surveillance could be considered in light of the forthcoming Australian Government's response to the ALRC's Report 108 on privacy.

⁵ Privacy Act 1988 (Cth) Schedule 3- National Privacy Principle 1.3

With this in mind the Office has commented on a few of the options for reform proposed by the Commission.

Establishing Mandatory Codes

23. At present, the Privacy Act allows organisations to develop privacy codes that are specific to an organisation, industry or type of activity. Once approved by the Australian Privacy Commissioner, these codes, which must be at least the equivalent of the statutory privacy principles, bind those organisations to the code, and effectively replace the NPPs.
24. In the Office's submissions to the Australian Law Reform Commission's (ALRC) review of privacy, the Office proposed that the Australian Privacy Commissioner should be empowered, in very limited circumstances, to make binding codes in relation to certain industries, practices or technologies that may raise heightened privacy risks⁶. The ALRC in its final report did not support this suggestion⁷.
25. The Office is still of the view that a qualified binding code making power modelled on the industry code provisions in Part 6 of the *Telecommunication Act 1997* would support the co-regulatory approach set out in ALRC Report 108.
26. The code model set out in the Telecommunications Act essentially creates a framework where the emphasis is on encouraging industry participants to voluntarily develop and comply with codes but where the regulator can intervene and impose a mandatory standard if necessary. In summary, under this framework:
- Bodies and associations that represent industry sectors may voluntarily develop an industry code, which can then be registered by the regulator
 - As part of consideration the code for registration, the regulator must be satisfied that certain criteria has been met, including appropriate industry and public consultation on the development of the code
 - The regulator also has the power to request a body or association develop an industry code; and to make compliance with an industry code mandatory
 - In certain circumstance, such as if there is no industry code or the industry code is deficient, the regulator has the reserve power to make an industry standard that applies to certain industry participants.

⁶ See: www.privacy.gov.au/publications/submissions/alrc/all.html#L19068

⁷ See the ALRC's discussion on this topic at:

www.austlii.edu.au/au/other/alrc/publications/reports/108/48.html#Heading89

27. Should this type of framework be incorporated into the Privacy Act it could facilitate more timely responses to new and emerging privacy issues, in particular those that relate to new technologies. Binding codes or standards might be appropriate for issues such as CCTV and face recognition technology or Radio Frequency Identification where industry has not sufficiently responded to the specific privacy challenges.
28. The Office suggests that this may be one means of addressing the regulation of surveillance in public places on a national level.

Voluntary Best Practice Standards

29. The Commission suggests as an alternative to mandatory codes the development of voluntary best practice standards to assist in the regulation of surveillance in Victoria and suggests linking voluntary best-practice standards to government procurement criteria as a possible strategy for encouraging responsible surveillance practices.
30. Section 95B of the Privacy Act has similar provisions. Commonwealth Government agencies are required to comply with the IPPs in the Privacy Act when handling personal information. At times agencies outsource a function that requires a contractor to collect and handle personal information on behalf of the agency.
31. When entering a Commonwealth contract, section 95B of the Privacy Act requires an agency to take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice that would breach an IPP if done by the agency. In particular, the agency must ensure that the Commonwealth contract does not authorise a contracted service provider to do or engage in such an act or practice.
32. In its submission to the ALRC privacy inquiry the Office noted that the contracted service provider provisions in the Privacy Act work well. The ALRC also concluded that the Privacy Act provisions relating to Commonwealth contractors remain appropriate and effective.
33. In extrapolating this to the Commission's proposal that regulation of surveillance in Victoria could be encouraged by linking best-practice standards to government procurement criteria, the Office notes that while this approach will contribute to encouraging responsible surveillance practices it will not independently lead to uniform regulation of surveillance in Victoria.

Development of a statutory cause of action

34. The ALRC has also recommended that federal legislation should provide for a statutory cause of action for a serious invasion of privacy. Further, the ALRC recommended that any such cause of action should contain a non-exhaustive list of the types of invasion that fall within the cause of action including where:

- there has been an interference with an individual's home or family life
- *an individual has been subjected to unauthorised surveillance*
- an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed or
- sensitive facts relating to an individual's private life have been disclosed⁸.

35. The Office supports the development of a statutory cause of action for invasion of privacy.⁹ The Office encourages the ongoing collaboration between governments to propose a cause of action that could be uniformly applied across all jurisdictions to ensure consistency and promote certainty.

⁸ See Recommendation 74-1 of the ALRC Report 108, May 2008.

⁹ Chapter 5 of the Office's response to the ALRC's DP 72 at:
http://www.privacy.gov.au/publications/submissions/alrc_72/PartA.html#ach5