



## October 2006 Lunchtime Seminar Series

### Presented by:

Geoff Code, Principal Solicitor  
Lindy Smith, Solicitor  
Helen Versey, Acting Privacy  
Commissioner

## Privacy: Avoiding the Pitfalls

### Part 1: Privacy and Confidentiality (Geoff Code)

Privacy is conceptually difficult to define. It is often said that there are four types of privacy interest – territorial privacy (eg limiting intrusions into homes or workplaces), personal or bodily privacy (eg protection from invasive procedures), communications privacy (eg privacy of mail and phones) and information privacy (eg privacy of information about individuals). The *Information Privacy Act 2000* (the *IP Act*), of course, creates an information privacy regime for the Victorian public sector and some of its contractors and provides individuals with remedies for breaches in relation to the privacy principles in the *IP Act*.

The state of the law in Victoria and Australia generally reflects the difficulty acknowledged by legislators and courts of identifying what is truly private and how to protect what is truly private. Legislatures in Australia and elsewhere have enacted privacy laws as particular needs arise, and have been active in the area of information privacy. At common law, the High Court is yet to recognise a

general tort of breach of privacy, although the Court has accepted that many forms of privacy invasion are actionable at general law,<sup>1</sup> and most commentators consider the Court has not closed the door to a tort.

The pitfall that I wish to briefly address today is knowing when a disclosure of personal information is subject to the *IP Act* regime or, alternatively, when it may be a breach of confidentiality. Briefly, there is an equitable principle that the courts will restrain the publication of information imparted in confidence which ought not to be divulged. Relief may be provided even if there is no breach of contract, fiduciary duty or other right. There must be a quality of confidence and confidentiality must be of substantial concern to a plaintiff. Confidential (or private) information may sometimes not involve personal information. Information privacy under the *IP Act* is a different concept because, among other things, it authorises use and disclosure of personal information for the primary purpose for which it was collected and in other limited circumstances. It also imposes other data handling standards.

In 2004, the UK House of Lords considered whether supermodel Naomi

This topic was the subject of the monthly VGSO lunchtime seminar held on 26 October 2006. These notes are published with the permission of the presenters, Geoff Code, Principal Solicitor, Lindy Smith, Solicitor, Helen Versey, Acting Privacy Commissioner. The notes are not to be regarded as legal advice.

Campbell's privacy was interfered with after the print media published photographs and stories about her drug rehabilitation treatment.<sup>2</sup> The Court considered the UK *Human Rights Act 1988*, which had introduced the *European Convention for the Protection of Human Rights and Fundamental Freedoms* into UK law. Although the Court accepted that the Convention requires the law to protect privacy of individuals, it did not propose that it be protected by a tort. I mention this case mainly because the Court dealt with it as an alleged breach of confidentiality.

The Victorian *Charter of Human Rights and Responsibilities Act 2006* creates a human right to not have one's privacy unlawfully or arbitrarily interfered with. The right goes wider than information privacy. It appears that compliance will require officers to take a broad approach to privacy in preparing programs and legislative proposals.

The Naomi Campbell case is convenient to my objective today, because it helps introduce a recent Supreme Court case about a breach of confidentiality in a similar context of celebrities (AFL footballers), their drug use and media interest.

In *AFL v The Age Company Pty Ltd*,<sup>3</sup> the AFL sought injunctions preventing publication of the names of three footballers who were said to have twice tested positive under the AFL's illicit drugs policy.<sup>4</sup> That policy prohibits use of cocaine, amphetamines, cannabis and, if there is no therapeutic use, heroin and other similar drugs. Under that policy, the first two positive tests are confidential between the player, the AFL medical officers and the testing agency. A third positive test results in publicity and the imposition of a penalty by the Tribunal.

*The Age* argued, in support of publication, that the information was no longer private and had passed into the public domain; that the existence of wrong doing by the players made the information no longer private; and that the public interest in publication outweighed the private nature of the information. I want to refer only to the first of these three arguments.

The Court examined various examples of claimed public dissemination of the players' names. The main one was that the players had been named by anonymous participants in unofficial internet chat rooms relating to football on a number of occasions. The others related to an article in a Sydney newspaper that was removed before publication but was forwarded in electronic form by Media Monitors to many of its clients; the naming of one player by a caller on a pay TV football program; and discussion between AFL officials and some members of the media. The court dismissed these other examples as not being sufficiently disseminated to the public at large.

The Court looked at the chat room threads in detail and found most of it was anonymous gossip and speculation. Unlike a newspaper, there was no accountability in dissemination in a chat room. It observed that an unethical publisher could anonymously seek to pass private information into the public domain in a chat room. The Court agreed with the High Court's observation, in *Dow Jones & Company v Gutnick*,<sup>5</sup> that although the internet throws up many challenges for established principles of common law, it does not mean the internet should be a 'law free zone'.<sup>6</sup> The Court found that the dissemination of the players' names in the chat room did not destroy the confidential or private nature of the test results. The

Court ultimately permanently restrained the publication of the players' names.

How does this case relate to current privacy statutes? The private information was clearly personal information within the meaning of the *IP Act*. It may have also included health information within the meaning of the *Health Records Act 2001* (the HR Act). However, it did not involve handling of the information by a Victorian public sector agency or any of its contractors, so the players had no cause of action under the *IP Act*. The private sector is subject to the information privacy regime in the *Privacy Act 1988* (Cth), but the press enjoy a journalism exemption if there is compliance with industry self-regulation. So, the players' would have been unlikely to bring an action against *The Age* if the names had been published. Other and more difficult questions would have applied if action was considered in relation to the participants to the chat room and its organizers.

The AFL case illustrates the need for care with electronic communications. We all know emails are documents for FOI and court discovery purposes. What may be said anonymously in chat rooms may have legal consequences. It shows that those of you who use internet/intranet discussion forums as a means of staff communication should take care, especially with confidential or personal information.

The US Congressman from Florida who recently resigned over salacious but, on-its-face, anonymous chat room discussion with adolescent Congressional work experience students should have taken care. Partly due to that chat room evidence, he is now likely to face criminal charges.

## **Part 2: The Surveillance Devices (Workplace Privacy) Act 2006 (Lindy Smith)**

### *Overview of the new law*

Legislation passed in September this year to amend the *Surveillance Devices Act 1999* (Vic) (*Surveillance Devices Act*) will tighten privacy safeguards at the workplace.

The *Surveillance Devices (Workplace Privacy) Act 2006* inserts a new Part 2A on workplace privacy into the *Surveillance Devices Act* that restricts the use of optical surveillance and listening devices by employers.

From 1 July 2007, when the new legislation comes into operation, it will be an offence for an employer to knowingly install, use or maintain an optical surveillance device or listening device to observe, listen to, record or monitor the activities or conversations of a worker in a toilet, washroom, change room or lactation room in the workplace unless authorised to do so under law.<sup>7</sup>

For a natural person, the penalty for the offence is up to level 7 imprisonment (2 years) or a level 7 fine (240 penalty units). For any other entity, the penalty is 1,200 penalty units.<sup>8</sup> Where the offence is committed by a partnership or unincorporated body, each individual member is liable.<sup>9</sup>

The new legislation applies to all employers, whether in the public sector or the private sector, and organisations that engage people on a voluntary basis. It protects the privacy of any person employed or engaged in almost any capacity - contractors, apprentices, volunteers, interns, people working on commission, and anyone employed under

the *Public Administration Act 2004* or any other Act.<sup>10</sup>

The only workers excluded from the protection of the new safeguards are people who are employed or engaged to perform services in connection with their employer's family or domestic affairs.

However, the prohibition is not absolute. Optical surveillance and listening devices that monitor workers while using the toilet, showering, changing their clothes or breast feeding their babies can be installed and used if done in accordance with a warrant or emergency authorisation, a Commonwealth law, or if required by a condition on a licence granted under the *Liquor Control Reform Act 1998*.<sup>11</sup>

In this way, the legislation attempts to respect privacy yet also recognise the interests of employers and the wider community in preventing and combating illegal activity. An employer who suspects that illegal activity is being undertaken at the workplace can seek police assistance to conduct surveillance under a warrant or emergency authorisation issued under Part 4 of the *Surveillance Devices Act*.<sup>12</sup> Victorian law enforcement agencies can of course initiate a request for a warrant or emergency authorisation under the same provisions or, if investigating a Commonwealth matter or undertaking a joint investigation, under the Commonwealth *Surveillance Devices Act 2004*.

The exception under the *Liquor Control Reform Act* reflects the fact that liquor licences may require surveillance to be installed anywhere in high risk licensed venues to protect staff and customers and combat problems arising from drug and alcohol abuse.

Information obtained under any of the exceptions to the general prohibition may be

communicated or published only in accordance with the exception. Failure to comply with this requirement is an offence that attracts the same level of penalties as for the unlawful use of optical surveillance and listening devices.<sup>13</sup> In addition, law enforcement agencies remain responsible, as they always have under the *Surveillance Devices Act*, for keeping the information they collect in this way secure and for destroying it if it is not likely to be required for law enforcement purposes.<sup>14</sup>

### Background

Since 1999, all Victorians have been protected from intrusion to some degree by the *Surveillance Devices Act*. It is an offence under that Act for a person who is not a party to the conversation or activity to use a listening device to record a 'private conversation,' or an optical surveillance device to observe or record a 'private activity,' without the express or complied consent of each party.<sup>15</sup>

There are further exceptions where the surveillance is authorised by a warrant or emergency authorisation or a Commonwealth law.<sup>16</sup> In addition, an occupier of the premises can authorise a law enforcement agency to install optical surveillance where reasonably necessary for the protection of any person's lawful interests.<sup>17</sup>

A 'private conversation' occurs in circumstances that indicate that the parties to it desire and reasonably expect to be heard only by themselves.<sup>18</sup> Similarly, a 'private activity' is one carried out inside a building in circumstances that indicate that the parties to it desire and reasonably expect to be observed only by themselves.<sup>19</sup>

The degree to which the *Surveillance Devices Act* protects workers is limited. First, most activities and conversations in the workplace do not fall within the definition of ‘private conversation’ or ‘private activity’. Second, the exception that permits surveillance with the implied or express consent of the parties to the conversation or activity is not a realistic safeguard in an employment relationship where the employee is effectively unable to withhold consent.

In the course of investigating the adequacy of laws affecting workers’ privacy, the Victorian Law Reform Commission identified the need to upgrade privacy safeguards at the workplace.

The Commission found that existing laws fail to provide a fair balance between employers’ interests and workers’ privacy. It concluded that stricter controls should apply in some cases and, in other circumstances, certain activities should be prohibited altogether. Among the activities that it argued should be prohibited is surveillance in private areas of the workplace.

Observing that all members of the community have a particularly high expectation of privacy in private areas such as toilets and bathrooms, the Commission argued that placing workers under surveillance in these places would have an unacceptable impact on their dignity and autonomy.

In its final report, released in October 2005, it recommended that ‘an employer should be prohibited from using any device to observe, listen to, record or monitor the activities, conversations or movements of a worker in toilets change rooms, lactations rooms, wash rooms or in any other prescribed circumstances.’<sup>20</sup>

The *Surveillance Devices (Workplace Privacy) Act* implements this recommendation.

### Other surveillance

The original, less restrictive, safeguards on the use of optical surveillance and listening devices will continue to apply if ‘private activities’ and ‘private conversations’ are monitored in circumstances other than those specifically addressed in the new legislation. For example, the original provisions will apply to any use of surveillance devices to monitor domestic workers and in the event that devices are installed in private areas of the workplace without the employer’s permission or knowledge.

Even where the activities and conversations being monitored by a public sector organisation do not fall within the definition of either ‘private activity’ or ‘private conversation’, the collection of information may still be regulated by the *Information Privacy Act 2000*. Information Privacy Principles 1.1 and 1.2 require organisations to collect personal information only if necessary, by lawful and fair means, and not in an unreasonably intrusive way.

Furthermore, from 1 January 2008, public sector organisations will also need to consider the impact of their actions on the right to privacy, as set out in the *Charter of Human Rights and Responsibilities Act 2006*: a person has the right not to have his or her privacy, home or correspondence unlawfully or arbitrarily interfered with and the right not to have his or her reputation unlawfully attacked.<sup>21</sup> After that date, it will be unlawful for a public authority to act in a way that is incompatible with a human right or, in

making a decision, to fail to give proper consideration to a human right.<sup>22</sup>

Private sector organisations undertaking surveillance that is not regulated by the *Surveillance Devices Act* or by contractual arrangements with a Victorian public sector organisation may have to comply with the *Privacy Act 1988* (Cth). The *Privacy Act* contains information privacy principles for the collection of personal information that are similar to those found in Victorian privacy legislation. However, businesses with an annual turnover of less than \$3 million are generally exempt, and the *Privacy Act* does not apply to the handling of employee records.

### **Possible further regulation**

The Victorian Law Reform Commission made 65 recommendations, including that all workplace privacy matters should be regulated by a new *Workplace Privacy Act*. The Victorian Government has stated that the *Surveillance Devices (Workplace Privacy) Act* is the ‘first stage in developing a more comprehensive regime to protect privacy in the workplace’.<sup>23</sup> There are certainly many more aspects of workplace privacy that may need to be regulated, such as other forms of surveillance and drug testing.

Meanwhile, an officers’ working group of the Standing Committee of Attorneys General (SCAG) is considering issues of workplace privacy and consistency in privacy regulation.<sup>24</sup> The Victorian Government has said that if SCAG cannot agree on a nationally consistent approach, it will ‘consider how best to protect the privacy of Victorian workers’.<sup>25</sup> This could mean acting alone.

Further regulation of the use of optical surveillance devices is possible as a result of the deliberations of another SCAG working group, chaired by Victoria, which is

examining the unauthorised use of photographs on the internet. The working group called for public submissions last year but a final report has not been issued.

At the same time, the Victorian Law Reform Commission has commenced investigations into whether law reform is necessary to ensure that surveillance in public places and the publication of photographs without consent are appropriately controlled. A consultation paper is to be released in 2007.

Victorian laws that protect privacy may also be reformed as a result of an inquiry currently being undertaken by the Australian Law Reform Commission into the extent to which the *Privacy Act* and related laws continue to provide an effective framework for the protection of privacy in Australia. The terms of reference extend to consideration of the privacy laws and regimes in all jurisdictions. An issues paper has recently been released and the final report is due in 2008.

As there are likely further changes to legislation which affect the way in which government agencies gather and handle personal information, it is important to conduct a privacy impact assessment when considering how to apply new technology to workplace practices. This helps to identify the possible risks to privacy, looking beyond compliance with existing privacy legislation. Even if there is no specific law against the proposed new methods or technology, it might still be open to challenge under the *Charter of Human Rights and Responsibility Act* for being incompatible with a human right.

### **Part 3: Information Privacy Act 2000 (Helen Versey)**

#### ***Introduction***

In the time available I will not be able to cover all aspects of the *Information Privacy Act 2000* (the IPA) or the Information Privacy Principles (IPPs) or provide you with all the answers. My focus is going to be on data security, with reference to compliance notices and complaint handling.

In a digital age - collecting storing, modifying, linking and sharing information is so much easier and faster. Technology, and with it the ability of government to share information that it collects about citizens, has great benefits. But it also carries great risks. The more information that is accumulated in one place the greater the risks. When information is shared and matched data quality can be an issue, either because of a mismatch, or when some of the information is inaccurate and is matched to accurate data, tainting it. But one of the biggest risks is data security.

Part of the rationale for the introduction of the IPA was to address community concerns about the implications new technologies have for privacy and security.

As the Minister for State and Regional Development said in the 2<sup>nd</sup> Reading speech to the *Information Privacy Bill*:

‘...governments should not, on the one hand, champion the benefits of electronic commerce and develop an increasing range of online public services and, on the other, offer no new protection in that environment. Similarly, governments should not urge consumers and businesses to embrace new technology and

electronic commerce and ignore the dangers that also attend their use’.<sup>26</sup>

Information Privacy Principle (IPP) 4 requires organisations to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

Failure to attend to data security can cause embarrassing, expensive and sometimes fatal consequences.

The 1989 murder in the US of actress Rebecca Schaeffer occurred because in spite of her having an unlisted telephone number and address a stalker tracked her down through the state motor vehicle records. One of the early conciliations in our office included payment of compensation of \$25,000 after a government body had disclosed the complainant’s new name and address to her violent ex-partner.<sup>27</sup> It was reported in the NY Times 29 June 2006 that a laptop taken home by employee of the Department of Veteran Affairs was stolen from home and contained personal information including date of birth and social security number of 26.5 million veterans and active service personnel (later modified to 17.5). Last year it was reported that for \$20 a person purchased a laptop formerly the property of the NSW Transit Authority containing payroll and financial information of employees, their access and employee numbers and passenger information including correspondence with the broadcaster Alan Jones.

Part 5 of the *Information Privacy Act 2000* (the IPA) gives individuals the right to complain about a breach of one or more of the IPPs to the Privacy Commissioner. If a complaint is not conciliated the matter can

be referred to the Victorian Civil and Administrative Tribunal (VCAT). If VCAT upholds the complaint it can amongst other orders, order an organisation to pay compensation up to \$100,000.

Part 6 provides that the Privacy Commissioner can serve on an organisation a compliance notice for a serious or flagrant breach of one or more of the IPPs. Compliance notices are enforceable and penalties apply for failure to comply.

In his term Paul Chadwick served a total of three compliance notices. These were on the Office of Police Integrity, Victoria Police and the Department of Justice. It is not without significance that all three were as a result of a serious breach of IPP 4 - data security.

#### *‘Jenny’s case’*

Some of you may recall that there was a great deal of media attention in August 2005 when a lady who called herself ‘Jenny’ (not her real name) appeared on the ABC *Stateline* program telling of how she had made a complaint to the Office of Police Integrity (OPI) about alleged unauthorised access of her personal information retained in the Victoria Police Law Enforcement Assistance Program (LEAP) database by her husband’s ex wife, who was a police officer, and other persons on behalf of the ex wife. On completion of its investigation into her complaint OPI inadvertently sent its own files containing correspondence and hundreds of pages of LEAP data to Jenny. The LEAP data were the fruits of an audit conducted by Victoria Police’s contracted service providers. The audit contained sensitive information about persons with a name the same or similar to Jenny and her husband.

Jenny did not return the files to OPI. Instead she delivered them to the Shadow Minister for Police who gave access to them to two

journalists. They were returned to OPI several weeks later. OPI was unaware they were missing until contacted by a journalist for *Stateline*.

The Privacy Commissioner investigated the matter under Part 6 and concluded a serious breach of IPP 4 had occurred. He found that the matters that had contributed to the breach were:

- No location tracking of paper files;
- Inadequate electronic case management system;
- Informal and inconsistent means of receiving and dispatching correspondence;
- Lack of written procedures for records management; and
- Poor audit trails for key processes.

However, he also found that the breach had to be considered in the light of the fact that at the time OPI was newly created and had inherited much from the old Ombudsman’s office procedures. By the time the Privacy Commissioner had concluded his investigation and published his report most of these matters of concern were being addressed. Hence the compliance notice did not require any specific action save for OPI to submit to an independent audit at its own expense after a 12 month period.

One of the aspects of the serious breach that had occurred was that the fruits of the audit had resulted in a large amount of LEAP data being sent to Jenny without anyone realising. The Privacy Commissioner’s report also deals with this aspect. It identifies that one of the problems was that the audit carried out to ascertain who may have accessed Jenny’s

personal information had resulted in masses of information about other people being generated. This was exactly one of the problems that resulted in the second Part 6 investigation.

### *Mr C's Case*

Mr C's case involved the release by Victoria Police of a large amount of personal information from the LEAP data base to employees of the Department of Justice.

Mr C was an employee of Corrections Victoria who became concerned that there had been unauthorised access to his personal information held on the LEAP data base and that it may have circulated in the prison system, putting him in danger. As a result of persistent complaints from him about this matter the Department requested Victoria Police to carry out an audit of persons who had accessed Mr C's LEAP data.

The results of the audit, if printed out, amounted to some 7,000 pages of A4. As a result of considerable pressure by Mr C, Victoria Police authorised its contracted service provider to forward the results of the audit to Mr C and the person in the Department who had requested the audit. The results were sent by unencrypted email to Mr C and a manager at the Department. Mr C promptly transferred the files to his personal e-mail so he could look through them at leisure. The audit involved personal information (including sensitive information) of about 291 individuals who had a name the same or similar to Mr C.

When Victoria Police realised the extent of the disclosure the officers involved took steps to retrieve the information, as did the Department.

Part of the Privacy Commissioner's investigation of the data security of LEAP necessarily involved the Department of

Justice. The Department is one of the external recipients LEAP data through E\*Justice system. The investigation revealed that there had already been some data security problems in E\*Justice system when it started receiving LEAP information. There were a number of instances of unauthorised access revealed by the Department's own investigation into the Mr C matter.

Findings of the Privacy Commissioner in relation to Victoria Police included:

- Inadequate procedures relating to the conduct of LEAP audits;
- The need for clear lines of authority for the conduct of LEAP audits, especially where requested by an external agency;
- The need for an update of the security and audit capacity of LEAP;
- The need to reduce paper print-outs of LEAP audits; and
- Inadequate training of personnel in internal procedures.

Findings regarding the Department of Justice included:

- Inadequate procedures to protect LEAP data in E\*justice system, including lack of ability to audit use;
- No Memorandum of Understanding in place between the Department and Victoria Police regarding the access to LEAP data through E\*Justice system;
- The need for training of personnel who have access to LEAP data through the E\*Justice system; and

- The need for the capacity to act swiftly to contain a breach if it occurs.

The Privacy Commissioner concluded that the identified inadequacies in both cases amounted to a serious breach of IPP 4.

In both cases the Privacy Commissioner also found that the organisations were already addressing the issues that he had identified as contributing to serious breaches of IPP 4. The compliance notices served on the organisations recognised this.

### ***Lessons learned from the Part 6 investigations***

There were common themes from the Part 6 investigations. These provide useful lessons for all organisations. The common themes were:

- Lack of internal procedures and training;
- Poor audit function to detect possible unauthorised access to the information held on the systems; and
- Lack of procedures to deal with a breach of security when it occurs so as to minimise the harm.

### ***Prevention and containment***

It is important to understand that technology which allows for sharing and amassing of personal information creates a 'honey-pot'. The more data you have in one place, the more attractive it is and the more vulnerable. Therefore you need to have better security to protect it, both from human error and human weakness.

The lessons learned from other privacy breaches and investigations both nationally and internationally are that the richer the data and the more people have access, the more

vulnerable it is to unauthorised access by staff out of curiosity, financial gain and, in the worst case, corruption.

Whether building a new system that records personal information or managing an existing one there are some basic matters data security that need to be addressed:

- Think about what personal information you need to collect to achieve your object. The less personal information you hold about identifiable individuals, the less risk of something going wrong. Necessity is a key under the collection principle (IPP 1).
- Have clear procedures for access control. Who needs access to the information and to how much? Can you have layered access? How can you audit access? Is it easy? Will the users know that unauthorised use is more likely than not going to be detected?
- Have written procedures and policies in place.
- Ensure staff are properly trained and understand lines of authority and procedures.
- Have procedures in place to contain a breach quickly if it occurs. How quickly can you move? Remember that if information goes into cyberspace it is difficult to retrieve and in some cases may be impossible. In *Complainant AD & others v the Department 2006* VPriv Cmr 5<sup>28</sup> human error resulted in names, telephone numbers, addresses and e-mail addresses being posted on the organisation's website.

Although the organisation moved swiftly to remove the personal information from the website when the mistake was discovered the search engines had already picked it up. A Google search on a name and postcode easily revealed the information. The organisation experienced great difficulty in having the information removed from the Google archives to prevent further disclosures.

### ***Privacy Impact Assessments (PIAs)***

Conducting PIAs at the very beginning, and making them ongoing, will help you identify the potential risks and address them. Note that IT experts also need to be involved. A mixture of the technical experts who can provide the security solutions and those that understand the privacy aspects will produce the best results.

### ***Notification of a breach***

In both compliance cases discussed above the Privacy Commissioner decided that even though hundreds of other peoples' personal information had been disclosed they should not be told. The test he used was "not reasonably likely that notification would alleviate more harm that it would cause".

In both cases he found:

- The extent of disclosure was very limited and he had received assurances (in some cases under oath) that the information had not been copied or further disseminated;
- The data had been retrieved and secured;
- The names were the same or similar to the complainants whose names had never been disclosed to public;

- It was likely that attempts to notify would fail in many cases because the data was out of date; and
- Even if notification was successful the nature of information had potential to do harm to persons informed (eg distress caused to victims of crime).

However there may be many instances where it is appropriate to inform persons of the breach. For instance if the information is disseminated widely and there is potential for serious harm to some of those whose information is disclosed. If a person discovers their information has been disclosed from sources other than the organisation involved this may reduce the potential to resolve quickly any resulting complaints.

### ***Handling a privacy complaint***

Most organisations have internal complaint handling procedures. Good complaint handling procedures for privacy complaints are important. They may avoid a complaint to the Privacy Commissioner.

Our office has an internal policy of referring enquirers to the appropriate privacy officer if the enquirer has not already raised his/her concerns direct with the organisation, unless there is a reason why the complainant should not deal direct with the agency in the first instance. In our 2005/6 Annual report we reported that 213 potential complainants had been redirected and did not come back with formal complaints.

Section 29(1)(c) of the IPA provides that the Privacy Commissioner may decline to entertain a complaint if an organisation has not had an opportunity to deal with a complaint. Note the requirement to

complain to the organisation first is not mandatory, unlike section 40(1A) of the federal *Privacy Act* which expressly states that the Privacy Commissioner must not investigate a complaint unless a complainant has given the organisation an opportunity to deal with the complaint, unless the Commissioner considers it is not appropriate for the complainant to do so.

Section 29(h) of the IPA allows the Privacy Commissioner to decline to entertain a complaint if an organisation is dealing or has adequately dealt with a complaint. Thus having effective internal procedures in place can enable the Commissioner conclude that a complaint is being adequately dealt with.

### ***Lessons learned***

Often when complainants come to us after trying to resolve matters with the organisation first it is often the quality of the response they received that motivates them to take the matter further. Here are some of the lessons I have learned from complainants about what works and what doesn't for internal complaint handling:

- A prompt response. If they have taken the trouble to write to you complainants are furious if they hear nothing. Don't wait until you have investigated the complaint - make some contact. An acknowledgement of the complaint, an explanation of the internal process and an estimate of time will help. Note under the IPA one of the grounds on which the Privacy Commissioner may decline to entertain a complaint is if it was made 45 days after a complainant became aware of the alleged breach. But if the delay in complaining to the Commissioner is caused by the organisation the discretion will not be exercised.
- Complex procedures don't help. Why does a complaint have to be in writing? Part 5 of the IPA requires the Privacy Commissioner to take certain statutory steps such as requiring a complaint in writing but internal procedures do not need to be so formal.
- If it is immediately apparent there has been an unauthorised disclosure take action quickly to contain the breach. It might make a difference to the eventual outcome.
- If something has clearly gone wrong be prepared to say sorry quickly. One of the most common statements complainants make is that if the organisation had just said sorry straight away they would have been satisfied. The longer a matter drags on the less likely a simple solution will be found.
- Complainants often say they want to prevent the same thing happening to someone else. If something has gone wrong what can you do to prevent it happening again?
- Don't be too legal in your response - phrases like 'the complaint is not substantiated' don't help.
- Explain things in plain language – it is our experience that even where we decline a complaint if we explain why an organisation acted in a particular way it can help resolve a complaint, for example where a disclosure was authorised under law.
- Ask yourselves what has really prompted the complaint – sometimes it is nothing to do with privacy but everything to do with the treatment

of the complainant by the organisation.

- Be careful about being a judge in your own cause. Have you got someone truly independent handling the complaint?

### Complaints under Part 5 of the Act

An individual can make a complaint to the Privacy Commissioner independent of a compliance notice. Note also that an individual who was a complainant under Part 5 may request the Privacy Commissioner to serve a compliance notice.<sup>29</sup> This may be used, for example, where an organisation has undertaken to do certain things to improve its systems and prevent a recurrence and has failed to take the action promised.

A compliance notice can be served after five complaints about the same subject matter in two years as well as for a serious or flagrant breach.<sup>30</sup>

The Privacy Commissioner's role under Part 5 is essentially that of a conciliator. Unlike the Health Services Commissioner under the *Health Records Act 2001* (Vic) and the federal Privacy Commissioner under the federal *Privacy Act 1988* there is no power for the Privacy Commissioner to make a determination if conciliation fails.

Section 29(1) provides that the Privacy Commissioner may decline to entertain a complaint within 90 days of receiving it on certain specified grounds. It is in an organisation's interests to respond to notification of a complaint in timely way and provide as much relevant information as possible. If an organisation is so late responding that the Privacy Commissioner is unable to take into account matters relevant to his/her powers under s 29 a complaint may go to conciliation unnecessarily.

Whether the Privacy Commissioner declines to entertain a complaint, or conciliation of the complaint is not possible or fails, the complainant has the same right under the IPA - to request the matter be referred to the Victorian Civil and Administrative Tribunal.

### Interventions

The *Victorian Civil and Administrative Tribunal Act 1988* provides that the Privacy Commissioner may intervene at any time in a proceeding under the IPA and can apply to VCAT for interim injunction.<sup>31</sup> The Privacy Commissioner has never applied for an injunction. There has only been one intervention by the Privacy Commissioner.<sup>32</sup>

When considering whether the Privacy Commissioner should intervene in a complaint before VCAT the following are considered:

- The complaint raises issues that are of wider public interest than individual redress; and
- The complaint raises an issue that requires interpretation of the IPA.

Intervention is intended to assist the Tribunal, not provide legal representation of the complainant. It is considered that it should be regarded as a role of 'counsel assisting' in order to help build privacy law in Victoria.

### Conclusion

As I said in the introduction I cannot give you all the answers. And you are not going to avoid all the pitfalls. I hope that what I have said will help you avoid some. And that if things go wrong you have some tools to help you reduce the impact.

Staff at our office are always available to give assistance and guidance. Early consultation on projects which may have significant privacy implications may avoid future problems. If organisations raise issues with us then we can map where the difficulties lie in applying the IPPs. This informs us of the areas where we need to provide more guidance. Our website [www.privacy.vic.gov.au](http://www.privacy.vic.gov.au) contains all our published guidance material and details of our public sector training programs.

<sup>1</sup> *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63 (15 November 2001).

<sup>2</sup> *Campbell v MGN Ltd* [2004] UKHL 22.

<sup>3</sup> [2006] VSC 308 (30 August 2006), Kellam J.

<sup>4</sup> The AFL has a separate ‘anti-doping’ code with respect to banned performance enhancing drugs. The code was not in question in this case.

<sup>5</sup> [2002] HCA 56 (10 December 2002).

<sup>6</sup> *AFL v The Age Company Pty Ltd* [2006] VSC 308, [55]; *Dow Jones & Company v Gutnick* [2002] HCA 56, [55] (Kirby J).

<sup>7</sup> *Surveillance Devices Act 1999* (Surveillance Devices Act) s 9B, inserted by s 3 of the new legislation. Following references are to new sections in the *Surveillance Devices Act* that have been inserted by the *Surveillance Devices (Workplace Privacy) Act 2006*.

<sup>8</sup> s 9B(1).

<sup>9</sup> 9D.

<sup>10</sup> s A.

<sup>11</sup> s 9B(2).

<sup>12</sup> Provisions concerning the issue of warrants and emergency authorisations are contained in Part 4 of the *Surveillance Devices Act*.

<sup>13</sup> s 9C(1).

<sup>14</sup> s 36.

<sup>15</sup> ss 6(1), 7(1).

<sup>16</sup> ss 6(2), 7(2).

<sup>17</sup> s 7(2)(c).

<sup>18</sup> s 3.

<sup>19</sup> s 3.

<sup>20</sup> Victorian Law Reform Commission, *Workplace Privacy: Final Report* October 2005 p xxiv.

<sup>21</sup> *Charter of Human Rights and Responsibilities Act 2006*, s 13.

<sup>22</sup> *Charter of Human Rights and Responsibilities Act 2006*, s 38(1).

<sup>23</sup> Attorney-General, Second Reading Speech, *Surveillance Devices (Workplace Privacy) Bill*, Legislative Assembly, 9 August 2006, p 2661.

<sup>24</sup> SCAG is a national council comprising the Commonwealth Attorney-General and Minister for Justice and Customs, the State and Territory Attorney-General and the New Zealand Attorney-General Norfolk Island has observer status.

<sup>25</sup> *Ibid.*

<sup>26</sup> Parliamentary Debates (Hansard) Legislative Assembly 54<sup>th</sup> Parliament First session Book 8 p 1906.

<sup>27</sup> *Complainant B v Statutory Entity VPrivCmr*[2003]2 on

[www.privacy.vic.gov.au/casenotes](http://www.privacy.vic.gov.au/casenotes).

<sup>28</sup> Available on [www.privacy.vic.gov.au/casenotes](http://www.privacy.vic.gov.au/casenotes).

<sup>29</sup> S 44(5) Information Privacy Act 2000.

<sup>30</sup> S 44(1) above.

<sup>31</sup> Schedule 1 Part IIA *Victorian Civil and Administrative Tribunal Act 1988*.

<sup>32</sup> See *Smith v Victoria Police (General)* [2005] VCAT 654.