THE GOVERNANCE OF PRIVACY: SPEAK SOFTLY AND CARRY A BIG STICK

Dr Anthony Bendall*

Introduction

Speak softly and carry a big stick; you will go far

US President Theodore Roosevelt used this phrase on a number of occasions as a description of his foreign policy[1]. It refers to the 'Monroe doctrine' of the early years of the twentieth century, by which diplomatic and multi-lateral approaches were initially preferred, backed up by the existence of an extremely effective and large military force. However, the phrase coined by the late President could just as easily refer to the various functions of a privacy commissioner.

Charles Bennett and Charles Raab in their book *The Governance of Privacy*[2] identify a number of roles that traditionally characterise privacy and data protection authorities around the world. These are:

- ombudsman;
- auditor;
- consultant;
- educator;
- policy advisor;
- negotiator; and
- enforcer.

The functions of the Privacy Commissioner under the *Information Privacy Act 2000* (Vic) [IPA] embrace all these roles (as do the functions of the Federal Privacy Commissioner and other privacy regulators in the region and around the world).

This paper will examine these roles in the context of a regulator and the challenges posed by having to juggle the different roles, especially where they potentially conflict.

Although the paper is presented from the perspective of a (Deputy) Privacy Commissioner, the functions of the Privacy Commissioner under the Information Privacy Act mirror those of other regulators who face similar challenges.

In the words of Bennett and Raab[3]:

> …it has become more and more difficult to classify [privacy and] data protection agencies according to any one model. They each perform an intricate blend of functions that appear in various mixes, and with different emphases, in different regimes. Through these activities, the framework laid down in statute, reflecting the data protection [or privacy] principles, is fleshed out, bringing the regulatory body into contact with a large number of public and private bodies, and with the public as well.

* *Deputy Victorian Privacy Commissioner. Paper to the 2008 Australian Institute of Administrative Law National Forum, Melbourne, 8 August 2008*

The Victorian Privacy Commissioner is appointed under the IPA to administer the regime created by that Act for the collection and handling of personal information by the Victorian public sector[4]. Any discussion about the role of the Privacy Commissioner necessitates an understanding of the independence and accountability of the Commissioner within the public sector[5]. The IPA provides for the Privacy Commissioner to be independent of the public bodies she regulates in a number of ways. As will be seen when I discuss the functions of the Commissioner, this independence is critical to the successful operation of the IPA.

The Commissioner is appointed by the Governor in Council (s 50(1) IPA)) and has her salary and allowances determined by Governor in Council (s 51). There are specific provisions for the removal, suspension and resignation of the Commissioner (ss 53 and 54). Apart from some automatic removal provisions such as conviction for an indictable offence, the Commissioner may only be suspended by Governor in Council, but unless both Houses resolve the Commissioner be removed within 20 sitting days of suspension, she must be restored to office (s 54(4)).

The Commissioner is a separate employer under s 16 of the *Public Administration Act 2004* (Vic) and a department for the purposes of the *Financial Management Act 1994* (Vic). Under the Financial Management Act, the Commissioner is required to submit the Commissioner's financial statements for the financial year to the Auditor-General and to provide the Auditor-General with a report of the Commissioner's operations during the financial year[6]. In addition s 46(1) of the Financial Management Act requires the Commissioner to cause a report of operations and audited financial statements to be laid before both Houses of the Victorian Parliament.

Functions of the Commissioner

The functions of the Privacy Commissioner are extensive and are listed in s 58 of the IPA. There are 23 listed functions in all. These can be summarised as follows:

- to promote an understanding and acceptance of the ten Information Privacy Principles (IPPs) and their objects [function (a)];
- to assess and approve codes of practice submitted by public sector agencies, and
- to review and recommend, where necessary, amendment or revocation of approved codes of practice where necessary [functions (b), (c) and (w)];
- to issue guidelines to assist agencies as they respond to Freedom of Information requests, transfer personal information outside Victoria and develop their own privacy codes of practice [functions (d), (e) and (f)];
- to examine agencies and audit their records of personal information to ensure their records and practices are consistent with the IPPs or an approved code of practice [functions (g), (i), (j) and (t)];
- to receive complaints relating to alleged breaches of privacy by public sector agencies,
- and try to settle them through conciliation [function (h)];
- to gather information, monitor developments in data processing and computer technology and report on the adequacy of safeguards for users of technology in order to minimise any adverse effects of developments on personal privacy. [functions (k), (m) and (v)];
- to advise government on legislation and policies relating to issues of personal privacy [functions (l) and (n)];

- to promote privacy protection through awareness programs and public statements, by listening to the concerns of the public and by co-operating with other privacy watchdogs [functions (o), (p), (q), (r) and (s)];
- to make suggestions to any individual or organisation about action in the interests of personal privacy [function (u)];
- under Part 6 of the IPA, where serious or flagrant breach, or 5 breaches within 2 years issue a compliance notice that is enforceable [function (i)].

Under s 60 of the IPA the Commissioner must have regard to the objects of the IPA[7] when carrying out her functions and powers. The objects of the Act are:

- to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;
- to promote awareness of responsible personal information handling practices in the public sector;
- to promote responsible and transparent handling of personal information in the public sector.

There is one important function that the Victorian Privacy Commissioner does not have, unlike counterparts at the Federal level, in New South Wales and a number of other jurisdictions[8] – the power to make a public interest determination to modify any of the information Privacy Principles (IPPs) to enable information to be handled in a way that is inconsistent with the IPPs. The Privacy Commissioner's role is limited to enforcing the standards set by Parliament in the IPA.

Consideration will now be given to the powers and functions of privacy commissioners in general, and the Victorian Privacy Commissioner in particular, according to the seven roles described by Bennett & Raab[9].

Commissioner as ombudsman

All data protection or privacy commissioners are responsible for the receipt, investigation and resolution of complaints from individuals who believe their privacy has been breached or interfered with[10]. A traditional role of the ombudsman, the resolution of complaints is central to any effective oversight of personal information and privacy, even though it can also be time-consuming and a significant drain on resources. The system for complaints-handling needs careful consideration and the specification of powers necessary for this function to be performed. Although subject to variations across jurisdictions, these powers normally include the power to enter premises, to require records to be produced and to summon the appearance of relevant persons. One issue is whether or not the commissioner should be expressly empowered to conduct 'own motion' investigations in the absence of a complaint. Some offices have this power.

The Victorian Privacy Commissioner does not have this 'own motion' power, but can only receive written complaints from individuals that their privacy has been breached. A breach of privacy occurs when an organisation fails to comply with one or more of the IPPs when handling an individual's personal information. The definition of 'personal information' under the IPA[11] requires the information to be recorded information, and includes opinion, whether true or not. The individual concerned must be identifiable from the information, or his /her identity must reasonably be ascertained from the information. This can include matching with other information[12].

The Privacy Commissioner will only accept a matter as a formal complaint if on the face of it the complaint involves personal information within the meaning of the IPA and it appears to involve possible breach of one or more of the IPPs.

The Commissioner's complaint handling role is that of conciliator. She has no power to determine whether a breach has occurred. However, the Commissioner has a discretionary power to 'decline to entertain' a complaint under s 29 of the IPA. Section 29 lists the circumstances that the Commissioner can decline to entertain a complaint. These include:

- no interference with privacy;
- the complainant hasn't complained to the respondent;
- the respondent has dealt, is adequately dealing with the complaint, or hasn't had an opportunity to deal with it;
- the complaint was made 45 days after the complainant became aware of the alleged breach of privacy;
- the complaint is frivolous, vexatious, misconceived or lacking in substance;
- the subject matter of the complaint is, or has been adequately dealt with under another enactment.

The Commissioner must make a decision to decline to entertain the complaint within 90 days of receiving the complaint. If the decision is made to decline the complaint then notice of the decision and reasons for it, are served on the complainant and respondent. The complainant may then request in writing that the complaint be referred to the Victorian Civil and Administrative Tribunal for determination.

The decision that there has been no breach of privacy involves some assessment of the complaint. For example, when responding to a complaint of disclosure, an organisation may be able to demonstrate to the satisfaction of the Commissioner that the disclosure was permitted under IPP2.1. In that case the Commissioner may decline to entertain the complaint.

The Victorian Privacy Commissioner has published a number of case notes about complaints received, in a de-identified form. A number of these case notes are about complaints the Commissioner has declined to entertain. They can be found on the website, www.privacy.vic.gov.au and on www.worldlii.edu.au. They demonstrate how the Privacy Commissioner has applied the IPA and interpreted the IPPs.

If a complaint is not declined, but conciliation is not possible, or was attempted but unsuccessful, then the Commissioner gives notice to both parties to that effect and the complainant has the right to require the Commissioner to refer the matter to VCAT.

Although Part 5 of the IPA sets out the process for handling complaints, the approach of the office is to encourage conciliation at all stages. Complainants will always be encouraged to deal direct with a respondent organisation first, it they have not already done so. Early resolution – before consideration is given to the application of s 29 – is explored.

The Commissioner can also refer complaints to other bodies such as the Ombudsman, the Health Services Commissioner and the Federal Privacy Commissioner if it appears the matter will be dealt with more appropriately by another regulator.

As this process is basically one of conciliation, it requires the Commissioner and her staff to be scrupulously unbiased, fair and open minded in their approach to complainant and

respondent. The Commissioner's role is basically to facilitate resolution between the parties, rather than to make a determination that there has been a breach or to impose an outcome.

Commissioner as auditor

Complaint investigation and resolution are inherently reactive processes[13]. However, Commissioners may have concerns about the privacy and personal information handling practices of a particular organisation that arise from a number of sources, leading to the conduct of more general audits of the organisation or of a particular practice or technology. Audits are not only more systemic, but they may be less confrontational than an investigation into the circumstances of a specific complaint. Audits are a powerful tool for a regulator. They can be used when the regulator is on notice that an organisation's handling of personal information may fall short of standards required, but not so serious as to warrant enforcement action (see below). They can be used to scope how an organisation or sector is handling information in a particular situation and they can be used to review whether assurances given about the protection of privacy in relation to a particular project have been adhered to[14].

They are also an educative tool, for the regulator, the public, and the organisation. Results of an audit can identify issues and guide organisations. The first audit carried out by the Victorian Privacy Commissioner was on a sample of 100 public sector websites, including local councils. As a result of the audit, organisations audited had an opportunity to engage in a 'webinar' to discuss matters arising out of the audit, and the Privacy Commissioner published website guidelines[15] to assist the public sector to be compliant with the IPA. Two years later, a follow up audit was carried out which showed a marked improvement in compliance overall.

Again, this process requires the Commissioner to act fairly and in an unbiased manner. However, following such an audit, it is open to the Commissioner to make statements and recommendations about the adequacy of privacy practices in a particular organisation or sector. Indeed, such statements or recommendations are actively encouraged and expected by certain stakeholders (e.g. privacy and civil liberties advocates) For these reasons, this power needs to be exercised judiciously and with a great deal of discretion, balanced by a firmness of purpose.

Commissioner as consultant

With or without audit powers, commissioners also constantly give advice to regulated organisations on how to comply with privacy principles[16]. The implementation of privacy law is inherently as much a consultative effort as a regulatory one, regardless of legislative powers. Much can be achieved in anticipation of policy and system development if privacy protection is built in at the outset, rather than 'retrofitted' at the end. Consultation and advice are highly preferable to adversarial relationships between commissioner and regulated, where conflicts can be expensive and unproductive, given commissioners' mission to encourage privacy cultures in organisations and to educate those who handle personal information as much as to ensure formal compliance.

Thus, privacy commissioners expect to be consulted when new systems are being developed which have privacy implications. Organisations will often want to know, in advance of significant resource commitment, whether proposals are in compliance with applicable law. This consultative function tends to occur outside of public scrutiny, as often quite sensitive issues have to be addressed. Commissioners also need to be quite careful that their advice does not prejudice their independence if subsequent complaints arise about the organisation concerned.

The Victorian Privacy Commissioner may examine and assess the impact on privacy of any proposed act or practice of an organisation regulated by the IPA. This means that proposed policies and projects can be looked at and advice given as to any potential adverse impact on privacy. To assist in this process, organisations are encouraged to carry out Privacy Impact Assessments (PIAs)[17] on proposals at an early stage. PIAs identify privacy risks and give organisations the opportunity to address and minimise them. This in turn may minimise the risk of an unintended breach of the IPA in the future.

As this process requires a great deal of good will on both sides, it requires the Commissioner to act in some ways as a partner with the agency seeking consultation, without compromising her independence or being afraid to differ from the organisation where required. Given the confidential and often sensitive nature of the discussions, a great deal of discretion is also required.

Commissioner as educator

There is a fine line between advisory responsibilities – generally conducted in confidence – and the performance of broader educational, awareness raising and research roles[18]. The analysis of wider privacy and surveillance questions and the continuous education of regulated organisations and the general public can do much to anticipate problems and encourage citizens to protect their own privacy. Most commissioners are given this role, the interpretation of which varies from office to office.

To an increasing extent, many commissioners see their roles not only in relation to public policy, 'big issues' and 'big events', but also in encouraging a culture of privacy protection throughout society, the economy and government in an era of widespread adoption of new and privacy-invasive information technologies. Thus, resources are often invested in instilling an understanding of the rules, and a privacy culture, in more accessible ways than can be done through the interpretation and application of legal rules in particular cases.

Commissioners also devote considerable resources to producing guidelines and advice on paper and in electronic form, from public platforms and through the media. In addition, commissioners are expected to give frequent speeches and presentations concerning the importance of privacy. Moreover, some offices commission special studies relating to specific privacy issues and others occasionally sponsor public opinion surveys[19] The Victorian Privacy Commissioner has a range of functions to promote understanding and protection of personal privacy[20]

These functions require some degree of public and media profile on the part of the Commissioner, which can at times be seen to be in conflict with the impartiality and discretion required for some of the other functions discussed in this paper. For this reason, commissioners need to be extremely judicious in the way they promote a culture of privacy.

Commissioner as policy advisor

Most legislation imposes responsibilities on commissioners to comment on the privacy implications of proposed legislation[21]. The Victorian Privacy Commissioner has a function to provide advice to the Attorney-General on proposed legislation and the impact it may have on personal privacy. When passing the IPA, Parliament recognised the importance of a regulator assessing the impact on privacy of proposed legislation. It gave the Privacy Commissioner this function and extended the functions of the Scrutiny of Acts and Regulations Committee (SARC) to include consideration as to whether a proposed Act or Regulation unduly authorises acts or practices that might have an adverse impact on personal privacy within the meaning of the IPA[22]. The Privacy Commissioner has made a number of submissions to SARC resulting in an alert being issued on major legislation[23].

As can be readily seen, this advice function may well bring the Commissioner into conflict with the policies of the government of the day and the bureaucracy charged with implementing those policies. Sometimes she will be obliged to give unpalatable advice. But it is an important part of the checks and balances of the democratic process and underscores the need for the Commissioner to be independent.

High-profile legislative changes to that involve radical implications for the processing of personal information are often that circumstances under which consultation can be most important, but conversely most fraught. Commissioners also frequently make submissions and give evidence to legislative hearings and publish their responses to government policy documents where privacy interests are affected.[24] Media statements and interviews also provide vehicles for giving responses to issues as they arise.

Even where this function is exercised judiciously, it can to an extent undermine the cooperative relationship between the government and the commissioner, on which the role of consultant in particular is reliant. An overly aggressive or strident approach to policy advice and discussion of issues in the media could undermine the consultative process completely.

Section 40A of the *Victorian Civil and Administrative Tribunal Act 1998* (VCAT*)* gives the Privacy Commissioner the power to intervene at any time in a proceeding under the IPA. It is not a power that is subject to a grant of leave by VCAT. When deciding whether to exercise this power, the Privacy Commissioner generally considers whether the case meets certain criteria. These include:

- whether the case requires an interpretation of provisions of the IPA that would impact beyond the immediate facts of the case;
- whether the intervention would assist the development of privacy law in Victoria;
- whether there is a public interest involved beyond the particular facts of the case which warrant an intervention.

The Privacy Commissioner does not consider it is her role to intervene to support one party or the other. The role is considered to be one of 'counsel assisting' VCAT, in effect a policy or legal advisor to the Tribunal. Therefore she would not intervene in a case simply because she believed there had been a breach of privacy which a respondent was denying, unless the denial was based on an interpretation of the IPA which the Privacy Commissioner believed to be incorrect.

The Privacy Commissioner has only intervened in one matter referred to VCAT by the complainant. That is the case of *Smith v Victoria Police*[25]. Mr Smith was charged with a number of offences. While in police custody he was photographed by police. Photographs taken of persons in custody are commonly known as 'mug shots'. He subsequently pleaded guilty to a number of offences including two counts of rape and was imprisoned for a total of 10 years.

Victoria Police received a request under the *Freedom of Information Act 1982* (the FOI Act) for access to Mr Smith's 'mug shot' from a local newspaper writing a story about the case from the victim's perspective. Section 33 of the FOI Act provides documents that contain personal information be exempt where disclosure would unreasonably interfere with a person's privacy. It has provision for a person whose personal information is to be released to be given notice. He/she has the right to challenge a decision to release in VCAT. It is the precursor to privacy laws. Victoria Police did not follow that procedure. Rather, it released under s 16(2) of the FOI Act which states that the Act is not intended to prevent or

discourage access being given to documents (including exempt documents) where they can properly do so or are required by law.

Section 6(2) of the IPA provides that the provisions of the IPA give way to the operation of the FOI Act. On the facts of the case, it may well have been appropriate for Victoria Police to have released the mug shot. But there were wider issues to consider. Victoria Police, since the provisions of s 33 of the FOI Act had been enacted requiring individuals whose personal information was to be released to be given notice, and giving them the right to appeal to VCAT, had adopted a policy of using s 16(2) of the FOI Act where a person had pleaded guilty or been found guilty of an offence and the appeal period had passed. This deprived individuals whose personal information was involved the right of appeal to VCAT.

Victoria Police also relied on the partial exemption provided by s 13 of the IPA which allows a law enforcement agency not to comply with certain IPPs, including the use and disclosure provisions, if it believes on reasonable grounds that non-compliance is necessary for law enforcement functions or community policing functions[26]. This case, in terms of the wider public interest, involved the following:

- Did the application of s 16(2) of the FOI Act oust the jurisdiction of the IPA by virtue of s 6(2) of the IPA?
- Was the release of the photographs 'proper' within the meaning of s 16(2) of the FOI Act in the light of Victoria Police's obligations under the IPA?
- What is the proper application of the exemption provided by s 13 of the IPA?
- What does 'community policing' mean?
- Should Victoria Police generally have a policy of releasing 'mug shots' to the media after conviction and the appeal period is ended when such publication will result in the photograph remaining forever in the public domain?

The matters outlined above raised matters of considerable importance, both in the interpretation of the IPA and its interaction with the FOI Act, and matters of public interest as to whether 'mug shots' should routinely be released. It should be born in mind that 'mug shots' are taken compulsorily at a time when a person has been arrested and for minor offences as well as serious matters. The subsequent publication has the potential to do serious harm to the individual. It was not to the point that in this particular case the offences were extremely serious and publication may well have been justified. For all these reasons the then Privacy Commissioner considered that this was an appropriate case to exercise the right to intervene.

Again, the power to intervene in VCAT proceedings needs to be exercised judiciously and with scrupulous care against the possibility of advocacy on the part of either party, otherwise the other policy advice and consultant functions of the Commissioner could be fatally undermined.

Commissioner as negotiator

Some commissioners have responsibilities to negotiate privacy codes of practice[27]. Codes of practice have historically been instruments of self-regulation, although in Victoria and a number of other jurisdictions, including New South Wales, New Zealand and the Australian Commonwealth private sector jurisdiction, they must be made by a Minister in consultation with the commissioner and have the force of law.

Part 4 of the IPA provides a process that allows organisations regulated by the Act to substitute for one or more of the Information Privacy Principles (IPPs) with a Code of Practice approved by the Governor in Council. A code may modify any one or more of the IPPs, provided the standards in the code are at least as stringent as the standard set by the IPPs. The code can apply to a particular type of information, a particular class of organisations or a specific type of activity. The role of a code of practice may be to have a purpose built regime for a particular activity, where the IPPs, which are generic by nature, need to be adjusted to fit the activity. A code can also prescribe how a particular IPP applies to a particular situation.

An organisation seeking approval of a code of practice under Part 4 must first of all submit it to the Privacy Commissioner, who in turn may advise the Attorney-General to recommend to the Governor in Council to approve the code, provided that the code:

- is consistent with the objects of the IPA; and
- prescribes standards at least as stringent as the IPPs.

The Privacy Commissioner, before deciding whether to advise the Attorney to approve a code, may consult any person she considers appropriate and must have regard to the extent the public have been given the opportunity to comment on the proposed code. This is consistent with a code substituting for the IPPs and having the force of law insofar as it replaces them. Where Parliament has set standards in legislation it is appropriate that the public have the opportunity to comment on any proposed change to them. There have been no codes made under the IPA since it came into force in 2001.

Commissioner as enforcer

There is a clear distinction between the powers of commissioners to investigate and recommend and enforcement powers that can mandate changes in behaviour. Virtually all commissioners have the former type of powers and functions; only some (including the Victorian Privacy Commissioner) have the latter.

The more advisory approach is often preferred because it avoids the adversarial relationships that arise when enforcement powers are used or threatened[28]. However, the ability to negotiate with regulated organisations is arguably enhanced by the existence of enforcement powers, even (or perhaps especially) if they are rarely used.

The strongest powers of the Victorian Privacy Commissioner are contained in Part 6 of the IPA which sets out the procedure for the Privacy Commissioner to serve a compliance notice[29] on an organisation where she decides:

- a serious or flagrant breach of one or more of the IPPs has occurred; or
- an act or practice in breach of one or more of the IPPs is one that has been engaged in by an organisation on at least 5 separate occasions in the last 2 years.

The second ground on which a compliance notice could be issued is one that does not have to be serious or flagrant, just persistent. It is likely to become apparent through complaints.

Provisions under Part 6 envisage that a compliance notice may be served following a complaint as s 44(5) provides that when deciding to serve a compliance notice the Privacy Commissioner can act on her own initiative or on application from a complainant. Section 44(6) provides that when deciding whether to serve a compliance notice, the Privacy

Commissioner can take into account the extent that an organisation has complied with any order of VCAT under Part 5.

Part 6 of the IPA gives the Privacy Commissioner significant powers to obtain information and documents when investigating matters that may give rise to the service of a compliance notice. These include being able to summon witnesses and examine them under oath. Failure to comply with a compliance notice makes an organisation liable to prosecution (s 48 of the IPA). An individual or organisation affected by a decision to serve a compliance notice has the right to apply to VCAT for a review (s 49).

Although these are the strongest powers of enforcement, they are the ones that are least used to date. Only two compliance notices have been served[30].

The first of these notices involved the Office of Police Integrity and 'Jenny's case'. A report by the then Privacy Commissioner about this matter was tabled in State Parliament on 28 February 2006. The report was the result of an investigation into the mistaken dispatch in 2005 of an original file by the Office of Police Integrity (OPI) to a complainant in country Victoria who is known as 'Jenny' to protect her privacy and the privacy of others. Jenny's case illustrates longstanding issues affecting the security of Law Enforcement Assistance Program (LEAP) data and effective auditing of use of the LEAP system by police. The report explains LEAP, the sensitivity of its data, its legitimate role in policing, and the importance of LEAP data being used properly and being kept secure.

The main points of the 82-page report are:

- Inadequate facilities and procedures led to the mistaken dispatch of the file.
- OPI did not intentionally deceive Jenny, but OPI's inadequate handling of her complaint had the effect of misleading her.
- A fresh audit by the Privacy Commissioner of access by police to data about Jenny in LEAP over the period September 2002 to May 2005 produced results that require further investigation and were referred to the Chief Commissioner of Police and to OPI.
- Personal information relating to 90 identifiable persons was in the OPI file, but it is not likely that notifying those persons would alleviate more harm than it would cause. The breach was limited, the data was secured, and attempts to notify would carry a significant risk of causing more privacy breaches[31].

The second notice also involved the security of personal information held in the Victoria Police database (LEAP) and this time the Department of Justice E*Justice database. It is known as 'Mr C's case'. A report of the investigation was tabled in State Parliament in August 2006.

Mr C was an employee of Corrections Victoria. He became concerned that there had been unauthorised access to LEAP information about him that may have been circulated in the prison system, putting him at risk. He asked management at Corrections Victoria to investigate. As a result, Victoria Police were requested to audit who had accessed personal information in LEAP about Mr C. Subsequently, the results of the audit were sent by unencrypted email to Mr C and a Department of Justice manager. The audit had generated information about persons with names the same or similar to Mr C. The investigation focused on Information Privacy Principle 4 which requires organisations to take reasonable steps to keep secure the personal information they hold and to protect it from misuse, loss, unauthorised access, modification or disclosure. The report reflected several years work by the office of the Privacy Commissioner relating to the security of information in LEAP.

In the course of the investigation into Mr C's case, information indicated that there were data security problems in relation to the database known as E*Justice, a part of the Criminal Justice Enhancement Program (CJEP), for which the Department of Justice is responsible. E*Justice contains data obtained from LEAP. Authorised personnel can use E*Justice to get access to LEAP data and increasingly Victoria police can use E*Justice for certain functions.

An analysis of the data security of E*Justice with a special focus on LEAP data was conducted for the Privacy Commissioner by an independent expert and significant weaknesses identified. The report concluded that, in order to secure personal information in LEAP, it is necessary to ensure that E*Justice is secure and that access to LEAP by E*Justice can be audited. The investigation found that the procedures and technology for LEAP audits were not adequate to provide the protection needed for the amount and sensitivity of personal information held in LEAP. Steps were being taken by the Chief Commissioner of Police to improve the security of LEAP data but further reasonable steps were required to better protect the personal information.

The report concluded that the Secretary of the Department of Justice was taking steps to improve procedures and systems to secure the personal information in E*Justice and audit the use of E*Justice. Some of those steps would need to be taken in conjunction with, or just after, the improvements being implemented by the Chief Commissioner.

As can be seen from the outlines above, the power to serve compliance notices has been used sparingly and only in very serious matters. This is indicative of the preferred approach of the Privacy Commissioner of education through advice and guidance, rather than enforcement through the powers provided. Overuse of these strong powers could undermine the trust and cooperation between the Commissioner and regulated organisations which allow a number of the other functions to be exercised.

Ultimate redress in most jurisdictions is vested in the courts, and each law outlines the circumstances under which disputes can be reviewed at the judicial level. In the belief that courts are not necessarily the most suitable institutions to deal with comparatively specialised and technical issues, some countries have established specialist tribunals. In[1] Britain, for example, the *Data Protection Act 1998* (UK) established a Data Protection Tribunal to which complainants or respondents may appeal a decision of the Information Commissioner; this body is constituted from a panel of experts as necessary.

In other jurisdictions, including Victoria, New South Wales and the Commonwealth of Australia, reviews are conducted by a generalist tribunal. As outlined above, in Victoria, this is VCAT. If a complaint under Part 5 of the IPA is not declined, but conciliation is not possible, or was attempted but unsuccessful, then the Commissioner gives notice to both parties to that effect and under s 37(3), the complainant has the right to require the Commissioner to refer the matter to VCAT. VCAT's hearing is not a review of the Commissioner's decision, but a de novo hearing to establish whether there has been a breach of the IPPs and if so, what remedy should result.

Conclusion

As can be seen from the discussion above, effectively exercising all of the various responsibilities, functions and powers vested by legislation is an extremely difficult balancing act for privacy commissioners. If the Commissioner is too compliant, her effectiveness in promoting and building a culture of privacy and in enforcing the provisions of privacy legislation in the case of repeated or serious breaches will be non existent. Conversely, if

she is too aggressive or strident, her ability to consult, persuade and negotiate with regulated organisations and the government will be equally undermined.

Endnotes

1 The phrase apparently originated in a letter from Roosevelt to Henry L. Sprague on January 26, 1900, when Roosevelt was Governor of New York. In this instance, Roosevelt was referring to his success in forcing New York's Republican committee to retract support from a corrupt financial adviser. Later usages, when Roosevelt was President, referred to US foreign policy under the Monroe Doctrine.
2 C. Bennett, C. Raab, The Governance of Privacy: Policy instruments in global perspective, (Ashgate, Hampshire, 2003), Chapter 5, pp. 95- 120;
3 Ibid., p. 107;
4 Section 9 of the IPA lists organisations regulated by the Act. These include Ministers, Parliamentary Secretaries, local councils, Victoria Police, courts and tribunals
5 For a full discussion of the independence of the Privacy Commissioner see: Appendix E, OVPC, Annual Report 2001/2002;
6 Section 45(3A) Financial Management Act 1994 (Vic)
7 Section 5 IPA
8 Part VI Privacy Act 1988 (Cth); s 41 Privacy & Personal Information Protection Act 1998 (NSW)
9 See note 1, above
10 Bennett & Raab, op.cit., pp.109-110;
11 Section 3 Information Privacy Act 2000 (Vic)
12 In *WL v La Trobe University (General)* [2005] VCAT 2592 (8 December 2005) Deputy President Coghlan ruled that the word 'ascertained' allowed for some resort to extraneous material and an individual may be identified when information held by an organisation is combined with other material. But the element of reasonableness about whether the person's identity can be ascertained will depend on the circumstances of the case.
13 Bennett & Raab., op.cit., p. 110
14 The Victorian Privacy Commissioner has published an audit manual to guide auditors and auditees on how privacy audits are conducted: See Privacy Audit Manual, November 2007, Edition.02;
15 See OVPC, Website Privacy - Guidelines for the Victorian Public Sector, May 2004
16 Bennett & Raab, op.cit., pp. 110-111
17 See OVPC, Privacy Impact Assessments - a guide, Edition 1, August 2004
18 Bennett & Raab, op.cit., pp. 111-112
19 For example, Office of the Privacy Commissioner (Australia), 2001, 2004, 2007, available at http://www.privacy.gov.au/publications/index.html#R, last accessed 25 July 2008
20 See IPA, s.58(a) and (o);
21 Bennett & Raab, op.cit., p.112
22 Section 17(a)(iv) *Parliamentary Committees Act 2003* (Vic)
23 See, for example: OVPC, submission to SARC in relation to the Terrorism (Community Protection) (Amendment) Bill 2005 - 23 January 2006; OVPC, Justice and Road Legislation Amendment (Law Enforcement) Bill 2007: submission to the Victorian Parliament's Scrutiny of Acts and Regulations Committee, August 2007, which raises concerns over the legislative response to the Smith case.
24 See, for example, the series of submissions made by the Victorian Privacy Commissioner to successive Senate Inquiries into the Human Services (Enhanced Service Delivery Bill) 2007, which proposed the collection of a large amount of personal information from virtually the entire Australian population and mandated the use of an 'Access Card':, including a micro-chip and photograph, in order for Australian citizens to obtain government services or concessions, available at www.privacy.vic.gov.au>publications>reports and submissions>submissions;
25 *Smith v Victoria Police (General*)[2005]VCAT 654 (19 April 2005); see case summary at [2005] AUPrivCS 36.
26 Section 13 Information Privacy Act 2000
27 Bennett & Raab, op.cit., p.113
28 Ibid., pp. 113-114
29 See OVPC, Procedure for Service of Compliance Notices, under s 44 Information Privacy Act, July 2003.
30 See: OVPC, Report 03.06 Mr. C's Case: Report of an investigation pursuant to Part 6 of *the Information Privacy Act 2000* into Victoria Police and Department of Justice in relation to the security of personal information in the Law Enforcement Assistance Program (LEAP) and E*Justice databases, July 2006; OVPC, Report 01.06 Jenny's case: Report of an investigation into the Office of Police Integrity pursuant to Part 6 of *the Information Privacy Act 2000*, February 2006;
31 See also OVPC, Responding to Privacy Breaches, Guide Edition 1, May 2008; Responding to Privacy Breaches - Checklist, Guide Edition 1, May 2008;