

- Surveillance Paper Released
- Privacy Awareness Week 2009
- Taking Photos Results in a Privacy Complaint
- Canadian Court Rulings on Privacy
- Privacy and Human Resource Management



Office of the
Victorian Privacy
Commissioner

Protecting not Preventing

Helen Versey Privacy Commissioner

A few weeks ago I was contacted by a journalist who, in the course of investigating health issues in restaurants, had made a Freedom of Information (FOI) application to a local council seeking details of complaints about restaurants in the local area. The information had been refused 'because of privacy'. Irrespective of whether the request involved personal information, I pointed out to the journalist that since the request had been made under FOI then that was the law that applied. Parliament when introducing the *Information Privacy Act* had decided that the FOI regime should be preserved for requests to access for personal information.¹

This is not the first time I have received such an enquiry from a journalist receiving this response to an FOI request. It is no doubt more convenient to an organisation to simply refuse a request that involves personal information

(VCAT). Equally, if the organisation decides to rely on the exemption under section 33 it should give the appropriate notice under the FOI Act to applicants so that they can exercise their rights of review by VCAT. Any release properly made under the FOI Act does not breach the *Information Privacy Act*.²

Privacy is not secrecy

'BOTPA' often occurs when organisations subject to secrecy provisions in other legislation claim it is privacy legislation that prevents disclosure, rather than the secrecy provisions. Privacy is not secrecy. Unlike privacy legislation, secrecy provisions often apply to non-personal as well as personal information and include penalties against individuals for non-compliance. They are invariably more restrictive than privacy legislation.

The *Information Privacy Act* does not prevent the disclosure of personal information but rather permits it in certain circumstances, even without the consent of the individual concerned. It takes into account other competing public interests, such as permitting disclosure to assist law enforcement agencies investigating crime, or for public health, safety and welfare purposes. What it does do is protect personal information from misuse by Victorian public sector organisations by requiring them to only collect what is necessary for their functions and use and disclose it for purposes prescribed by the Act, or with the consent of the individual concerned.

The theme for Privacy Awareness Week (3 – 9 May) is 'Privacy – Protecting not Preventing'. I hope that the public sector will remember this and avoid using BOTPA in the future. ■

¹ Section 12 *Information Privacy Act 2001*(Vic)

² For more detailed information about how the *Freedom of Information Act* and the *Information Privacy Act* work together see [Info Sheet 05.08 Freedom of Information and the Information Privacy Act](#) at www.privacy.vic.gov.au.

privacy:
protecting not preventing

Privacy laws **protect** personal information but do **not prevent** you from doing your job.

Personal information is now on the internet, databases, USB keys and laptops. New technologies are changing the way we work but the Information Privacy Principles (IPPs) are still your guide to responsible information handling.

For more information contact your organisation's privacy officer or go to www.privacy.vic.gov.au.

**new technologies,
same responsibilities**

3-9 MAY 2009 Privacy Awareness Week

The logo for the state of Victoria, featuring a stylized 'V' with a white outline and a blue fill, with the word 'Victoria' written below it.

Privacy Awareness
Week is 3-9 May
2009. See page 2.

Surveillance Paper Released

Dr Anthony Bendall, Deputy Commissioner

The Victorian Law Reform Commission has completed the first stage of its inquiry into surveillance in public places. The Commission released a [Consultation Paper](#) on Monday 30 March. The paper seeks public submissions and is available at www.lawreform.vic.gov.au.

The paper explains how surveillance is used in public places and how it is regulated. It contains a discussion of privacy theory in the context of public places and also examines the risks and benefits of public place surveillance. Finally, the paper contains a number of reform proposals and asks a series of questions to gain feedback from the community to inform the Commission's final report.

The major reform proposals are guided by these four draft policy principles, designed to inform and guide any changes to regulation.

1. People are entitled to some privacy when in public places;
2. Wherever practicable, public place surveillance should be transparent;
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; and

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

Based on the four principles, the six proposed options for reform encompass:

1. A role for an independent regulator to monitor, report and provide information about public place surveillance in Victoria.

While the specific regulator is not named in the paper itself, the Commission's chair, Professor Neil Rees, [said](#) at the paper's launch, "We suggest there is an existing state regulator, the privacy commissioner, whose functions could be broadened to deal with this particular issue."

2. New voluntary best practice standards to promote responsible use of surveillance in public places.
3. Mandatory codes to govern the use of surveillance in public places with sanctions for non-compliance.



4. A licensing system for some surveillance practices.
5. Changes to clarify and strengthen the *Surveillance Devices Act 2004*.
6. A new statutory obligation to refrain from committing a serious invasion of privacy.

The closing date for submissions is 30 June 2009.

In the United Kingdom

The Victorian paper adds to a growing literature on surveillance around the world. In January, the British House of Lords Constitutional Committee released its report, [Surveillance—Citizens and the State](#). In the report, the Committee urges the UK Government to exercise more restraint over the use of data collection and electronic surveillance:

"We regard privacy and the application of executive and legislative restraint

Privacy Awareness Week 2009

Privacy Awareness Week is being held 3–9 May. The promotional material for Victorian public sector organisations remind staff that privacy laws are designed to protect personal information, while allowing them to do their jobs.

The *new technologies, same responsibilities* slogan on the Privacy Awareness week poster highlights the fact that public sector staff also have important

obligations to keep personal information secure. "As our recent [survey](#) into the use of portable storage devices reveals, there are many risks to the security of data on devices such as USB keys, iPods and mobile phones. These new technologies bring many benefits but also some risks. The Information Privacy Principles still apply regardless of the technology that is being used for handling personal information," Privacy Commissioner Helen Versey says.

Privacy Awareness Week events are being held for staff of [Victorian public sector agencies](#), and by the [Asia Pacific Privacy Authorities](#). An animated video being released by the [Asia Pacific Privacy Authorities](#) reminds young people to be mindful of what they are doing online as what they post on the internet could have unintended consequences. See www.privacyawarenessweek.org. ■



photo: David Taylor

Taking Photos Results in a Privacy Complaint

Anthony Zaspel, Senior Policy and Compliance Officer

The Privacy Commissioner recently considered a complaint regarding the circumstances of collecting, and then using, images collected at a public event.

In summary, a Local Council took photos at a public event it organised. The Complainant and his family were not aware that the Local Council was taking photos, believing that only members of the public in attendance were doing so.

The Complainant became aware that he and his family's photo had been taken and then used only when the Local Council distributed a publication within the municipality which had the family's image on the front cover.

Initial attempts to resolve the complaint within the Local Council were unsuccessful; with the Local Council asserting it had not breached the (Commonwealth) National Privacy Principles in its formal response to the Complainant. Misquoting the relevant privacy principles further upset the Complainant, who then made a formal complaint to Privacy Victoria.

In response to the complaint, the Local Council conceded the need to better manage the collection and use of images within its database of photos and agreed to participate in conciliation. The matter was successfully conciliated in no small part due to the attentive, empathic and genuine acknowledgement of the Complainant's concerns by the Local Council representative.

See [Complainant AM v Local Council \[2009\] VPrivCmr2](#) at www.privacy.vic.gov.au ■

to the use of surveillance and data collection powers as necessary conditions for the exercise of individual freedom and liberty. Privacy and executive and legislative restraint should be taken into account at all times by the executive, government agencies, and public bodies." (paragraphs 144, 452).

The report encompasses a broad overview of surveillance and data collection, an analysis of the advantages and disadvantages of surveillance, an examination of existing legal regulation and safeguards and the roles of current regulators, government, the Parliament and citizens. The Committee made a wide range of recommendations, including that:

- Before introducing any new surveillance measure, the government should endeavour to establish its likely effect on public trust and the consequences for public compliance
- The government should consider expanding the remit of the UK Information Commissioner to include responsibility for monitoring the effect of surveillance practices on the rights of the public
- The government should amend the provisions of the *UK Data Protection Act 1998* (UK) so as to make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment prior to the adoption of new surveillance, data collection or processing scheme, including data sharing. ■

Canadian Court Rulings on Privacy

Two recent court cases in Canada highlight the need for people using online services to carefully read Terms and Conditions. The *Toronto Star* (March 16) [reported](#) on two cases where Ontario courts had permitted the disclosure of personal information by private companies to law enforcement agencies. This was on the basis that customers had agreed to the possibility of the private companies doing so when they accepted the service's Terms and Conditions. "...these cases provide an important reminder about the limits of Canadian privacy law, which invariably leaves privacy subject to policies that subscribers rarely bother to read" the *Star* said.

In a separate case, the [Alberta Court of Queen's Bench](#) upheld a ruling from Alberta's privacy commissioner that ordered a Calgary nightclub to stop scanning driver's licences before allowing people inside. While the ruling only applies to one particular nightclub, the report says that the Alberta Information and Privacy Commissioner would view the ruling as a precedent for any future complaints. In her judgment, Justice Carolyn Philips found that the collection of personal information was unreasonable, as the nightclub had failed to produce any evidence that it contributed to reducing violence or unlawful behaviour by the club's patrons. ■

Privacy and Human Resource Management

David Taylor, Director Privacy Awareness

The relationships between Privacy and Human Management were explored during the March meeting of the Privacy Victoria Meeting in Melbourne.

Susan Heron, CEO of the Australian Institute of Management (Victoria/Tasmania) spoke from a business perspective. She described how Human Resource managers were the “people experts”, charged with being the authority on all matters that an organisation needs to know and do that are part of managing the most critical resource of any organisation—its people. At its most fundamental, HR must ensure that the appropriate privacy laws are applied from the point of a person’s job application until they leave the company and thereafter.

HR managers also must know what can and cannot be communicated outside the company in relation to matters such as workers’ compensation, superannuation, payroll and state and federal taxation. At this point, they are the delegated office of the company with all the authority and risk that such a position implies. If they get it wrong, the company is exposed.

Ms Heron made the point that because of the new capability requirements placed on

HR, it must take a leadership role when dealing with privacy laws. HR needs to liaise effectively with top level internal stakeholders such as Board members, CEO, Chief Financial Officer and the Chief Information Officer, who all have to understand how the company deals with privacy—it is not just technology.

George Karaisaridis from WorkSafe Victoria described the workers’ compensation process, including the great variety of people who may need to access an injured worker’s personal information. Privacy laws do not prevent WorkSafe and its Agents perform their statutory functions to provide just and fair compensation and a range of entitlements and benefits to injured workers. WorkSafe and its Agents are subject to stricter confidentiality and secrecy provisions. If there is an inconsistency between a provision of privacy legislation and the *Accident Compensation Act 1985* (ACA), the provision in the ACA prevails to the extent of the inconsistency (s6, *Information Privacy Act*).

Matthew Smith, from Accenture HR Services, a Victorian government contracted service provider, described

the full range of personal information collected, handled, used and disclosed during the HR process as well as some common privacy issues facing HR practitioners. These included:

- Requests from an employee’s manager to receive the employee’s personal contact details;
- Requests from third parties (such as banks, real estate agents) for personal information such as employment history and salary details;
- Confidential discussions between HR and an employee where an employee discloses details about a medical condition, which if left unmanaged, could pose a risk to the health and safety of that employee or others
- A request from another prospective employer about a current or former employee’s work performance and history;
- Online employment applications—how much data is collected and why is it required, how long is it kept for?; and
- Recruitment selection reports—demonstrating merit in the recruitment process without breaching privacy—de-identify other applicants.

In addressing these issues, Mr Smith stated that it is essential that HR staff remember that *purpose must govern use*—the reason that you collect information must govern the way in which you use the information.

Copies of these presentations are [available](http://www.privacy.vic.gov.au) at www.privacy.vic.gov.au. ■

Be Aware

Privacy Aware is published four times a year by the Office of the Victorian Privacy Commissioner. The material in Privacy Aware is intended only to inform. It should not be relied on as legal advice. Material is compressed and simplified for newsletter purposes and should not create expectations about how the Privacy Commissioner may deal with any specific matter in particular circumstances under the *Information Privacy Act 2000 (Vic)*. Privacy Victoria accepts no liability for loss or damage that may be suffered by any person or entity that relies on information in this newsletter.

Copyright held by the Office of the Victorian Privacy Commissioner unless otherwise indicated. Permission to reproduce work of others should be separately sought.

One of the purposes of this newsletter is to increase public access to information about privacy. Articles in which the Office of the Victorian Privacy Commissioner holds copyright may be copied for non-commercial use. The material should be used fairly and accurately and Privacy Aware should be acknowledged as the source. The authors of material, where known, should be credited, consistent with moral rights provisions of copyright law.

GPO Box 5057
Melbourne Victoria 3001
Australia
DX 210643 Melbourne

Level 11, 10-16 Queen Street
Melbourne Victoria 3000
Australia

Local telephone 1300 666 444
Local fax 1300 666 445

www.privacy.vic.gov.au
enquiries@privacy.vic.gov.au

