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

privacy victoria

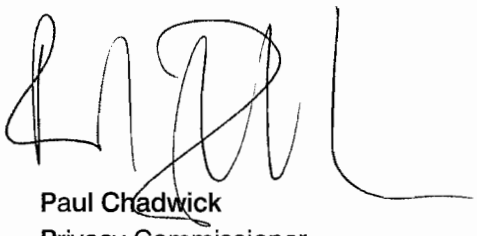
Office of the
Victorian Privacy
Commissioner

The Hon. Rob Hulls, MP
Attorney-General
55 St Andrews Place
Melbourne Victoria 3002

Dear Attorney-General,

I enclose for tabling in the Victorian Parliament my report of an investigation into the Office of Police Integrity pursuant to Part 6 of the *Information Privacy Act 2000*.

Yours sincerely,



Paul Chadwick
Privacy Commissioner
February 2006

Ordered to be printed
Victorian Government Printer 2006
No 166 Session 2003–06

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

Office of the
Victorian Privacy
Commissioner

Pursuant to Part 6 of the *Information Privacy Act*

Report 01.06

Office of the Victorian Privacy Commissioner
GPO Box 5057, Melbourne Victoria 3001, Australia
DX 210643 Melbourne
Level 11, 10-16 Queen Street, Melbourne Victoria 3000, Australia
Local Call 1300 666 444 Local Fax 1300 666 445
www.privacy.vic.gov.au enquiries@privacy.vic.gov.au

An independent statutory office established by the Victorian Parliament under the *Information Privacy Act 2000*.

Contents

Summary

1 The Office of Police Integrity (OPI) was established by the Victorian Parliament in November 2004 to detect, investigate and prevent police corruption and serious misconduct. One of OPI's functions is to consider complaints from the public against police. The amendments to the *Police Regulation Act* that created OPI also created the Director, Police Integrity to head OPI and required that the holder of the statutory office of Director, Police Integrity must be the Ombudsman. The holder of both offices is Mr George Brouwer.

2 In June 2005, OPI lost a file relating to a complainant from country Victoria. The woman is known as 'Jenny' to protect her privacy and the privacy of others involved in the circumstances of her complaint. (**Section 1, Section 3**) The file was received by Jenny through the post in a parcel to which was attached an envelope containing a letter to Jenny from OPI.

3 Jenny was supposed to get the letter but not the file, which included printouts of personal information relating to a large number of people not connected to Jenny's case. The information had been derived from the main Victoria Police database, called LEAP, during OPI's handling of Jenny's complaint. (**Section 2, Section 5**)

4 The file was returned to OPI after being out of its custody for nine weeks without OPI being aware of the fact. (**Section 7**)

5 Soon after the file had been returned to OPI and the matter reported in the media, Mr Brouwer invited the Office of the Victorian Privacy Commissioner (OVPC) to investigate the circumstances of the loss and the handling by OPI of Jenny's complaint. Mr Brouwer gave an assurance of full co-operation, and this was honoured by OPI during the OVPC investigation. The Chief Commissioner of Police, Ms Christine Nixon, facilitated the co-operation of Victoria Police.

6 Under Part 6 of the *Information Privacy Act*, the Privacy Commissioner may serve a Compliance Notice on an organisation if it appears that the organisation has acted in contravention of an Information Privacy Principle (IPP) and the contravention is serious. Information Privacy Principle 4 states that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. OPI's loss of its file of Jenny's case meant that the requirements of IPP4 had not been met. (Section 10)

Findings about loss of file

7 The investigation located no documentary proof in the systems of the relevant organisations of how the file left OPI and reached Jenny's post office box in country Victoria.

8 The recollections of relevant staff provide some information but do not include the detail necessary for a conclusive finding of precisely how the file left OPI and got to Jenny.

9 My findings are based on what is more probable than not, having regard to the available evidence and to hypotheses that have been tested and ruled out. (Section 6)

10 No evidence was found to indicate that the file was intentionally leaked.

11 The period November 2004 to June 2005 was a period of rapid and tumultuous change in Ombudsman/OPI. In ways relevant to my findings and recommendations, it was a period unique in the lives of both organisations. It was a prelude to structural and operational separation of OPI from the Office of the Ombudsman, a process that had begun and continues still. (Section 4)

12 At the time, the two entities, Ombudsman and OPI, shared the same facilities and staff for three distinct tasks: dispatching correspondence such as letters to complainants; returning files to storage; and arranging for police material to be transferred back to Victoria Police. These functions happened in the same makeshift space. Staff had varying levels of experience. Their roles overlapped.

13 On the balance of probabilities, I find that –

- On or about 2 June 2005, OPI complaints-handling staff finalised a letter for Jenny and took it, with the file containing the LEAP data, to the shared mailing/filing facility. The complaints-handling staff intended that the mailing/filing staff who worked there would put the letter in an envelope and post it to Jenny and would put the file into storage at OPI.
- Instead of being placed in storage, the file was mistaken by mailing/filing staff for Victoria Police material, and was wrapped for delivery to Victoria Police.
- The letter for Jenny was put in an envelope with Jenny's address showing through the clear plastic window, but then the envelope was mistakenly taped to the wrapped package.
- The package left OPI intended for the Victoria Police, probably the Ethical Standards Department (ESD).
- En route, Jenny's address was noticed and the package was assumed to have been misdirected. This happened either at the initial sorting centre of the courier company used by OPI, or at the main mail centre of Victoria Police.
- Without being opened, the package was re-directed to Australia Post for delivery to Jenny and reached her post office box service.
- No evidence was found to indicate that any Victoria Police personnel had cause to suspect that the OPI file of Jenny's case containing LEAP data was passing through the mailing system of Victoria Police on its way to Jenny.
- The main cause of the loss of the file by OPI was inadequate facilities and procedures in the combined Ombudsman/OPI operation at the time, the first week of June 2005.

Compliance notice to ensure OPI's data security in future

14 I am satisfied that OPI has since taken reasonable steps to strengthen the relevant facilities and procedures. (Section 10)

15 The strength of those facilities and procedures needs to be tested periodically. Having regard to the sensitivity of the information which OPI's statutory functions require it to collect and handle, any weaknesses in its data security need to be identified swiftly and remedied, for reasons that encompass privacy protection as well as other public interests.

16 Accordingly, I have served on the Director, Police Integrity a Compliance Notice under section 44 of the *Information Privacy Act* requiring specified action within a specified period for the purpose of ensuring compliance with IPP4 in future.[1] The Compliance Notice is reproduced at **Appendix 1** of this report.

17 Additional recommendations have been made to the Director, Police Integrity in relation to OPI complaints handling, and to the Director and the Chief Commissioner in relation to the data security of LEAP and investigations of complaints of misuse of the personal information in LEAP. **(Section 10)**

Auditing access to LEAP data about Jenny

18 Jenny reasonably understood that OPI had arranged an audit of occasions of access to LEAP data about Jenny in the period 2002-2004. However, only the period April 2004 to September 2004 had been audited. While OPI did not intend to deceive Jenny, its handling of her complaint was inadequate and its initial response to her had the effect of misleading her.

19 A fresh audit was conducted by OVPC – independent of ESD and OPI – of occasions of access to LEAP data about Jenny during the period from 1 September 2002 to 31 May 2005. **(Section 8)**

20 The audit identified eight occasions of access requiring further investigation and OVPC referred the preliminary results to the Chief Commissioner and Director, Police Integrity for further investigation. Given the history of Jenny's case, I have requested that the Privacy Commissioner be informed of the outcome.

21 I have also recommended to the Chief Commissioner and Director, Police Integrity that a further audit be conducted into any occasions of access to LEAP data about Jenny in the period 1 January 2002 to 31 August 2002, a period which pre-dates the Privacy Commissioner's jurisdiction and so could not be covered by the audit OVPC conducted during this investigation.

22 I have recommended that relevant data in LEAP relating to Jenny be tagged so that any future occasions of access to data about Jenny will automatically be flagged for follow-up checks by internal investigators or OPI or both to ensure that the access was for a proper policing purpose.

23 The OVPC investigation into Jenny's case again illustrated the longstanding and complex problems of securing the personal information in LEAP and in auditing use of LEAP effectively. These problems, which OPI has itself diagnosed[2], will be addressed in greater detail in the report by OVPC of its investigation into disclosure electronically by Victoria Police, via IBM, of a large amount of LEAP audit data to employees of the Department of Justice (Corrections Victoria) in 2005.

Notification not recommended

24 Analysis of the LEAP data in the OPI file of Jenny's case shows that it contains almost 500 names, many of which are repeats caused by the LEAP audit processing that was used.

25 The printouts in the file contain a limited amount of sensitive personal information relating to 90 identifiable persons. In privacy cases, the presumption is that the subjects of a privacy breach should be notified about the breach, unless exceptional circumstances make notification neither necessary nor desirable. The decision whether to notify should be made in a structured way, and explained.

26 I have decided not to recommend that OPI attempt to notify the 90 persons about the breach of their privacy resulting from OPI's loss of its file. The question is: Would notification be reasonably likely to alleviate more harm than it would cause? In the circumstances of this case, I have decided that it would not. (**Section 9**)

27 The structure of the decision and my reasons are explained in **Section 9** of this Report. In summary, the reasons are –

- The amount of sensitive personal information about each of the 90 is limited.
- The extent of the unauthorised access to the file was limited, and to the LEAP audit data more so.
- Assurances have been sought and obtained that copies of the sensitive personal information were not made.
- The data has been returned and is again secure.
- Destruction of unnecessary copies has been recommended.
- The predominant names in the audit data are names the same as, or similar to, Jenny and her husband, whose real names have remained secure throughout the media reporting, political debate and OVPC investigation.
- If OPI attempts to notify the 90, even careful and well-intentioned efforts to do so are likely to fail in a proportion of cases because of inaccurate or out-of-date information, causing foreseeable harms.
- Assuming OPI were to overcome the communications problems and successfully make secure contact with all 90 persons, a proportion of the 90 are likely to suffer harm by the fact of being made aware.

28 In all the circumstances, I have concluded that it is not reasonably likely that notification would alleviate more harm than it would cause.

[1] Section 44 (2).

[2] *OPI, Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP)*, March 2005, OPI LEAP Report

1 The limits of Jenny's case

1.1 Jenny's husband is a member of Victoria Police. Her husband's former wife is also a member of Victoria Police. His former wife has remarried too, and her new husband, who was previously married, is also a member of Victoria Police. Marriages and divorces are matters intensely private to the participants.

1.2 Knowing this much, readers of this Report can appreciate from the outset that it is not a simple task to investigate and report in public on this or any privacy case. We ought not, in Virginia Woolf's phrase, dabble our fingers in the stuff of other people's souls.

1.3 As is often the case for Privacy Commissioners, this investigation involves some matters very personal to some participants and some matters of legitimate public interest. Privacy must be protected as far as possible, but a public accounting is necessary, in particular about the data security of case files of the Office of Police Integrity (OPI) and about the continuing problems of securing the personal information in the Victoria Police Law Enforcement Assistance Program database known as LEAP and described in **Section 2**.

1.4 In this Report, as in most privacy matters, it is necessary to strike a balance between privacy and disclosure. An example of that balance is the use of the fictitious name 'Jenny', with no reference to geographic location, by the journalists who first disclosed this case. With care, it is possible to protect individuals' privacy while still putting issues into the public arena for appropriate response. The investigation by my Office has used stringent security to try to ensure that Jenny and others whose privacy is implicated are not identified. In this Report, personal information is kept to the minimum I consider necessary to give a proper and fair account to Parliament and the public.

1.5 Protecting privacy also requires prudent self-protection. If Jenny exercises her undoubted right to comment in the media, it would be better for her privacy and for the continuing privacy of others if she did so without her face and voice being recognisable. Journalists and parliamentarians tend to know more about protecting the identities of sources than those with limited experience of the media.

1.6 The legal backdrop to this case (**Section 3**) is relevant to how it unfolded. Jenny made five separate complaints to Victoria Police, the Ombudsman/OPI, Office of the Federal Privacy Commissioner and Office of the Victorian Privacy Commissioner. Broadly summarised, the complaints relate both to the handling of Jenny's personal information and to the processing of her complaints about that handling.

1.7 Jenny's complaints have implications far wider than Jenny's personal privacy or the privacy of other people affected. Her case is symptomatic of some longstanding problems with the security of LEAP data. Her complaints to the Ombudsman/OPI coincided almost exactly with the period in which OPI was being grown from within the Ombudsman's office – that is, November 2004 to June 2005. This transition period is relevant to my findings. With the acuity of hindsight, it seems clear that at the time it was likely that a file would go astray and that there would be insufficient liaison between Ombudsman/OPI and Victoria Police over the handling of a complaint such as Jenny's.

1.8 Both of the bigger issues – police database security and Victoria's system for independent oversight of the police force – have been matters of political controversy in recent times. Both issues involve important factors besides privacy protection. Neither issue can be resolved through the operation of the *Information Privacy Act* alone. To view Jenny's case in that way drains the inherent complexity out of the broader questions about police databases and police accountability in a technology-rich community committed to the rule of law. It also neglects the range of participants necessary to reach enduring answers, and places on the *Information Privacy Act* more weight than it was designed to bear. The debate and resolution of the broader issues are properly the responsibilities of the Government and Parliament.

1.9 The collection and handling of the personal information of Victorians by state and local government organisations is the proper business of the *Information Privacy Act* and the Office of the Privacy Commissioner. To the extent that Jenny's case engages the *Information Privacy Act* and the functions of my Office, I have acted and will continue to act, but only to that extent.

2 Law Enforcement Enhancement Program (LEAP) and personal information

2.1 General description

2.1.1 LEAP has been in operation since 1993 and is the main data system for the day-to-day policing of Victoria.

2.1.2 In March 2005, the Office of Police Integrity gave the following general description –

> LEAP is the primary mainframe corporate application and information system utilised by Victoria Police. It is used to record crime incidents and personal particulars and captures a range of information including details of lost and stolen property and vehicles of interest to law enforcement. LEAP provides an online interface to internal and external systems to facilitate name, vehicle and place searches. It is also used in relation to fingerprint classifications, case management and intelligence collation. Access to LEAP peaks at around 350,000 transactions daily and the system is linked to over 5,000 terminals 24 hours per day. The system is extensively used in support of operational policing and as a resource to provide management data.[1]

2.1.3 The President of the Victorian Civil and Administrative Tribunal (VCAT), Justice Stuart Morris, has provided an overview of LEAP –

> [LEAP] is used to perform many and diverse functions from recording crime to checking interstate vehicle details. It is also used to record every reported crime in Victoria. It holds data on intervention orders, family violence, abused children and the like. It has warning flags to assist members in the management of potentially dangerous and life threatening situations. It also holds data in relation to all persons who have been interviewed or charged by Victoria Police; and it holds all court outcomes for all crimes and some traffic matters.

> The LEAP database is a relational database which interfaces with other systems. It allows an inquirer to enter a query from one of many points and then move the query to other areas. It is an essential tool used by all operational and investigative areas of the police force. For example, it is a primary intelligence tool for the profiling of suspects used by the Protective Security Intelligence Group within the Victoria Police, as well as the Counter Terrorism Unit, Major Drug Investigation Division and other crime squads responsible for the investigation of serious criminal offences.[2]

2.1.4 LEAP involves recurring and complex issues affecting the information privacy of the individuals whose personal information is in the system. These issues, which tend to be common to police databases in Australian and overseas jurisdictions, will require attention in the transition to the foreshadowed replacement of LEAP.[3]

2.1.5 Several of the issues will be examined in greater detail in a forthcoming report by OVPC of another investigation involving disclosure electronically by Victoria Police, via IBM, of a large amount of LEAP audit data to employees of Department of Justice (Corrections Victoria).[4] The facts are unrelated to Jenny's case, but several of the issues about LEAP use and security are similar.

2.2 Difference between 'live' LEAP and LEAP audit data

2.2.1 In considering LEAP use and security, it is important to appreciate the difference between the experience of using LEAP 'live' in day-to-day policing work and the experience of examining LEAP audit data. The LEAP data in OPI's file of Jenny's case consisted of printouts of LEAP audit data.

2.2.2 Live LEAP is a rather old-fashioned, text-based computer experience. Users type requests into fields in order to view information that has been categorised as belonging to that field. LEAP tends to lack the range of live links, icons and point-and-click capabilities most people associate with contemporary computer experiences. However, a person with access to live LEAP can check whether there is data behind a wide range of fields.

2.2.3 Reading LEAP audit data is very different. The data is drawn from an archive of all the screens viewed by all of LEAP's users. The screens are a kind of 'frozen' record of screens of LEAP use over the years. You see a still image of what the police member saw as he or she used LEAP at a precise time of day or night on a date in the past. You can see what data the user entered, and into which fields he or she entered it, in order for him or her to bring up information about, say, a particular person, address or vehicle.

2.2.4 The archive is held on computer tapes, each containing a month of LEAP use by all its users. The archive is not arranged in 'files' that correspond either to individual users of LEAP or to the individual data subjects. To this extent, the term 'police files' is not accurate, although it is understandable that it is commonly used.

2.2.5 The LEAP archive is not readily searchable in the way we nowadays think of searching a large dataset with search tools 'Google style'. A LEAP audit is neither as straightforward nor as swift as it should be. Depending on how it is conducted, it can create its own problems of data quality and data security.

2.2.6 If investigators want to check whether a given person was looked up on LEAP, or how a particular user has behaved during a particular session of LEAP use, investigators must first determine the time period they want to examine. They must then devise a 'search string' that is best tailored to finding any relevant screens. Typically, a search string will include a person's name and/or some other distinguishing piece of information. The range of potential search strings is not sophisticated, at least not by contemporary information technology standards. It is relatively easy for a search string to return a large amount of data about many people completely unconnected with the persons who are the objects of the particular audit. As Jenny's case and other cases have shown, big volumes of sensitive data create security issues, and may create data analysis problems, for the people conducting the audit.

2.2.7 Once a search string has been devised, IBM, the contracted service provider to Victoria Police, will arrange for the tapes of data from the relevant time period to be checked and for the search results to be returned to the investigators for analysis.

2.2.8 The type of personal information about individuals held in LEAP varies greatly. For instance, the majority of Victorians could expect that nothing would appear about them in the field entitled 'DNA status' since only a minority would have had a DNA sample taken and processed through the forensic procedures provisions of the *Crimes Act*. By contrast, because LEAP is connected to the VicRoads database, the majority of adult Victorians are likely to be accessible through LEAP, if only as a licensed driver or as owner of a registered vehicle. The fact that a person is a driver or owns a particular vehicle is generally not sensitive personal information.

2.2.9 Several fields do contain sensitive personal information about a proportion of the population. For some people, their criminal record data will be accessible through LEAP. For others, who have been victims of crime, LEAP data may include some details of what happened to them in the incident. Where the crime was of a sexual nature, the data is most sensitive. Others may be recorded as being associated with a person of interest to police, either generally or in relation to a particular incident. LEAP fields allow for the inclusion of a physical description including gender, hair and eye colour, height and build, distinguishing marks and ethnic appearance.

2.2.10 In LEAP audit data, this kind of information is rarely extensive. It shows only what the user actually looked up at the time. Audit data does not show all of the information that may lie behind the various fields and be able to be looked up when LEAP is being used 'live' in real time. To illustrate: a police member checking a registered vehicle may need to know only the name of the registered owner, not any other information about that person. The archive will contain the screens of only this enquiry and the data it elicited, not any other data that LEAP may hold about the person. So, in practice, the audit data of particular screens referring to an identifiable person may be confined to a single brief item of information.

2.3 Relevance of data quality to the need for data security

2.3.1 The quality of LEAP data is uneven. Keeping it accurate, up-to-date and not misleading is a continuous challenge. A simple illustration: LEAP may contain a short narrative of a particular incident attended by police. The data will be only as good as the information the member was able to collect at the time. Quality varies with the varied skills and styles of those who collect the information and the personnel who type it into the system. These narratives should not be thought of as lengthy, considered findings of a full police investigation or of a court proceeding. They are necessarily 'shorthand' accounts. However, the data's very brevity has its own implications if LEAP audit material gets into unauthorised hands. It may mislead those unfamiliar with policing, which like most specialised types of work has its own jargon and abbreviations.[5] The data may mislead police too if they rely too heavily on it without taking reasonable steps to verify it, depending on the context. The varying quality of the information needs to be understood in context.[6] The remarks entered by a police member who attended an incident may be relevant to police and readily understood by them, even in abbreviated form. Even when the information is an accurate account of what the member was told by persons interviewed at the scene of an incident, the data may still be objectively inaccurate if the persons interviewed were unreliable witnesses (whether through confusion, injury, self-interest, malice or any number of other reasons). Facts that later come to light may undermine the reliability of the data put into LEAP at a particular time, even though the police who provided it for LEAP did so in good faith. Human frailty affects data quality too: a hectic shift, answers misheard, dislike for paperwork, unclear handwriting on forms used by data processing staff. These realities can be acknowledged, but they underline the need for careful security of data that is recognised as being of uneven quality yet of considerable sensitivity.

2.3.2 LEAP data, even if accurate and up-to-date, can lead to inferences that are not accurate. The power of inference is greatly underestimated as a factor in the harms that may be caused by privacy breaches. People often put two and two together and get five, or seven. The mere fact that an identifiable person is disclosed as being recorded in LEAP may produce adverse inferences, depending on context and on the attitudes of the persons to whom disclosure is made. For instance, to be mentioned as being an associate of a person with a criminal record may itself be discreditable in some people's eyes. Other people may think that just because you are listed as an associate of a person does not necessarily mean that you have knowledge of that person's record or have any reason to believe police may once have had an interest in the person. The fact that a person is recorded in LEAP as having been a source of information to police about a violent incident is a fact that the source may be comfortable for other police to know, but uncomfortable for a wider audience to know, in particular the offender.

2.4 Why LEAP is important for proper policing

2.4.1 It should be apparent from this necessarily general description that much data in LEAP, although sensitive and of varying quality, is of practical assistance in the course of proper policing duties. It should be equally apparent that data in LEAP, *because* it is sensitive and of varying quality, requires a high level of security and an awareness of the harms it could do out of its proper policing context.

2.4.2 Police need LEAP, or better still a technologically improved but equivalent type of database, for practical, legitimate reasons.

2.4.3 Police called to respond to neighbours' reports of apparent violence in a house need to know if the address has been the site of other violent incidents. Police who stop a vehicle need to be able to check if the registered owner has had involvements with, say, firearms. Police can reasonably expect access to certain information that will forewarn them of danger before they put themselves in harm's way, or so that they can keep others from harm.

2.4.4 Less dramatically, but also importantly, access to a measure of information about members of a community is a basic part of policing that community. Information is necessary for police to be able to react to, and to follow up, the myriad of incidents that the community expects police to handle.

2.5 Why it is important to use LEAP data properly and keep it secure

2.5.1 Just as police have reasonable expectations, so does the community.

2.5.2 Wariness about the content and use of police databases is a marker of a healthy liberal democracy. Excessive surveillance and data-gathering by police forces of personal information about citizens can lead to abuses of power. The issue is not theoretical.[7]

2.5.3 Leaving to one side any questions about excessive collection, and assuming for present purposes that all the data in LEAP is necessary for legitimate policing purposes, it is necessary to be continually aware that the data is both sensitive to the members of the community to whom it relates and valuable to a range of potential users for many non-policing purposes. For instance, the data in LEAP has commercial value.

2.5.4 So, while the need to secure the data is strong, so are the pressures for its improper use and disclosure. Measures to secure the data are constantly tested by these countervailing pressures for the information to flow.

2.5.5 The literature[8] indicates that misuse of police and other government database information falls into four broad categories:

1. Personal – that is, use by police and other public servants of official database information to assist them or others in their personal affairs, such as to check on a neighbour, a person met socially, a person with whom they are conducting business, or perhaps just to satisfy curiosity about celebrities.
2. Political – that is, to obtain information, without having a proper policing purpose, about people involved in the political process.
3. Commercial – that is, systematic disclosure of police database information to those to whom it is commercially valuable, for example, credit providers, private investigators.
4. Criminal – that is, leaks to criminals that inform them about what police know and do not know.[9]

2.5.6 The corruption that particularly categories three and four can breed takes the problem of police database security beyond the concerns of privacy protection. Privacy breaches remain one of the consequences of misuse of police databases, but typically there are graver consequences.

2.5.7 Transparency is one safeguard against misuse.[10] But in this policing context, transparency has practical limits. Since it is counter-productive to describe police datasets, systems and their security in too much detail, a measure of trust is necessary. To an extent, both Victoria Police and specialist oversight organisations have to be trusted.

2.5.8 The community can reasonably expect police to collect only the personal information necessary for legitimate policing, to use it only for proper purposes, to treat appropriately what is of uneven quality, and to secure all of it.

2.5.9 It is a kind of bargain. In return for community acceptance of the existence and proper use under law of databases such as LEAP, police and oversight bodies have obligations to fulfil. Misuse of the data must be vigorously deterred. As with any data system with a large human element, lapses in security are likely to occur. But the lapses ought to be able to be detected swiftly. Investigations should be thorough. Remedies, where needed, ought to be prompt. Public explanations have to be plain-spoken (without themselves undermining data security).

2.5.10 Honouring this bargain is part of what is necessary for Victoria Police and OPI to maintain public confidence.

[1] OPI, *Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP)*, March 2005, p 9.

[2] *O'Sullivan v. Victoria Police* [2005] VCAT 532 paras 6-7.

[3] Announced by the Premier 22 August 2005.

[4] OVPC Media Release 16 August 2005.

[5] For an illustration of how category headings, as much as the data in those categories, may mislead, see the decision and orders of Morris J in *JF v. Victoria Police* [2005] VCAT 1641, paras 7-9.

[6] Different datasets connected to LEAP may have their own weaknesses: see, for instance, Ombudsman Victoria, *Own Motion Investigation into VicRoads Registration Practices* (June 2005); Information and Privacy Commissioner, British Columbia, Canada, Investigation Report P95-005 Cars, people and privacy: *Access to Personal Information through the Motor Vehicle Database* (31 March 1995), Appendix 2 and Appendix 3 relate in particular to Canadian Police Information Centre (CPIC) data.

[7] See, for instance, Victorian Ombudsman's reports on Victoria Police Special Branch files (May 1984 and March 1990) and *Allegations Raised Concerning the Operations of the Operations Intelligence Unit and Other Related Issues*, Second Interim Report of the Ombudsman, November 1998, pages 82-83 (first interim report May 1998; final report May 1999).

[8] OPI, LEAP Report. NSW Independent Commission Against Corruption (ICAC) *Report on Unauthorised Release of Government Information* (August 1992); ICAC Annual Report 1993, page 20-30; *Report on Investigation into Matters Relevant to Police and Confidential Information* (June 1994) at www.icac.nsw.gov.au; Queensland Crime and Misconduct Commission (CMC, formerly Criminal Justice Commission) *Protecting Confidential Information: a Report of the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000), *Integrity in the Queensland Police Service: QPS Report Update* vol 1 (March 2001) both at www.cmc.qld.gov.au; WA Royal Commission into Police Corruption in the Western Australia Police Service – *Information Management and Security*, Discussion Paper (February 2003) www.police.royalcommission.wa.gov; WA Royal Commission into Police Corruption, Report, see, for examples of misuse for personal, political, commercial and/or criminal purposes, Chapters 11, 13 and 19; WA Corruption and Crime Commission *Protecting Personal Data in the Public Sector – report of an inquiry into unauthorised access and disclosure of confidential personal information held on the electronic databases of public sector agencies* (September 2005) www.ccc.wa.gov.au; Australian Senate, Standing Committee on Legal and Constitutional Affairs, Report on *Unauthorised Procurement and Disclosure of Information*, June 1991; Commonwealth Auditor-General, Report *Protection of Confidential Client Data from Unauthorised Disclosure* (1998). Consultations by OVPC with its counterpart privacy and data protection commissioners in other countries confirmed the general picture produced by Australian inquiries. UK Home Office, *Promoting Ethical Policing: Police Corruption in England and Wales – an assessment of current evidence*, Home Office Online Report 11/03 (2003); *Promoting Ethical Policing: summary findings of research on new misconduct procedures and police corruption*, Home Office Online Report 12/03 (2003) www.homeoffice.gov.uk. Overseas cases of misuse of police databases include:
   - in New Zealand, a police officer was involved in a tenancy dispute with a woman and accessed the police database to find her new address: *Tenant complains officer accessed her details on Police computer for personal use* Case note 40087 [2003] NZPrivCmr 6, http://www.worldlii.org/nz/cases/NZPrivCmr/2003/6.html;
   - in the United States, a database operated by the Minnesota Chiefs of Police Association ("MJNO" – Minnesota Jurisdictional Network Organization) was shut down following concerns about its accuracy and security. The database came to light following reports of it being used to detain a man at a political rally: Rep. Mary Liz Holberg (R-Lakeville), "Why one legislator cares about data protection" (Spring 2004) 3(3) *FYI* 1, newsletter of the Minnesota Department of Administration's Information Policy Analysis Division, http://www.ipad.state.mn.us/newsletters/0404fyi.pdf. Also see references to data privacy concerns in relation to the MJNO and the integrated criminal justice database (CriMNet), prompting legislative amendment to improve compliance and oversight: State of Minnesota, Office of the Legislative Auditor (James Noble, Legislative Auditor), *CriMNet: Evaluation Report*, March 2004, http://www.auditor.leg.state.mn.us/ped/pedrep/0405all.pdf.
   - in Canada, Edmonton police were found to have inappropriately accessed the police database for purposes unrelated to law enforcement: Alberta Information and Privacy Commissioner, Report on Investigation into the *Use of Personal Information - Edmonton Police Service - Investigation #3210*, Investigation report F2005-IR-001, 27 April 2005, http://www.oipc.ab.ca/ims/client/upload/F2005_IR_001.pdf. The misuse occurred during the course of a stakeout by police of a public event attended by a journalist who had written articles critical of police and the chairman of the statutory police accountability body. Police appear to have hoped to intercept for drink-driving one, or perhaps both, as the men left the venue. http://www.cbc.ca/edmonton/features/police/. Information about the results of disciplinary proceedings was still pending when this Report was finalised.

[9] The disclosures may be made knowingly or unwittingly, and, of course, may involve leaks from information in datasets other than LEAP – see *Director of Public Prosecutions v Christopher Gerald Marks* [2005] VSCA 277 and OPI, *Report on the Leak of a Sensitive Victoria Police Information Report* (February 2005).

[10] For example, to demonstrate the efficacy of auditing is one way to deter improper access.

3 Jenny's five complaints and the applicable laws

3.0.1 Jenny's concerns involve several government organisations with overlapping roles.

3.0.2 Australia's federal system of government often means that a given set of circumstances affecting a member of the public and giving cause for complaint will be covered by a Commonwealth law and a Commonwealth regulator, by a State law and a State regulator, or by both, with greater or lesser overlap. This applies in Jenny's case, where both the Federal Privacy Commissioner and the Victorian Privacy Commissioner have jurisdiction to handle different parts of her concerns.

3.0.3 Sometimes, an apparently simple matter gets even more complicated. The circumstances giving rise to the complaint may be covered by more than one State law and more than one State regulator. This also applies in Jenny's case, where her complaint concerns the behaviour of serving members of Victoria Police and the handling of her personal information by police. The combination brings into play the jurisdictions of three State office holders –

- Chief Commissioner of Police (in relation to internal police force management);
- Director of Police Integrity (in relation to oversight of the police force); and
- Victorian Privacy Commissioner (in relation to collection and handling of personal information by the police force and by OPI).

3.0.4 It is a basic aspect of the rule of law that authorities stay within their jurisdiction. If they operate beyond their power, the courts will rightly pull them back within the limits of the power the law allows them. In practice, overlaps need to be handled carefully or else subsequent actions may be invalidated, with loss of time and effort for all.

3.0.5 In my view, the main responsibility to try to make complaints systems work rests with government authorities and not with the members of the public who bring a complaint. The authorities ought to consult with each other, transfer complaints to the proper regulator and explain to the complainant what has been done.[1]

3.0.6 For complainants, who are outside all this bureaucracy and who naturally look at the situation from the specific point of view of getting their own complaint promptly handled, these explanations about various jurisdictions and the limits of powers can be frustrating. These perceptions are understandable, but overlapping jurisdictions and referrals are unavoidable in many cases. Jenny's is one such case.

3.0.7 I turn now to each of the several aspects of Jenny's concerns and differentiate the jurisdictions, giving only the minimum necessary personal information. It should make it easier for the reader to follow later sections of this Report.

3.1 First complaint

4 December 2001 complaint to Victoria Police about inappropriate access by a Victoria Police member to personal information about Jenny in Victoria Police records (the LEAP database).

3.1.1 The investigation by the Victoria Police Ethical Standards Department (ESD) resulted in a Victoria Police member being formally counselled in February 2002, on the recommendation of the Deputy Ombudsman (Police Complaints), for having made an inappropriate access to LEAP data about Jenny.

3.1.2 The *Information Privacy Act* became enforceable on 1 September 2002, so the Victorian Privacy Commissioner does not have jurisdiction to accept a formal complaint from Jenny under Part 5 of the Act in relation to this First Complaint.

3.1.3 The matter is nevertheless relevant to my investigation under Part 6 of the *Information Privacy Act* for the following reasons. It is evidence of a past willingness inappropriately to seek information about Jenny from LEAP. It is relevant to determining the timeframe of any subsequent audit of LEAP access by Victoria Police members to data about Jenny. It provides an example of how ESD dealt with a case of inappropriate LEAP access in liaison with the Ombudsman, who at that time prior to the existence of OPI had a more limited role in relation to complaints against police. The existence of the First Complaint was known to OPI when it handled Jenny's 11 November 2004 complaint (Third Complaint), and to ESD when it liaised with OPI during OPI's handling of the Third Complaint.

3.1.4 During this investigation I examined ESD's file of its handling of the First Complaint and have made recommendations to the Chief Commissioner and the Director, Police Integrity, that aspects of ESD's approach be re-examined with a view to using the experience of Jenny's case to assist efforts to avoid recurrences of misuse of LEAP data. (LEAP is described in Section 2)

3.2 Second complaint

1 November 2004 complaint, addressed to the Federal Privacy Commissioner but sent initially by Jenny to my Office, about –

- how a private business handled a letter Jenny sent to the business in which Jenny had included financial data about herself; and
- the conduct of a Victoria Police member in obtaining the letter and, according to Jenny's complaint, using it to the detriment of Jenny's husband and, by association, Jenny.

3.2.1 The Victorian Privacy Commissioner has jurisdiction only in relation to the collection and handling of personal information by state and local government organisations and their contracted service providers. The Federal Privacy Commissioner has jurisdiction under the Commonwealth *Privacy Act 1988* over private sector organisations, such as the private business involved in Jenny's concerns.

3.2.2 With Jenny's consent, my Office referred this Second Complaint to the Federal Privacy Commissioner on 5 November 2004. Any investigation into how the private business behaved, or how non-Victorian Government organisations handled personal information that originated from the private business, is a matter for the Federal Privacy Commissioner, who has the relevant jurisdiction. I asked the Federal Privacy Commissioner to expedite the processing of Jenny's complaint.

3.2.3 Jenny sought advice from the enquiries staff of my Office in February 2005 about her concerns that any Victoria Police member would act as she believed one Victoria Police member had acted in obtaining and using the letter from the private business. My staff advised at the time that the Ombudsman (meaning OPI, which had by that time formally taken over the Ombudsman's police complaints work) was the more appropriate organisation to consider such a complaint about police conduct.

3.3 Third complaint

11 November 2004 complaint to the Ombudsman/Office of Police Integrity about conduct of a Victoria Police member in obtaining and using certain financial data that Jenny had supplied to a private business.

3.3.1 OPI decided in December 2004 to seek, in liaison with Victoria Police, an audit of access to LEAP data about Jenny and her husband. The timeframe for the audit was arranged between OPI and ESD. When Victoria Police received the audit data from IBM, Victoria Police sent the audit data to OPI. OPI assessed it and wrote to Jenny on 31 December 2004. OPI also separately sought in writing from ESD confirmation of the outcome of the 2001 complaint (First Complaint), and ESD provided that confirmation. OPI's handling of this Third Complaint has been examined in the course of the OVPC investigation (**Section 5**).

3.4 Fourth complaint

3 May 2005 complaint to OPI seeking appropriate action against a Victoria Police member for obtaining, using and retaining the letter Jenny had sent to the private business containing certain financial data.

3.4.1 OPI's handling of this complaint resulted in a letter to Jenny from OPI dated 2 June 2005. This is the letter that was taped to a parcel containing the original OPI file of Jenny's case, including the LEAP data from the audit conducted during the handling of the Third Complaint. How this happened is described in **Section 6**.

3.5 Fifth complaint

15 August 2005 complaint to the Victorian Privacy Commissioner about access, without a proper policing purpose, to LEAP data about Jenny by one or more Victoria Police members.

3.5.1 This was a formal complaint by Jenny to the Victorian Privacy Commissioner under Part 5 of the *Information Privacy Act*. The Chief Commissioner of Police was duly advised of it, as the Act requires. I sought and received the Chief Commissioner's co-operation for the conduct of a fresh audit of accesses to LEAP data about Jenny by police. Jenny's husband's right to complain formally was explained to him. He said he did not want to make his own complaint under the *Information Privacy Act*, nor did he wish me to arrange a separate fresh audit of access made to LEAP data about him. Jenny formally withdrew her complaint on 14 November 2005.

3.5.2 The fresh audit of access to LEAP data about Jenny continued because, notwithstanding withdrawal of the Part 5 complaint, the audit was relevant to the Part 6 investigation. My recommendations resulting from the audit are in **Section 8**.

3.5.3 It is important for readers to appreciate the difference between what a user of LEAP may see when using the database 'live' in real time and what a reader of audit data may see when examining material drawn from the archives of past LEAP use (**Section 2**).

3.5.4 Appreciating the difference allows the reader to recognise the validity of Jenny's concerns to stop any improper access to LEAP data about her by serving members of the Victoria Police, who have ongoing access to the system 'live' in real time. Appreciating the difference also assists an understanding of the implications for other people's privacy of OPI's loss of its file, which contained LEAP audit data (**Section 9**).

[1] Parliaments, when creating statutory complaints-handling systems, can recognise and facilitate this necessary liaison by providing appropriate functions and powers for referrals: see, for instance, *Information Privacy Act 2000* (Vic) section 29 (3), *Ombudsman Act 1973* (Vic) sections 15A and 20B.

4 OPI at the time of Jenny's case

4.1 Transition

4.1.1 Jenny's Third Complaint, addressed to the Ombudsman, was received on 16 November 2004, the day OPI came into formal legal existence.

4.1.2 Jenny's case almost exactly coincided with the period in which the Office of the Ombudsman was being internally reformed and, at the same time, the Office of Police Integrity, a separate statutory entity, was being grown from inside the Office of the Ombudsman. The Ombudsman and Director, Police Integrity are the same person, Mr George Brouwer.

4.1.3 Among many changes affecting both the Ombudsman's office and OPI during the relevant period, November 2004 to June 2005, two are of significance to the findings of the OVPC investigation.

4.1.4 The first was the review and upgrading of the records management and complaints-handling systems, which needed to be modernised both for existing Ombudsman functions as well as for OPI.

4.1.5 The second relevant type of change was to the staff. OPI grew from four to 80 staff in a year. Some of the long-serving staff from the Ombudsman's office left the organisation, or moved from the group handling complaints about police to join other parts of the expanding Ombudsman/OPI operations.

4.1.6 In any complaints-handling operation, the knowledge built up by the personnel who work on a particular matter, and the relationships that those personnel develop with both complainant and respondent, can be important. Familiarity with the facts and a certain continuity develop. These can improve accuracy, aid efficiency and promote mutually acceptable settlements. If, as in Jenny's case, it becomes necessary for others later to reconstruct what happened, this continuity can assist recall. In this case, the continuity was lacking because the relevant part of the Ombudsman's office – the part that handled complaints against police - was in transition to becoming OPI. Different staff, with varying experience, worked on different stages of Jenny's complaint.

4.1.7 Handling paper files and managing their location are partly physical tasks affected by environment. During the period relevant to Jenny's case, the Ombudsman/OPI office premises were remodelled. OPI staff shifted floors. In its early days, OPI lacked its own procedures, separate facilities and support staff. OPI relied on Ombudsman's office processes, which had themselves been reviewed, had been found to be in need of improvement, and were in the process of undergoing change.

4.1.8 In my view, these internal factors and the pressures they created contributed to OPI's inadequate handling of Jenny's case and its loss of its file of Jenny's case.

4.2 Effects on liaison

4.2.1 Internal change can also affect external relationships. During the period relevant to Jenny's case, there is evidence of unsatisfactory liaison between Ombudsman/OPI staff and Victoria Police. My comments should not be taken as findings about the past or current health of liaison between the whole of Victoria Police and OPI. Their interaction covers a wide field and involves many matters unrelated to LEAP access complaints or to ESD.

4.2.2 A measure of tension is natural and inevitable between a police force and the statutory organisation designed to provide independent oversight of police. Tension may be heightened when a new oversight organisation is created at a time of political controversy over how best to fight corruption, plug leaks in police data security and break a cycle of murders among criminals. These were the circumstances surrounding OPI's creation in 2004.

4.2.3 Even allowing for a degree of natural tension, in my view Jenny's case would have been better handled had the liaison between Victoria Police and Ombudsman/OPI staff been better. Victoria Police personnel arranged on OPI's behalf the audit of access to LEAP data. (OPI has since arranged its own access to LEAP and its own capacity to arrange LEAP audits through IBM.) Victoria Police did not provide assistance in interpreting the results of the audit data in Jenny's case. In the past, ESD generally had provided some interpretation of LEAP audit data to the Ombudsman/OPI staff dealing with a complaint. In Jenny's case, the raw LEAP data was simply conveyed in electronic form to OPI without ESD examining it, sifting it with software available to ESD, and providing advice to OPI.

4.2.4 Nor did ESD and OPI liaise effectively to ensure that the OPI complaint handlers took sufficient account of the background to Jenny's concerns. This background could have been gleaned from the ESD file on her 2001 complaint. While some of the material in that file was already replicated in the Ombudsman/OPI file, the complete file was located at ESD and police records indicate that it was not consulted at the relevant time.

4.2.5 If OPI, with ESD's co-operation, had reviewed the investigation of Jenny's First Complaint in the context of her Second, Third and Fourth Complaints, the OPI audit analysis is likely to have been more thorough, Jenny's core concerns would probably have been better addressed, and senior police management would have been better equipped to address staffing issues.

4.2.6 During the investigation, Victoria Police personnel stated that they lacked resources to do both their own work and OPI's. OPI has elsewhere reported that ESD was carrying a major workload at around that time.[1] In Jenny's case, however, it seems reasonable to conclude that another factor in the generally poor liaison was some strained working relationships. Just as some ESD personnel may not have been inclined to assist more than the minimum, some OPI personnel may have been disinclined to ask for or to accept sufficient ESD assistance. It is neither just nor constructive to attempt now to weigh and apportion blame among individuals.

4.2.7 Looking to the future, Jenny's case illustrates how, in practice, the deterrence, detection and investigation of misuse of personal information in police databases requires co-operation between Victoria Police – in particular ESD - and OPI. Progress is most likely to be made when the two liaise effectively. OPI will always need to be equipped with the powers, expertise and technology to act independently of Victoria Police in order for OPI to be an effective oversight body, but in practice the quality of liaison between the two organisations is important.

4.2.8 The inadequate liaison in Jenny's case may not have been typical of the relationship between ESD and OPI in relation to other matters. OVPC examined only this case, although in interviews staff of both Ombudsman/OPI and Victoria Police tended to remark on the difficult situation at the time.

4.2.9 As stated in paragraph 4.2.1, my comments should not be taken as findings about liaison between Victoria Police as a whole and OPI.

4.2.10 The OVPC investigation examined the draft Standard Operating Procedures for the Victoria Police Ombudsman Liaison Office in the Office of the Deputy Commissioner (Specialist Operations) and records of certain consultations with the Ombudsman over the Procedures in July 2004. Those Procedures set out a detailed framework for effective liaison. For instance, they stated in part: 'These guidelines are underpinned by a willingness to be open and frank with the Ombudsman investigators and assist in any way possible to determine the truth of issues under investigation.'

4.2.11 The experience of Jenny's case suggests that translating the Standard Operating Procedures from statements of intent by the most senior ranks into routine practice among all levels in both Victoria Police and OPI is likely to be an evolutionary process that will require monitoring.

4.2.12 Since the period in which Jenny's Third and Fourth Complaints were handled, significant personnel changes have taken place at OPI and ESD. A review of ESD began in 2004-05 and is due for completion in 2005-06.[2]

4.2.13 During the course of the OVPC investigation, Jenny expressed to OVPC her satisfaction with the progress of the fresh investigation that OPI had begun into her case. That investigation involved different OPI personnel from those who had handled her Third and Fourth Complaints.

[1] OPI *Annual Report 2004-05*, p 39.

[2] OPI *Annual Report 2004-05*, p 39.

5 Handling of Jenny's complaint by Ombudsman/OPI

5.1 Involvement of Ombudsman in First Complaint

5.1.1 The ESD investigation into Jenny's First Complaint in 2001 (**Section 3**) involved the Assistant Ombudsman (Police Complaints) Mr Brian Hardiman, who is also referred to in police documents as Deputy Ombudsman (Police Complaints).

5.1.2 It was then part of the statutory functions of the Office of the Ombudsman to oversee the handling by Victoria Police of complaints against police from the public, and Mr Hardiman and his senior staff would regularly meet officers from ESD to review the handling of complaints by ESD and consider what action was appropriate.

5.1.3 The ESD file states that the policewoman who had made unauthorised access to LEAP data about Jenny received 'counselling as directed by the Ombudsman'. The OPI file contains copies of some of the ESD file material. It also contains notes by Mr Hardiman. Both files record that police were to discuss with the policewoman and with management at the station where she worked the statement headed 'Discipline Action arising from misuse of LEAP', circulated by e-mail by the then Deputy Commissioner (Policy and Standards) Mr Peter Nancarrow on 13 December 2000.

5.1.4 The statement read as follows (emphasis in original) –

> Members are reminded that Force Command view the preservation of the integrity of the data contained within the LEAP database and other Force holdings as being of extreme importance. This position was recently confirmed in the Police Appeals Board decision relating to ...[name of a member] who appealed against dismissal from the Force as a result of discipline charges for inappropriate release of information being found proven against him.
>
> > *The Board wishes to communicate to members of the force that the LEAP system contains so much sensitive and private information that abuse of its use will be visited with the most severe sanction unless extenuating circumstances are proved. The need to deter misuse of the system is a strong factor in the disciplinary process and dismissal will be the most appropriate sanction in most cases.*
>
> Members should carefully consider any retrieval or release of information that is not ***strictly*** part of an investigation in which they are *directly* involved. Where any doubt whatsoever exists they should consult with a sub-officer or Officer for guidance prior to retrieving the information sought or requested. Members are reminded that Force databases including LEAP have audit capacities which can re-construct all activities performed within the database and that this information is held permanently. Members will be held accountable for all activities performed under their logon and should comply with policy and logoff at all times when not actually at the computer.

5.1.5 Mr Hardiman's notes also state that a copy of an Ombudsman's annual report reference to the LEAP issue was to be provided and discussed with the policewoman and local management.

5.1.6 The ESD file states that the policewoman was counselled on 19 February 2002 and that Jenny was advised of the outcome of Jenny's complaint. The ESD file indicates that 'the person reporting the incident was satisfied with the proposed action.'

5.1.7 The Victoria Police 'Public Incident Resolution' (PIR) process was followed by ESD in relation to Jenny's First Complaint. In the Ombudsman's Annual Report for 2001-02 the PIR process was discussed in a specific context. The Ombudsman stated in part that the PIR complaint procedure was promoted by police as a user-friendly, first port-of-call complaints procedure for less serious complaints. The Ombudsman noted the casual nature of the procedure and stated that it had little emphasis on the benefits of a structured mediation-conciliation process. Noting recommendations for replacing PIR in the specific context he was discussing, the Ombudsman then stated –

> It seems to me that many of these recommendations may have wider application and are timely because of the ESD's current review of the PIR procedure as a result of surveys indicating that the procedure could be improved.[1]

5.1.8 Notwithstanding the prominence that Jenny's case has since acquired, it is necessary to keep in mind that Jenny's First Complaint was only one among a total of 2,201 received in 2001-02, of which more than 1,300 were put directly to the Ombudsman[2]. Apart from handling Jenny's complaint itself, a senior manager could reasonably have seen it as an indicator of certain issues to be managed locally, and that it constituted another example of the wider issue of misuse of LEAP (an issue to which the Ombudsman had already drawn attention[3]). Viewed from a Victoria Police and Ombudsman perspective, the First Complaint would not have seemed as important as other matters then facing them. This is not to diminish its undoubted importance to Jenny.

5.1.9 However, and allowing for the acuity of hindsight, in my view the ESD file of the First Complaint, together with the relevant parts of OPI's file, in themselves provided a base that should have led to better handling by OPI of Jenny's Third Complaint in 2004 and Fourth Complaint in 2005. A combination of the information on file and the joint organisational memories of ESD and the Ombudsman/OPI should have led to a more thorough investigation of the Third Complaint. The OPI personnel who handled the Fourth Complaint lacked the organisational memory and did not see the ESD file or consult sufficiently to get the fuller picture necessary to a better result.

5.1.10 At its 2002 stage of development, Jenny's case exemplified an aspect of the wider problem of ensuring the security and proper use of personal information in LEAP. That aspect was the apparent gap between the firm policies of Force Command and the application of those policies in particular cases.[4]

5.2 November 2004 – Third Complaint arrives

5.2.1 Jenny's Third Complaint came in a letter dated 11 November 2004. It was received by the Office of the Ombudsman on 16 November 2004, the day OPI came into formal existence. The complaint was treated as an OPI matter.[5]

5.2.2 Jenny enclosed details of her Second Complaint, which was directed to the Federal Privacy Commissioner (**Section 3**).

5.2.3 In her letter, Jenny did not allege any further improper access to LEAP data about her. Rather, she gave background to her First Complaint and Second Complaint and sought the Ombudsman's guidance about appropriate action.

5.2.4 The file[6] was assigned to an experienced investigator. An acknowledgement letter to Jenny dated 14 December 2004 from Ms Sue Schwarz, Senior Investigations Officer (Police Complaints and Review), stated in part that 'because of the serious nature of your complaint this Office has decided to carry out preliminary inquiries to determine what further action is warranted.'

5.3 LEAP audit arranged

5.3.1 The preliminary inquiries involved a LEAP audit.[7]

5.3.2 Ms Schwarz was interviewed in the OVPC investigation. She stated that the Third Complaint would have been considered serious because it involved wrongful access to information and such matters had been treated particularly seriously because of recent publicity. The complaint would have been discussed with the investigator before a decision to seek an audit of access to data about Jenny. Audits were costly and Ms Schwarz did not authorise them unless there was an issue to be dealt with.

5.3.3 At that time, late 2004, liaison between the Ombudsman/OPI and Victoria Police was intended to be conducted under Standard Operating Procedures developed in July 2004 in consultation with the Ombudsman.[8] The Ombudsman Liaison Office (OLO) was headed by Superintendent Peter Teather. OLO was part of the Office of the Deputy Commissioner (Specialist Operations), Mr Peter Nancarrow. The primary role of the OLO was to provide a single entry point into Victoria Police for requests from the Ombudsman for documentation, interviews and resources.

5.3.4 On 16 December 2004, the OPI investigator e-mailed Mr Teather the text of a Confidential Memo headed with Jenny's real name, the Ombudsman/OPI file number and the reference number of the ESD file on the First Complaint. Mr Teather was asked to arrange for an audit to be conducted on LEAP access by two serving Victoria Police, the policewoman the subject of the First Complaint and her husband, 'as detailed in the issues of complaint listed'. The matters listed referred to allegations of unlawful access during 2002-2004 to LEAP in relation to Jenny and her husband, who is a serving member of Victoria Police. The outcome of the ESD investigation of the First Complaint was briefly described.

5.3.5 The proposed audit period covered the period from the time the First Complaint had been dealt with (January-February 2002) to the then present (December 2004).

5.3.6 Mr Teather made contact with the ESD Intelligence Management Unit, which formulated search strings for LEAP audits in liaison with IBM, the contracted service provider running the operating systems supporting LEAP. An ESD staff member asked Mr Teather to obtain from OPI 'better details for this request. The time frame is way too long, can it be refined to a shorter time frame.'[9]

5.3.7 Mr Teather asked Ms Schwarz or the OPI investigator to phone the ESD staff member to clarify directly with him the assistance OPI required.[10]

5.3.8 On 20 December 2004, the OPI investigator made the following file note in the electronic case management system -

> Called [ESD staff member] re this matter. He asked if I could narrow the search time frame. I reviewed the complaint and finally suggested May-September 2004 for both the complainant and [her husband]. He said that could be the starting point and if nothing comes up for that period I could reconsider whether further period needs to be looked at.

5.3.9 The OPI investigator and the ESD staff member were interviewed during the OVPC investigation.

5.3.10 The OPI investigator did not recollect what the ESD staff member had asked at the time they liaised about the time frame. The May-September 2004 period could have been related to an event that may have precipitated an occasion of access to LEAP. Or it could have been a matter of choosing the closest period in time and, if there were no result, then broadening the timeframe. How police actually did an audit was up to them. The OPI investigator, who could not recall ever having dealt with a LEAP audit before, did not see the results of the audit, having gone on leave just prior to Christmas and returned to a different role within OPI.

5.3.11 The ESD staff member stated that the suggestion to reduce the time frame had been his. The decision to do so had been the OPI investigator's. He said an audit of the whole two years would have taken between four and six months. If OPI wanted an earlier result the OPI investigator needed to cut the period for audit. There was competition for the available IBM time for audits from among various parts of Victoria Police as well as OPI. ESD had limited resources to design search strings and interpret audit results for others seeking audits. The ESD staff member confirmed that an audit time frame could be designed around dates of events relevant to an investigation. He outlined the ESD approach to designing search strings, which was resource intensive but regarded by ESD as the best approach to ensure that all the data involved has been collected. He observed that it was not an approach used throughout Victoria Police, and there were others with different views and methods.

5.4 Issues arising from the audit process

5.4.1 These varying approaches to LEAP audits have relevance to this investigation and to security of LEAP generally. They generate different amounts of data, some very large. The larger the audit dataset the bigger the amount of sensitive personal information that will be extracted from the LEAP archive, and the greater the number of people whose data will be involved, much of it irrelevant. Depending on the form in which the data is held (electronic or paper), and depending on how widely it is disseminated, the product of a LEAP audit can pose data security problems. The large datasets can also hinder rather than help an investigator, in the sense that they are very large 'haystacks' in which to find a 'needle'. The chances of efficient analysis of a LEAP audit dataset decline as the size of the dataset grows, especially if the investigator lacks appropriate search software, or has the data formatted awkwardly, or has only paper printouts to work with, or is insufficiently versed in what to look for.

5.4.2 The complexity of the privacy problem posed by OPI's loss of its file in Jenny's case relates directly to the amount of LEAP audit data the file contained (about 500 A4 pages).[11] The amount of LEAP data extracted relates directly to how LEAP audits are designed and conducted.

5.4.3 Similar issues have arisen – about a much larger amount of data – in the separate OVPC investigation of the disclosure electronically by Victoria Police, via IBM, of LEAP audit data to two employees of Department of Justice (Corrections Victoria). The broader issues are being addressed in that investigation and recommendations for improvements will be made in the report of that investigation.

5.4.4 Better auditing of access to LEAP is part of what is required to improve the security of personal information held by Victoria Police.[12] Technologically advanced capacity for swift and effective audit will be an essential element of the foreshadowed database to replace LEAP (together with strong security against loss or tampering for the audit trail itself).

5.4.5 Capacity for sophisticated and quick audits needs to be made widely known. If users believe the odds of being detected are high, deterrence is increased.

5.4.6 The ESD staff member stated that he did not see the results of the audit he arranged for OPI. He went on leave on 17 December. Police e-mail records show that the audit request was sent on 21 December 2004 from ESD-IT-Management to the staff member at IBM who at the time handled liaison with Victoria Police. The IBM staff member arranged for the audit data extraction from the main computer archive and on 29 December sent the results electronically to the ESD staff member's secure e-mail box. The ESD staff member was absent on leave, so another member of the ESD staff sent the audit data - without reading it, he stated at interview – to Mr Teather, who e-mailed at 8.17am on 30 December to Ms Schwarz at OPI, attaching the six files of data and noting that due to the large volume no hard copy would be forwarded. Mr Teather stated that he did not - and could not from a practical point of view - read all the data before passing it on to OPI.

5.4.7 The period from OPI's request for an audit to delivery of results to OPI was 14 days, which included Christmas.

5.5 Data security issues: multiple paper copies and transmission of unencrypted data

5.5.1 A printout of the data in the audit for OPI was retained on the OLO files in the Deputy Commissioner's office. When OPI's loss of the file was reported in the media in August 2005, a second paper copy of the audit data was made at ESD for its file on Jenny's case. Each copy amounts to about 500 pages.

5.5.2 I recommend that both these paper copies – and in due course the copy on the OPI file – be destroyed when they have served any necessary purpose.[13] Only the search strings should be retained, because with them the data can be retrieved from the main computer archive if required in future.

5.5.3 It is good data security practice and risk management to keep, for the minimum necessary period, only the minimum necessary number of copies of large amounts of sensitive personal information. If printouts of sets of LEAP data proliferate they can go astray as a set, or they can be dismantled and parts can be put to other uses which may expose the personal information to loss and unauthorised access.[14]

5.5.4 The audit data was unencrypted when it was sent by e-mail from OLO to OPI, a practice that is a serious data security risk when it involves sensitive personal information, particularly the large quantities that typically comprise LEAP audit data. During the OVPC investigation, Mr Teather advised me that the practice was being reassessed.

5.5.6 I recommend encryption of LEAP data - and the personal information in any other datasets - that travels electronically outside networks that Victoria Police has satisfied itself are secure to a standard commensurate with the sensitivity of the data.

5.5.7 The issue is unlikely to arise in the same way again for Victoria Police in relation to OPI because, since the 2004 audit in Jenny's case, OPI has arranged independent access to LEAP and, through IBM, OPI itself can obtain LEAP auditing. For the security of this, OPI will be responsible.

5.5.8 However, Victoria Police needs to resolve data security issues in contexts in which LEAP or similar data is authorised to flow, for proper purposes, to and from law enforcement agencies and other organisations in Victoria, interstate or overseas.[15] The flows can be expected to increase due to initiatives such as cross-border responses to terrorism and organised crime, Working With Children Checks and other criminal record screening, identity management projects and tighter fines enforcement.

5.5.9 Consultations in recent years between OVPC and Victoria Police indicate that the encryption issue is being addressed in the development of the Mobile Data Network, which will use wireless technology to give police access to datasets - including LEAP and presumably its successor databases - via terminals in police vehicles and, in future, hand-held devices.

5.6 30-31 December 2004 – Response to Third Complaint

5.6.1 The OPI investigator who had been handling the Third Complaint was on leave when Ms Schwarz received the audit data from Mr Teather on the morning of 30 December. Ms Schwarz stated that at about that time Ombudsman/OPI had 'an incredible volume of work'.[16] New staff were being brought in and trained. With no one to allocate files to, Ms Schwarz split them between herself and Mr Alan Hicks, a senior investigator with Ombudsman/OPI, who was of equal seniority to Ms Schwarz and occupied the office next to hers. She forwarded Mr Teather's e-mail to Mr Hicks at 11:07 am on 30 December.[17] Their equal rank meant that, in effect, Ms Schwarz had lost control of the matter and Mr Hicks was now solely responsible for it.

5.6.2 Mr Hicks printed out the audit data and combined it with the existing file material to make a file comprising two lever arch folders.[18] In the folders, each month of the six months of audit data is separated from the others by a coloured divider sheet.

5.6.3 Mr Hicks stated that he did not recall having had any prior knowledge of the matter and had no knowledge of the parties. He did not recall taking part in the decision to reduce the period for audit from two years to six months.

5.6.4 On 31 December, Mr Hicks made the following filenote in the electronic case management record of Jenny's case –

> Allocated this file on 30.12.2004. Downloaded all LEAP material received from Supt Peter Teather. See previous request from Sue Schwarz for LEAP records. Examined LEAP material. Unable to locate amongst material provided any record of either [policewoman's name and police member's number] or [policewoman's husband's name and number] accessing details of [Jenny]. Matter to be finalised.

5.6.5 Also on 31 December, Mr Hicks phoned Jenny to get details of her concerns. Notes in the OPI file indicate that Mr Hicks checked the police member numbers of the policewoman and her husband. Interviewed by OVPC, Mr Hicks stated that it had been unusual for him to be analysing raw LEAP data. Usually, ESD did it, investigated and made a report to the Ombudsman/OPI about any access detected and reasons for access, if any, and the Ombudsman would check and comment on any action taken or proposed.

5.6.6 Mr Hicks stated that over the period in question (December 2004) the office was working in something of a vacuum, being neither Police Ombudsman nor OPI. There was no standard operating manual about how to investigate complaints. Standards were being developed, and had been developed over the previous year about other matters.

5.6.7 Also relevant was the tension that had been experienced between OPI and ESD at around the time of Jenny's complaint (Section 4).

5.6.8 On 31 December, Mr Hicks sent Jenny a letter, the text of which is reproduced below without identifying details –

> **Subject: Your complaint against [name and number of a policewoman]**
>
> Thank you for your correspondence received 11 November 2004 and I also make reference to our telephone conversation of 31.12.2004.
>
> As I understand the situation your principal concern is the matter of your privacy in relation to any access concerning your personal details that may have been conducted of Police records and access to your personal correspondence by [policewoman named]. I note that you allege that [name] has breached your privacy rights and that you have referred this matter to the Victorian Privacy Commissioner for his attention.
>
> I also note that [ESD investigator named] conducted a previous investigation in December 2001 in relation to your allegation that [policewoman named] had previously improperly accessed your details on the Victoria Police Law Enforcement Assistance Program (LEAP). From your comments I understand that [name] was counselled for her actions on that occasion however my file does not provide me with a definitive outcome of that matter. I intend to seek advice from the Assistant Commissioner Ethical Standards Department (ESD) Victoria Police in this regard.
>
> In relation to your recent correspondence and at the instigation of this Office a further LEAP audit has been conducted between the period 2002-2004 in relation to any access to records pertaining to either yourself or your husband [name and number of husband]. I have examined the product of that audit and I have established that there is no record of any such access.
>
> Depending on the outcome of any action that the Victorian Privacy Commissioner may take on your behalf, if you feel that there are any outstanding issues concerning [policewoman named] in respect to breaches of your privacy through misuse of Police records I would be prepared to re-visit those further matters on your behalf.
>
> If you have any queries in the meantime please telephone me on [number given].

5.6.9 The references in the letter to the Victorian Privacy Commissioner mean the Federal Privacy Commissioner and Jenny's Second Complaint.

5.6.10 Mr Hicks wrote to the Assistant Commissioner ESD, also on 31 December, seeking details of any action taken against the policewoman for the apparent breach of LEAP protocols. Mr Hicks made a filenote on 10 January 2005 that an inspector from ESD had phoned him with details of the counselling in February 2002 (First Complaint).

5.6.11 Mr Hicks closed the file, as he was authorised to do.

5.7 Audit data analysed

5.7.1 I turn now to what the LEAP audit data contains about occasions of access to information about Jenny and her husband. I will then return to Mr Hicks' explanation of how he analysed the data.

5.7.2 The LEAP audit data on OPI's file was examined during the OVPC investigation.

5.7.3 The data covers the period April 2004 to September 2004, not 2002-2004.

5.7.4 No occasions of access to LEAP data about Jenny or her husband by the policewoman who had been the subject of the First Complaint, or by her husband, a policeman, were detected.

5.7.5 One occasion of access to data about Jenny by a different policewoman was detected. This access was also detected in the fresh audit conducted during the investigation by OVPC (**Section 8**) and the initial results were referred to the Chief Commissioner and to the Director, Police Integrity for further investigation. As **Section 2** explains, LEAP is a basic policing tool in constant daily use by police for myriad legitimate purposes. No adverse conclusion should be made from the simple fact of an occasion of access. It is necessary to investigate further the reason for the access and what was done with any information obtained.

5.7.6 The LEAP audit data on OPI's file contains 22 occasions of access involving data about Jenny's husband, a policeman. Two are the husband himself using LEAP in his policing work. Others are access by other police to data that mentions Jenny's husband, mostly in his policing role, for instance, as a victim in cases of assaults on police, or as the informant when he has been involved in charging people with offences. Jenny's husband's name also appears in lists of persons who have his name or a similar name. LEAP generates such lists in response to queries by members who may be dealing with an entirely unrelated matter involving a person of that name. Further investigation of these occasions of access to data about Jenny's husband is a matter for the Chief Commissioner and OPI. Jenny's husband requested that the fresh audit conducted by OVPC during this investigation not include an audit of access by others to data about him (**Section 8**).

5.7.7 The point for present purposes is that the LEAP data on the OPI file contained one occasion of access to data about Jenny and 22 to data about her husband. Mr Hicks letter of 31 December 2004 to Jenny had stated in part –

> In relation to your recent correspondence and at the instigation of this Office a further LEAP audit has been conducted between the period 2002-2004 in relation to any access to records pertaining to either yourself or your husband [name and number of husband]. I have examined the product of that audit and I have established that there is no record of any such access.

5.7.8 After the OPI file reached Jenny in June 2005, Jenny, her husband and a policeman friend familiar with LEAP audits found these occasions of access. They also noted that the audit covered only six months in 2004. They compared these facts with Mr Hicks' letter.

5.7.9 During the OVPC investigation, Mr Hicks was questioned in detail about the apparent discrepancies.

5.7.10 *On the audit time frame being six months and not two years* –

Mr Hicks stated that he had no recollection of the audit covering a period shorter than the two years to which his letter referred. He said he had no recollection of having read the file note by the first OPI investigator relating to her discussion with the ESD staff member to reduce the period of the audit. Mr Hicks said that if he made a mistake, it was because he had not looked at the dates of the audit data, but rather had referred to the memo on the file from Ms Schwarz to Mr Teather requesting an audit for 2002-2004.

5.7.11 *On the fact that the audit data did contain references to access to data about Jenny and about her husband* –

Mr Hicks stated that he examined the audit data for occasions of inappropriate access to data about Jenny by the policewoman who was the subject of the First Complaint and by the policewoman's current husband. He did this by looking for their individual police member numbers. (When a police member is logged on to LEAP, his or her unique number appears with his or her name. This number appears in LEAP audit data.) Mr Hicks said he was concentrating on the two persons that Jenny was alleging had looked her up on LEAP. He did not find the record of access by the other policewoman because he was not looking for access by anyone else. If he had found that particular occasion of access, he would have investigated further.

5.7.12 Mr Hicks stated that he could not recall that access to data about Jenny's husband had been part of the complaint. An OVPC investigator took Mr Hicks through each of the references in the audit data to Jenny's husband and Mr Hicks explained how he would have dealt with each of them if he had been looking for them and had found them.

5.7.13 I was present at two of the three interviews with Mr Hicks during the OVPC investigation. He was co-operative. His explanations of his work practices and of his approach to the analysis of LEAP audit data were plausible and given in a forthright manner. His phone call to Jenny, his follow-up with the Assistant Commissioner ESD and his offer to Jenny to re-visit the matter in future are indications of a good faith attempt to deal with the complaint.

5.7.14 I am satisfied that in writing the letter to Jenny dated 31 December 2004 Mr Hicks did not intend to deceive her or her husband about the length of the period audited or what the audit data contained.

5.7.15 Although I find there was no intention to mislead, I also find that a reasonable person in the position of Jenny and her husband would in fact have been misled by the way the letter was expressed.

5.7.16 In my opinion, the letter could reasonably be understood to mean that OPI had initiated the conduct of an audit of LEAP use between the period 2002-2004 in relation to any access to records pertaining to either Jenny or her husband, had examined the product of that audit, and had established that there was no record of any such access.

5.7.17 To read the letter in the way Mr Hicks recollects he intended requires a great deal of reliance on the words 'no record of any such access'. Those words alone have to convey to a reasonable person the meaning 'no record of any access by the policewoman or her policeman husband to LEAP data about Jenny'. In context, they fail to do so.

5.7.18 Given the history of the matter, and the fact that serving police were at the heart of Jenny's concerns, when Jenny and her husband read the OPI file and the audit data it contained they would have been understandably suspicious that they had been deceived by the letter of 31 December.

5.7.19 I conclude that they were let down by inadequate complaint-handling by OPI caused by the following factors operating in combination –

- The Office of Ombudsman/OPI was in a tumultuous period of change at the time the complaint arrived and was being handled.
- Ombudsman/OPI at that time lacked sufficient experienced staff for the complaint to receive the attention that the circumstances of the case merited, including sufficient experience in the design of a LEAP audit and analysis of raw LEAP audit data.
- Liaison between Ombudsman/OPI at that time was not working well enough to ensure that a complaint of this kind would be adequately handled and that the expertise Ombudsman/OPI lacked would be properly supplemented by expertise that existed in Victoria Police.
- A degree of superficiality, attributable at least in part to workload and the speed with which the matter was handled.
- The flaws had no prospect of being detected and corrected because in Ombudsman/OPI at that time a person acting alone could handle a complaint investigation, decide the matter, write the explanation to the complainant, dispatch it and close the file without a procedure to ensure that at least one other person in OPI of requisite experience had been consulted.

5.7.20 I recommend that OPI complaints-handling procedures ensure that no one person be able alone to investigate, determine, respond to the complainant and close any substantive complaint from a member of the public relating to the collection and handling of personal information by Victoria Police.

5.7.21 Regardless of the seniority of a person, he or she can always benefit from the views of a colleague who, having heard a summary or read a draft response, may make useful queries, suggest checks, or offer alternative approaches that may avert error or otherwise improve results.

5.8 May-June 2005 – Fourth Complaint

5.8.1 Jenny's Fourth Complaint, a letter dated 3 May 2005, was registered as having been received in OPI on 12 May.

5.8.2 Mr Hicks was on leave and had no involvement in OPI's handling of the Fourth Complaint. Ms Schwarz was preparing to leave the organisation after a considerable period of service and was managing the backlog of complaints. The recently appointed complaints manager, Ms Sue Tait, handled matters that were received after 18 April. Ms Tait allocated the Jenny matter to an OPI complaints handler who had joined OPI earlier in 2005. This meant that the two people who were to handle and decide Jenny's Fourth Complaint did not have the 'corporate memory' that may have given OPI's handling of Jenny's case better continuity.

5.8.3 Jenny's 3 May letter summarised previous events and renewed her concern about a policewoman having possession of a copy of a letter Jenny had written to a private business (Second Complaint, **Section 3**). Jenny wanted OPI to address the matter as an issue of police ethics.

5.8.4 The complaints handler reviewed the OPI file and produced a written summary for Ms Tait which noted in part: 'The allegation does not relate to [the policewoman] using her capacity as a police officer to gain or use information. The document [that is, Jenny's letter to the private business] does not appear to have been gained through the exercise of police authority.'[19]

5.8.5 After a series of draft response letters were worked on by the complaints handler under Ms Tait's supervision, Ms Tait finalised a letter to Jenny which she dated by hand 2 June 2005 when she signed it.

5.8.6 Her decision, in essence, rested on a distinction between the policewoman's personal life and action taken in the course, or purported course, of her duty as a police officer. Ms Tait's letter stated in part –

> On the basis of the information before me, I have not been able to detect any action by [policewoman named] that could be construed as misconduct or any other action that warrants disciplinary action under the Police Regulation Act.
>
> Accordingly, I am unable to take this matter further and now propose to close your file.

5.8.7 The letter also cited Mr Hick's letter of 31 December 2004 as having advised Jenny that 'the investigation into your previous complaint was unable to substantiate your allegation that [policewoman named] had misused police records to breach your privacy.'

5.8.8 The substantive issue on which Ms Tait's decision rested will not be considered in this Report. The ethical standards expected of police on and off duty are matters for decision-makers other than the Privacy Commissioner to determine.[20] A new investigation has been opened into Jenny's case by the Director, Police Integrity. I have recommended to Victoria Police and OPI that either or both of them investigate further the initial findings of the fresh audit described in **Section 8** of this Report. Those processes will consider the application of relevant law and ethical standards to the facts found.

5.8.9 My comments are directed solely to the issue of how OPI handled the Fourth Complaint and any lessons that may be derived. I find that, as with the Third Complaint, the time the Fourth Complaint was handled was a time of transition in which OPI was still being grown out of the Office of the Ombudsman. Part of this process involved recruitment of new staff who were augmenting and replacing, at various levels of the organisation, staff who had within themselves a significant amount of 'corporate memory' about handling police complaints in general and about certain recurring matters. Jenny's case was one such matter.

5.8.10 It was reasonable for the OPI complaints handler and Ms Tait to rely on Mr Hicks' findings in relation to the Third Complaint. They were entitled to assume an experienced investigator had a sound basis for the statements in the letter dated 31 December 2004. However, in this reliance they unwittingly compounded the flaws in the handling of the Third Complaint.

5.8.11 OPI's handling of the Fourth Complaint would have been improved by OPI obtaining from Victoria Police and assessing for itself the ESD file on the First Complaint and by checking the status of Jenny's Second Complaint, which had been made to the Federal Privacy Commissioner for jurisdictional reasons and which was referred to in Jenny's 11 November 2004 correspondence.[21] The Second Complaint was self-evidently important. It was of such concern to Jenny she had renewed on 3 May 2005 her complaint of 11 November 2004.

5.8.12 Jenny received Ms Tait's letter of 2 June in an envelope taped to the package that contained the original OPI file (**Section 6**). Jenny was then able to compare the letter with the material on the file relating to the ESD investigation of her First Complaint, and with the LEAP audit data generated during OPI's handling of her Third Complaint. She would have reasonably inferred that this constituted what Ms Tait had referred to as 'the information before me'.

5.8.13 Jenny's subsequent correspondence to OPI – as well as correspondence from, and interviews with, Jenny during the OVPC investigation – indicate, in detail, that Jenny:

- did not regard the initial ESD investigation in 2001 as having been adequate and she refuted part of its findings, which had been made without the investigator interviewing her;
- was not as satisfied with the Public Incident Resolution process in 2002 as the ESD file may have conveyed (First Complaint);
- believed OPI should have investigated her Third Complaint and her Fourth Complaint more thoroughly and should not rely only on information from ESD;
- wanted to know why the LEAP audit for the Third Complaint had not covered the period 2002-2004 and why the original OPI file with LEAP audit data had been sent to her;
- now knew the LEAP audit data contained an occasion of access to data about her and occasions of access to data about her husband by police and believed that that access ought to be further investigated by OPI; and
- particularly wanted the Second Complaint dealt with and wanted to put a stop to what she regarded as the potential for serving police to obtain and use personal information about Jenny and her husband.

5.8.14 It is rare for a complaints-handling entity to be placed in the position in which the mailing of its original file to Jenny put OPI. The complainant's knowledge in many ways became better than the complaint-handling body's, because Jenny personified continuity whereas the handling of Jenny's Third and Fourth Complaints had coincided with the discontinuity created by the transition and growth processes of Ombudsman/OPI in 2004 and 2005.

5.8.15 The detail of OVPC's investigation has sharpened hindsight to a degree that should produce caution in those who judge now the people whose circumstances and knowledge at an earlier time were vastly different. That caution having been sounded, it can fairly be concluded that Jenny and her husband have been let down by the complaints handling processes and it is appropriate that fresh investigations are underway.

5.8.16 But the prominence of this matter ought not in itself affect its fair resolution on its merits.

5.8.17 The details of Jenny's case are intimately private, and not just to Jenny and her husband, but to others who must also be treated fairly.

5.8.18 The result of the Federal Privacy Commissioner's handling of the Second Complaint was not available at the time this Report was finalised. It may not be appropriate for detail about that investigation and decision to be made public.

5.8.19 It is now for OPI and Victoria Police, in light of the Federal Privacy Commissioner's decision, my findings and their own fresh investigations to consider again Jenny's case.

---

[1] Ombudsman Victoria, *Annual Report 2001-02*, p 26.

[2] Ibid p 53. OPI's *Annual Report 2004-05* indicates that it received direct 2,350 of the 3,561 complaints against police received that year (p 30).

[3] For example, Ombudsman Victoria, *Annual Report 2000-01*, p 20.

[4] Recent signs suggest the gap is closing. This issue will be further addressed in the OVPC report of its separate investigation into another case of LEAP audit data disclosure involving Victoria Police and Department of Justice (Corrections Victoria).

[5] The *Police Regulation Act* allows a discretion for OPI to determine that it is in the public interest for OPI to investigate a complaint itself rather than refer it to Victoria Police.

[6] The development of the material on the file is explained in Section 6.

[7] LEAP audit data is described generally in Section 2 and in a specific context in Section 9. Section 8 illustrates part of the process of auditing LEAP access.

[8] See Section 4.

[9] E-mail 17 December 2004.

[10] E-mail 17 December 2004.

[11] Section 9.

[12] See also OPI, *LEAP Report* (2005) for an analysis of some of the flaws and proposed remedies.

[13] Information Privacy Principle 4.2.

[14] As illustrated by the practice of police at Frankston Police Station recycling printouts of LEAP data for use as notepads. A visitor to the station removed some sheets. The practice was ordered to stop after it was brought to light in the media in October 2005.

[15] IPP4 (data security) and, to the extent applicable to police, IPP9 (transborder data flows).

[16] In OVPC's experience, this is not unusual when a complaints-handling body is in the news media, as OPI was, because public awareness of its existence increases, so enquiries and complaints increase.

[17] Mr Hicks' diary and a file note in the electronic case management system also show him being allocated the file on Jenny's case on 30 December.

[18] The physical state of the file is relevant to my findings about how OPI lost it, Section 4.

[19] Filenote, OPI case management system, 17 May 2005.

[20] See Section 1, The Limits of Jenny's Case.

[21] See Section 3.

6 How did the OPI file get to Jenny?

6.1 How the file developed

6.1.1 How OPI investigated Jenny's complaint is examined in **Section 5**. For the moment, the focus is solely on how the OPI file developed physically and what happened to it. In 2001 Jenny complained to the Victoria Police Ethical Standards Department (ESD) about improper access by a policewoman to personal information about Jenny.[1] At that time, part of the role of the Ombudsman was to be notified about complaints against police, liaise with ESD about how matters would be handled, make recommendations and be advised of any follow-up action.

6.1.2 This liaison between ESD and the Ombudsman meant that some material about the 2001 investigation was already on file at the Office of the Ombudsman when Jenny's complaint of November 2004 was received.[2]

6.1.3 The earlier material and Jenny's new complaint were amalgamated into one file.

6.1.4 At the time, the complaints files of the Senior Assistant Ombudsman (Police Complaints) were pale blue manila folders. They would be marked with a file number, complainant's name, investigating officer's name, date of creation and date of completion. A string and button in the top left corner held the pages together.

6.1.5 This is how the file looked when in late December 2004 it was assigned to a senior complaints handler, Mr Alan Hicks. Mr Hicks preferred to work with files that were in folders. He dismantled the Ombudsman string-and-button file, cut down its blue cardboard cover to retain its basic data such as file number, added the printouts of the LEAP audit data obtained from Victoria Police, hole-punched it and placed everything into two lever-arch folders. He attached labels to the spines of each folder identifying the contents with the file number and the words 'LEAP PRINTOUTS FOR PERIOD 2002-2004 ACCESS BY [name and number of police member] AND [name and number of police member] FOLIO [1 and 2 respectively]'.

6.1.6 In this form, the OPI file looked like police material. It contained:

- the ESD and Assistant Ombudsman (Police Complaints) material about the First Complaint;
- correspondence from Jenny about the Second Complaint and the Third Complaint, and copies of OPI correspondence to Jenny;
- some of the communications between OPI and Victoria Police about the Third Complaint; and
- about 500 pages of LEAP audit data.[3]

6.1.7 Folio 1 contained the material in the first three categories and some LEAP audit data. Folio 2 contained LEAP audit data only.

6.1.8 However, the external form of the file – that is, two folders – by now resembled the Victoria Police materials that would regularly be transferred to and from Assistant Ombudsman (Police Complaints) in the process of liaising with ESD over complaints.

6.1.9 At that time, staff in Ombudsman/OPI were more used to complaints files being in the blue manila folders with string-and-button fastenings. It was not common for large amounts of LEAP audit data in paper form to comprise parts of Ombudsman/OPI complaints files. If a staff member not familiar with Jenny's case had opened Folio 2 to check what kind of file it was, he or she would have found only LEAP audit data. It would have been reasonable for such a staff member to infer that the folder – and its companion folder, Folio 1 – comprised Victoria Police material.

6.2 Tracking the file in the office

6.2.1 The OVPC investigation included detailed work, by independent expert consultants appointed by the Privacy Commissioner, into the records management and mailing systems of OPI.

6.2.2 One strand of the investigation attempted to reconstruct the exact movements of the file of Jenny's case within the OPI office. Another strand traced the creation of the letter of 2 June 2005, which was OPI's response to Jenny's Fourth Complaint. One aim was to find out how and when the file and the letter came together. Another aim was to determine precisely how the file came to be wrapped instead of put into storage, how the enveloped letter was attached to the wrapped package and how the package made its way to Jenny. An important extra objective was to identify any weaknesses in the OPI facilities and procedures so that, if they still existed, they could be remedied in order to prevent a recurrence. It is in the nature of OPI's statutory functions that it handles sensitive information with implications for public interests other than privacy protection.

6.2.3 The OVPC investigators used a variety of information sources including floor plans, systems logs, organisation charts, rosters, electronic case management data, and word-processing records. Interviews were conducted with Ombudsman/OPI staff, contractors, courier and postal service providers, security and Victoria Police staff. The investigators were hampered by a lack of some information which either was not captured at all by the systems then in use at OPI or had been captured but overwritten between the relevant period leading up to the dispatch of the package on or about 2 June 2005 and the date OPI had been informed of its loss of its file (4 August 2005; file returned 5 August).

6.2.4 Weaknesses in facilities and procedures were found to have existed at the relevant time and these are described generally in this Report. Detailed analyses by the experts have been provided to the Director, Police Integrity, together with recommendations for systems improvements.

6.2.5 This section of the Report deals only with how the OPI file is most likely, on the balance of probabilities, to have left OPI and come into Jenny's possession.

6.2.6 For these purposes, at this point in the Report we pick up the file's trail in the Ombudsman/OPI office on 31 December 2004, when the investigator Alan Hicks finished handling Jenny's Third Complaint (**Section** 5).

6.2.7 Readers will recall that Mr Hicks had closed the Jenny matter in the electronic case management system after handling the Third Complaint (**Section** 5). The practice at the time in Ombudsman/OPI was that a 'closed' file could be worked on again without formally re-opening it. The processes for re-opening a file in the case management system then in use were regarded as tedious, and staff stated that it was sometimes easier to write a letter and place it on a closed file rather than re-open it. The effect is that in the case management system records the status 'closed' does not preclude further entries being made. It is a questionable records management practice. OVPC was advised that this practice has been changed.

6.2.8 Mr Hicks stated that if a file comprised two lever arch folders he would sometimes tie them together with white ribbon before handing them over for filing. He did not recall what he had done with the file of Jenny's case, but he expected that he would have physically handed the folders to the staff member who oversaw filing for the file to be returned to a storage compactus. At that time, the compactus was not locked and anyone could access it. OVPC was advised that access to the compactus must now be made through records staff.

6.2.9 Jenny's Fourth Complaint was a letter received in OPI on 12 May. A recently appointed complaints handler was assigned to Jenny's case on 17 May by the manager of complaints, Ms Sue Tait.

6.2.10 Paper files, which had been inherited from the former Police Ombudsman system, did not at the time have a front coversheet to record the names and dates of the files' movements within the office. OVPC was advised during the investigation that this had been remedied.

6.2.11 The electronic case management system then in use in Ombudsman/OPI overwrote the earlier custodian data every time custody of a file was changed. Such a system relies on prompt, accurate updating of who has custody of a file at a given time so that it can be located if needed. Management have since advised OVPC that the inadequacy of the case management system had been recognised at the time and that Ombudsman and OPI were both in the process of introducing updated case management systems, each tailored to the needs of the two entities.

6.2.12 The relevant registry staff stated that they had no recollection of retrieving the file of Jenny's case from the special bays in the compactus where large files were kept.

6.2.13 The log for the case management system shows that the file was extracted from its location in the large files area on 26 May 2005 and marked to Sue Tait by the complaints handler to whom she had assigned Jenny's Fourth Complaint. Other evidence contradicts this data. The complaints handler stated that the folders were on Sue Tait's desk when he took possession of them. The file shows evidence of work on it on 17 May. The most likely explanation is that the original movement of the file from storage to Sue Tait was not recorded, nor the original movement of the file from Ms Tait to the complaints handler, but that the complaints handler did record the movement back to Ms Tait when on 26 May he gave her a draft response letter to Jenny, which he attached to the file.

6.2.14 The complaints handler stated that he clearly recollected the two folders. While he worked on the matter, he stored them in the locked filing cabinet at his desk. At first, he attached to the folders his draft response letters to Jenny and provided everything to Ms Tait for reference. However, both the complaints handler and Ms Tait stated that Ms Tait sent back drafts for revision on more than one occasion. The complaints handler stated that as the exchanges wore on he had kept the folders in his possession and given only the revised drafts to Ms Tait until he was finished his part in the process.

6.2.15 Ms Tait stated that she had no recollection that OPI's file of Jenny's case was comprised of two lever-arch folders. She stated that when she first learned of the loss of the file she thought it must have been one of the old Ombudsman string-and-button files and that this would be embarrassing because the files were so old-fashioned and because OPI had by then introduced new complaints files which were a distinctive bright blue, contemporary in design and better able to be tracked.

6.2.16 Properties metadata from the word processing system shows that the version of the 2 June letter that was sent to Jenny was printed at OPI at 12.50pm on 2 June. The original of the 2 June letter signed by Ms Tait is in Jenny's possession. During the OVPC investigation it was sighted by me, and Jenny provided copies. There should be a copy of it on blue paper on the OPI file that went to Jenny and was returned, but there is not.

6.2.17 At OPI at the time, file copies of correspondence were printed on particular blue paper and staff refer to these copies as a 'blue'. When the file was returned to OPI on 5 August 2005, it contained a blue copy of one of the drafts which was similar in wording to, but not the same as, the final 2 June letter. On the draft, the month printed is May, with no date handwritten or typed. Jenny stated that this was the first document on the file when she received it.

6.2.18 The significance of the May blue copy being on the file but there being no blue copy of the final 2 June letter, is that the person who produced the correspondence would normally produce the blue copy and arrange for the signed letter, blue copy and relevant file to be taken physically to the mailing/filing area. The outwards correspondence would be attached to the file with the blue copy. The correspondence was intended to be dispatched, and the blue copy, having been marked to show that the original had been dispatched, was intended to be added to the file prior to the file going into storage.

6.2.19 Ms Tait stated that she would have created a blue copy had she been the person taking the material to the mail room. Ms Tait indicated that she signs or initials blue copies and she might put a line through an old draft version. The May blue copy on the file has no line through it. There is no blue copy of the 2 June letter on the file. Ms Tait stated that there might have been a chance that she pulled the wrong blue copy off the file. That is, Ms Tait might have pulled off the blue copy of the 2 June letter, which is not on the file, instead of pulling off the blue copy of the old May draft, which is on the file. This is no more than a possible explanation, but it is a plausible one.

6.2.20 In the absence of evidence or a clear recollection by the relevant staff, I can make no definitive finding as to why the file, when returned to OPI, contained no blue copy of the 2 June letter sent to Jenny. Another plausible explanation is that the blue copy was lost during the period the file was out of OPI's custody.

6.2.21 The available evidence does not allow a definitive finding to be made about whether it was Ms Tait or another person who delivered the signed letter and the two folders that comprised the file to the mailing/filing area of the office on or about 2 June.

6.3 Dispatch

6.3.1 At the time of the loss of the file, the Office of Ombudsman and OPI shared the same mailing/filing facilities. The area has since been demolished and OPI now has separate facilities on a different floor from the Ombudsman.

6.3.2 At the time, the area of the office where the mail was processed and dispatched was also the area where staff brought files to be returned to storage and files to be returned to Victoria Police, usually the ESD.

6.3.3 At the time, a secure area in the north-west corner of the office was where basic preparation and sorting took place. In a non-secured area on the east side, the final addressing, franking and sorting into standard mail or items for DX delivery took place. Location data that could have pinpointed better the whereabouts of particular staff on the days in question was not available to OVPC investigators, having been overwritten by the time of the investigation. Recommendations for longer retention periods for this and other key data have been made to OPI.

6.3.4 Complaints-handling staff tended to rely on the mailing/filing staff to analyse the correspondence and files to determine their correct treatment. Put broadly, there were three options: mailing; storage at Ombudsman/OPI; or return to ESD.

6.3.5 The files of Jenny's case comprised two lever-arch folders and would have been too big to fit into the pigeon hole of the staff member who normally would have put files back into storage when they were not in use. This being so, the two folders would have been left on the bench under the pigeon holes. This was the same bench on which sat the trays for outward mail and for material to be returned to Victoria Police.

6.3.6 There were no written instructions to follow. The staff working in the area at the time had varying levels of experience, from a recruit under supervision to a long-serving and experienced staff member.

6.3.7 The material to be returned to ESD usually went in a particular type of sealed bag by a specific courier method. The two folders would not have fitted in one of these bags. A register was supposed to be kept of the items that had been returned to ESD. The register was inspected at the time the loss of the file became known and was found to be in some disarray. (It contained no reference to the file of Jenny's case.)
One OPI staff member and one Victoria Police staff member, interviewed separately, recalled one past incident in which OPI material had mistakenly been sent to Victoria Police and had had to be returned.
OVPC has been advised that it is now the specific responsibility of one particular OPI staff member to keep this register in proper order.

6.3.8 On the weekend immediately following the most likely dates for the 2 June letter to have been dispatched to Jenny, OPI staff moved to another floor. Preparations for that move were underway in the week prior.

6.3.9 The mailing/filing facilities and procedures of Ombudsman/OPI at the time were such as to make the mistaken dispatch of a file with a letter likely.

6.3.10 The facilities and procedures did not amount to the reasonable steps required for data security in an organisation such as OPI. They were not commensurate with the sensitivity of the material being handled and the serious potential consequences of such material going astray - for complainants, for third parties named in complaints, for Victoria Police and for OPI.

6.3.11 The facilities, when combined with the process, placed too much reliance on judgments being made by staff who could not, without much more precise instructions, be expected to know how to recognise and treat the particular materials being delivered to them by other staff.

6.3.12 The mailing/filing staff on duty on the relevant days stated that they could not recall specifically the 2 June letter to Jenny or the OPI file of Jenny's case or the parcel containing the file with the letter taped to it. A parcel of that size would not have been able to be posted in what was the usual way, placed in a mail box in the street near the OPI office. No staff interviewed could recall carrying a parcel of that size at around that date to the nearby post office where large-size items would be posted over the counter. Australia Post has no records of such an item. No relevant CCTV footage exists. The fact that the parcel was franked is the only evidence that the parcel may have gone by post direct from OPI to Jenny. However, that evidence does not exclude the other route which, for other reasons, is more plausible.

6.3.13 In the absence of sufficient evidence, it would be unjust to name the relevant mailing/filing staff who may have contributed to the mistaken dispatch of the file with the letter. No evidence was found of malicious intent or negligence by those staff.

6.3.14 Based on the available documentary evidence and on interviews with relevant personnel, on the balance of probabilities the most plausible explanation for how it happened that the OPI file of Jenny's case reached Jenny is as follows –

- The two folders, with the signed 2 June letter attached to the front of one of the folders or just inside it, reached the mailing/filing area on Thursday 2 June or Friday 3 June.
- Staff member X removed the letter to Jenny, folded it and placed it in an envelope with a plastic window through which Jenny's name and post office box address were visible.
- X then placed the two folders in or near the tray for material to go back to ESD. (It has been explained how the file had come to resemble police material – see 'How the file developed' above.)
- X asked staff member Y to wrap the folders because X was not so familiar with that process.
- Y assumed X had sorted the folders, so Y did not question whether they were intended for return to ESD.
- Y wrapped the folders (in a manner that matches the way they were wrapped when Jenny received them – see 'Delivery to Jenny' below) and placed the parcel in the tray for items intended for return to ESD.
- Items were carried from the north-west secure area to the eastern area of the floor for franking and dispatch.
- Seeing the letter with the parcel, X assumed the package needed franking, weighed it, franked the envelope and either X or Y attached the envelope and franking label to the parcel.
- X or Y, still under the impression that the contents of the parcel were for ESD and not having noticed Jenny's name and address on the envelope by now taped to the parcel, arranged for the parcel to leave OPI's office with other ESD items picked up by the company that operates the DX service.
- Then, either

  at the DX mail centre in an inner suburb of Melbourne, Jenny's name and address were noticed by sorting staff and the parcel was removed from the container dedicated to Victoria Police items and placed into the bin for items to be re-directed to Australia Post

  or

  the parcel was sorted into the Victoria Police DX mail and delivered to the main Victoria Police mail centre where Victoria Police mailing staff, examining it for information about whom to direct it to, saw Jenny's name and address and themselves re-directed it to Australia Post without opening it or having knowledge of the contents of the parcel.
- Australia Post delivered the parcel.

6.3.15 No evidence was found that the parcel reached ESD and was from there re-directed to Jenny.

6.4 Delivery to Jenny

6.4.1 Jenny's mail is delivered to a box at the small post office near her home in country Victoria.

6.4.2 The original notice, which would have been in Jenny's post office box informing her that a parcel awaited collection at the counter, was unavailable to OVPC investigators because the notices are recycled, not filed. They are not unique to the item or to the addressee. The post office staff interviewed did not recall a parcel of this description among the many they handle.

6.4.3 Jenny stated that she collected the parcel from the post office on 14 June 2005. Her description of the wrapping matches the manner in which the Ombudsman/OPI mailroom at the time wrapped parcels containing lever-arch folders: the folders tied together with white cotton tape; covered with plastic bubble wrap; and then wrapped in brown paper; with the franked envelope attached by brown tape to the outside of the parcel, address visible through the clear window of the envelope.

6.4.4 The parcel's actual wrappings were unavailable to OVPC investigators for analysis and comparison with OPI's wrapping materials. Jenny stated that when she got home from collecting the mail she threw the wrappings into the fire in front of her in her living room as she sat on the sofa opening the parcel.

6.4.5 Jenny stated that she would not always pick up mail from her post box daily, and that sometimes several days would go by before she checked its contents. On the basis of a dispatch date from OPI of 2 or 3 June, allowing time for misdirection to Victoria Police, for that misdirection to be corrected, and for the item to make its way through the Australia Post system, the period from dispatch to receipt of the parcel by Jenny would be within the expected span. The period aligns with audit data on Australia Post delivery times for Victorian country areas.

6.4.6 The OVPC investigation could locate no log, incoming or outgoing mail inventory, computerised scanning data, franking machine records or security camera footage of the parcel in transit through the systems of OPI, the courier company OPI uses, Victoria Police or Australia Post. Investigators were advised by the relevant organisations that such records either did not exist or had been overwritten or otherwise routinely disposed of in the period between dispatch of the OPI file and its return.

6.4.7 Available evidence is consistent with Jenny having obtained the folders comprising the OPI file in a parcel received through the post.

6.4.8 No evidence was found to indicate that the OPI file came into Jenny's possession any other way.

---

[1] First Complaint, Section 3.

[2] Third Complaint, Section 3.

[3] For a general description of LEAP audit data, see Section 2.

7 What happened to the file before its return to OPI?

7.1 The file was out of OPI's custody for nine weeks without OPI being aware of that fact.

7.2 This was the period of greatest risk to the privacy of those whose sensitive personal information was among the LEAP audit data in the file.[1] The printouts were readily able to have been copied and further disseminated.

7.3 During the investigation I sought and received assurances from Jenny, her husband and others known to have had possession of the file that they had not made copies of the LEAP audit data.

7.4 Jenny stated that she took the parcel home unopened. It was a cold day and she sat in front of the fire. She removed the paper and plastic wrapping and put it in the fire, having first removed the envelope containing the letter from OPI. She cut the cotton tape that bound the two folders together. In a letter to the Privacy Commissioner, Jenny wrote:

> Opening the first binder I saw a copy of the letter I had just opened from the front of the parcel.[2] The next section of the binder revealed my original documents sent to the OPI and their original correspondence to and from ESD for information pertaining to my complaint. My first thought was: 'Why on earth...'
>
> The second section of the folder revealed LEAP records of persons unknown to myself with personal information, telephone numbers, addresses, criminal history, ethnic origin and sexual preferences.
>
> I slammed the binder shut! I sought out my husband and told him I had opened the parcel and said 'there is something very, very, very wrong here.'
>
> Being a Police Officer, he quickly ascertained that the documents were LEAP records of a similar surname to us.

7.5 Jenny's husband found the references to him in the LEAP data.[3]

7.6 They sought the advice of a policeman friend who had formerly worked at ESD and was familiar with the LEAP audit process. The man was interviewed during the OVPC investigation. He stated that Jenny and her husband had brought the folders to his office at a police station for him to examine them. He could not recall the date. He had custody of the file overnight at his home while he examined it. The file was genuine; he believed it had been sent to Jenny through a clerical error, not deliberately. He found in the LEAP audit data that there had been access to data about Jenny and Jenny's husband. The audit had not been thorough enough and, having also read the correspondence on the file, he concluded that OPI had not been truthful and had misled Jenny. He contacted Jenny, told her what he had found and concluded and asked her to collect the file from him.

7.7 He stated that he was familiar with Jenny's frustration over her complaint and the background to it. He advised Jenny and her husband to go to a Member of Parliament. He contacted Mr Richard Dalla-Riva MLC, with whom he had worked in the past, and was advised to contact Mr Kim Wells MLA, the Opposition spokesman on police matters.

7.8 Interviewed by OVPC, the policeman friend of Jenny stated that he had not contacted ESD. His recollection was unclear about whether he had advised his superior at the station where he worked, a superintendent, about the matter.

7.9 The issue was of significance to OVPC's investigation into a serious privacy breach. In such cases, the first priority is to contain the breach. If Victoria Police members of the rank of superintendent or above had knowledge that an OPI file containing a large amount of LEAP audit data had been lost by OPI and was in the hands of a member of the public, they would have had an obligation to act. Knowledge in officers of those ranks, in my view, would have meant that Victoria Police, as an organisation, would reasonably have been regarded as having knowledge of the matter. If the organisation had the knowledge, at a minimum Victoria Police would have been obliged to alert OPI.

7.10 For reasons specific to the circumstances of this case, it was not appropriate for OVPC directly to investigate this aspect of the matter. Accordingly, I requested the Chief Commissioner to inquire on her own authority whether any Victoria Police officers equivalent or superior in rank to superintendent were informed by the superintendent at the relevant station or by Jenny's policeman friend that the OPI file was in the possession of Jenny, the policeman friend or Mr Wells prior to 5 August 2005, the day the matter was first reported in the media.

7.11 The Chief Commissioner arranged for an investigation to be conducted by an Assistant Commissioner. The Chief Commissioner advised me on 10 January 2006 that, on the information provided to her, she accepted that neither the superintendent at the relevant station nor any officers equal to or superior in rank to him had any knowledge of possession of the OPI file by Jenny, Jenny's policeman friend or Mr Wells prior to 5 August 2005. I accept the Chief Commissioner's assurance.

7.12 Jenny stated that she contacted Mr Wells on 21 June 2005. Arrangements were made and she took the file in a recycle shopping bag to a meeting in a restaurant in a country town on 24 June 2005. Jenny stated that a member of Mr Wells' staff met her there and, after satisfying herself as to his credentials, Jenny handed him the file. Mr Wells and his staff arranged for the file to be viewed by two journalists, Ms Josephine Cafagna from the ABC TV program *Stateline*, and Mr Paul Austin, from *The Age*. Jenny was interviewed for *Stateline* and also spoke to Mr Austin.

7.13 OVPC did not investigate Mr Wells' actions in this matter, having no jurisdiction to do so. Members of Parliament are not covered by the *Information Privacy Act*.[4] Also, longstanding privileges apply to MPs acting in the course of their duties as Members of Parliament, and these must be respected by statutory regulators. I wrote to Mr Wells on 9 August 2005, stating that I was not investigating his actions, explaining that my first priority was to establish that the sensitive personal information relating to a large number of individuals had been made secure, and requesting confirmation that the information had been secured when in his custody.

7.14 One of Mr Wells' parliamentary colleagues, Mr Andrew McIntosh MLA, wrote to me on 25 August 2005, stating that no copies existed of the private information supplied by Jenny and handed to the OPI, and that save for two members of Mr Wells' staff and the two journalists no other person (including members of Parliament) had been provided access or afforded details of the private information. I accept Mr McIntosh's assurance.

7.15 OPI learned about the loss of its file on 4 August 2005 from a journalist from the ABC *Stateline* program.

7.16 Mr Wells handed the file back to a staff member from OPI at Parliament House on 5 August 2005.

7.17 The matter was first reported in public on the *Stateline* program that evening. Jenny appeared on the program with her face and voice recognisable, although her real name and the geographic location were not given.

7.18 In a letter to the Privacy Commissioner during the course of the investigation, Jenny stated that she had originally asked for anonymity but had been told that credibility was higher if a person was prepared to face the camera. I accept that this is a standard journalistic approach.[5] However, privacy cases require particularly careful handling by the media. They can be reported fairly without exacerbating harms such as avoidable new privacy breaches. This matter undoubtedly involves issues of genuine public interest. Journalistic scrutiny is appropriate. Jenny, like anyone, has a right to be heard. But the privacy interests are also weighty.

7.19 Disclosure and identity protection often need to be balanced in journalistic decision-making. It would be prudent if the identity of Jenny were more carefully protected in any future media reporting. This would be more likely to ensure continuing protection of her privacy and the privacy of others involved in the circumstances of this case, while at the same time ensuring that the public interest issues are aired.

---

[1] Section 2 and Section 9 explain the privacy issues in more detail.

[2] The wording was almost an exact copy. Jenny was describing what appears to have been the blue copy of a May draft, still on the file, of the 2 June letter (Section 6).

[3] See Section 5.

[4] Unless they are Ministers or Parliamentary Secretaries: section 9(1).

[5] Jenny stated that the journalists and Mr Wells and his staff had acted with integrity in their dealings with her. She also acknowledged Mr Brouwer's apology and his assurance of another investigation, given in a letter to her dated 5 August 2005.

8 Fresh audits of access to LEAP data about Jenny

8.1 As **Section 5** outlined, Jenny reasonably understood OPI's letter to her of 31 December 2004 to mean that OPI had undertaken an audit of occasions of access to LEAP data about her between 2002 and 2004. In fact, the initial audit covered only the six months April to September 2004.

8.2 It was necessary for OVPC to arrange fresh audits of occasions of Victoria Police access to LEAP data about Jenny covering the period 2002 to 2004. (Readers may be assisted to refer to **Section 2**, where audits of LEAP access are broadly described.)

8.3 The *Information Privacy Act 2000* became enforceable from 1 September 2002. The OVPC audit could begin only from that date, no earlier. OVPC oversaw an audit of the period 1 September 2002 to 31 May 2005. Audits of access prior to 1 September 2002 are matters for Victoria Police and OPI. I have recommended that Victoria Police and/or OPI conduct an audit into the period 1 January 2002 to 31 August 2002.

8.4 Jenny was advised of these matters during the investigation. She gave consent for the access by OVPC to her data in LEAP and I communicated that consent to the Chief Commissioner. Jenny's husband, a serving member of Victoria Police, requested that no OVPC audit be conducted of access by others to data about him.

8.5 The fresh audit by OVPC needed to be conducted independently of ESD and OPI, and with particular care for the security of the audit results as they became available. The Chief Commissioner agreed to my request that the Chief Commissioner personally direct one appropriately qualified person in Victoria Police to work directly with OVPC to prepare sufficiently precise audit search strings, liaise with IBM to gather the data, and provide the data direct to OVPC, without reference to ESD or any other part of Victoria Police besides the Chief Commissioner. The audit data was received by OVPC in stages. OVPC conducted its analysis with the initial assistance of the Chief Commissioner's nominee and then with independent technical advice.

8.6 This process produced the initial results that access had been made to data about Jenny on 11 occasions between 1 September 2002 and 31 May 2005. None of those occasions were of access by the policewoman who had made the access to LEAP data about Jenny in the past (the subject of Jenny's First Complaint to ESD, **Section 3**). None of the occasions of access were by the policewoman's husband, who is also a member of Victoria Police. Two occasions of access appeared to have happened through the chance operation of the LEAP software, which brought up Jenny's name in response to unrelated queries by one Victoria Police member and one data entry operator. One occasion of access was the expected access by the ESD staff member who had liaised with OPI over Jenny's 2004 complaint to OPI (Third Complaint, **Section 5**). Eight occasions of access required further investigation.

8.7 These initial OVPC findings, together with the original electronic copies of the audit data used by OVPC, were provided by OVPC direct to the Chief Commissioner with a recommendation that the occasions of access be further investigated by Victoria Police and/or OPI. The initial findings were also provided to the Director, Police Integrity, with the same recommendation.

8.8 Any disciplinary or other action in relation to individual Victoria Police personnel that may be appropriate following the further investigations is a matter for the Chief Commissioner, with OPI oversight, under relevant law.

8.9 I have recommended that, given the history of this case, the results of any further investigations and any action taken be communicated to the Privacy Commissioner.

8.10 I emphasise that the investigations into the occasions of access detected by the OVPC audit are not yet complete and adverse conclusions ought not be prematurely drawn. Readers should bear in mind that LEAP is intended to be accessed by police for proper policing purposes (**Section 2**). Occasions of access detected in the OVPC audit may well have been for proper policing purposes. From the initial audit data, it is not possible to state the reasons for the occasions of access that were detected. Without further investigation, it is also not possible to know whether the personnel who checked data about Jenny were known to her or to other participants in the circumstances giving rise to Jenny's concerns.

8.11 The fresh audit by OVPC had a by-product. It revealed certain flaws in the processes for auditing LEAP use. It would be counter-productive to detail the flaws in a public report. They have been brought to the attention of the Chief Commissioner and OPI. Since the efficiency of LEAP audits is a factor in effective deterrence of misuse of LEAP, such flaws require analysis and repair. They will receive further attention in the separate OVPC investigation into the disclosure electronically of a large amount of LEAP audit data by Victoria Police, via IBM, to employees of Department of Justice (Corrections Victoria).

9 Decision not to recommend notification

9.1 Issue summarised

9.1.1 Information Privacy Principle 4 (Data Security) states –

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

9.1.2 This investigation has found that OPI's data security was inadequate at the time of the loss of its file about Jenny's case.

9.1.3 A Compliance Notice under Part 6 of the *Information Privacy Act* has been served on the Director, Police Integrity and OPI to ensure that certain improvements to OPI's facilities and procedures are made and maintained (**Appendix 1**).

9.1.4 Together, these recommendations address the aspect of this investigation aimed at avoiding recurrences of lapses in data security in relation to LEAP, and ensuring that if lapses do occur they are detected swiftly.

9.1.5 It remains to deal with the question of whether OPI ought to contact the identifiable persons whose sensitive personal information was contained in the LEAP audit material in OPI's file of Jenny's case. Should OPI inform those persons that their data was lost and then returned, and give them an opportunity to make their own complaint against OPI to the Privacy Commissioner under Part 5 of the *Information Privacy Act*?

9.1.6 I have considered this issue in light of applicable law, principle and the facts. I have decided not to recommend that the identifiable persons be notified. I have concluded that notification is not reasonably likely to alleviate more harm than it would cause. What follows is an explanation of my reasons.

9.2 Numbers potentially affected

9.2.1 For the purposes of this explanation, assume Jenny's surname is Z and her husband's surname is V. It may also be useful to read this explanation in conjunction with the section of the Report that describes LEAP and LEAP auditing (**Section 2**).

9.2.2 About 490 names appear in the paper printouts of LEAP audit data contained in OPI's file of Jenny's case. Most names are repeats of Z and V, with variations in the spellings. This is chiefly because of the way the search of the archived LEAP data was originally conducted. The search for references to Jenny and her husband brought up the names of many people who share those or similar names. Other names came up too, for instance as a suspect or victim or witness in descriptions entered into LEAP by police who attended incidents in which a person named Z or V was involved.

9.2.3 Most names appear in isolation from other identifying information, so a reader would not be able to determine whom the data relates to among the many Victorians whose surname is Z or V. Accordingly, the issue of privacy breach does not arise in the majority of cases.

9.2.4 But the issue of privacy breach does arise for some, and it has to be squarely faced.

9.2.5 Addresses appear with 143 names. Date-of-birth data appears with 169 names. Phone numbers appear with 16 names. Allowing for poor data quality, it remains the fact that the identities of at least some of these people could reasonably be ascertained from the information in the OPI file.[1] Identification becomes more likely for the names that appear with any two or with all three of the additional items - that is, with address and/or date of birth and/or phone number.

9.2.6 It is in relation to a proportion of these people that the issue of notifying them that their privacy may have been breached arises for decision in this matter.

9.2.7 The relevant proportion is the 90 persons whose names appear with address and/or date-of-birth and/or phone number *and* with at least one item of sensitive personal information. That is, they are reasonably identifiable and in connection with a piece of sensitive data that relates to them.

9.2.8 Personal information has been categorised as being 'sensitive' in the current context where it is non-public and disclosure may do harm.[2] Categories of sensitive information include: convictions; charges; inclusion in lists of associates of a wrongdoer; victim status; positive status as having been fingerprinted or DNA profiled or linked to violence or drug use; and a provider of information to police about the wrongdoing of another.

9.2.9 As outlined in **Section 2**, the amounts and types of sensitive personal information recorded about the **90** persons varies. For some, it is their own criminal record data. For those who are in LEAP because they have been victims of crime, the data may include some details of what happened to them. Others may be recorded as being associated with a person of interest to police. The amount of information is not extensive, but in some cases its nature, combined with its very brevity, may be more likely to lead to adverse inferences. This makes the data more sensitive than it might otherwise be if it appeared with more context, detail and explanation.

9.3 Notification of privacy breach – the basic principles

9.3.1 The presumption is that privacy breaches ought to be notified to those whom they potentially affect.

9.3.2 The starting point is the objects section of the *Information Privacy Act*, in which Parliament made it clear that the collection and handling of personal information is to be responsible and transparent.[3] Part of being open about the handling of people's personal information is to tell them when something goes wrong and to explain to them what has been done to try to avoid or remedy any actual or potential harm.[4] Where there is a reasonably foreseeable risk of harm, notification gives people an opportunity to take steps themselves to avoid or mitigate harm.[5]

9.3.3 In exceptional circumstances, notification may be neither necessary nor desirable.

9.3.4 In deciding whether the circumstances of any case are exceptional such as to make notification neither necessary nor desirable, the following factors should be considered in context by an appropriately senior decision maker in possession of the relevant facts -

1 The potential for reasonably foreseeable harm to result from the breach for the persons whose information is involved (referred to as the 'data subjects') or others affected, having regard to:

- the nature of the information, in particular its sensitivity;
- the amount of information;
- the extent of the unauthorised access, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, especially in mass media or online;
- any relationship between the recipient/s and the data subjects;
- the degree to which the data subjects may already be aware of the breach of their information privacy and be able themselves to minimise harm;
- the steps taken by the organisation to contain the breach and minimise harm.

2 The potential for notification itself to cause reasonably foreseeable harm to the data subjects (or any other person), excluding potential harm to those responsible for breach (such as damage to reputation, or exposure to disciplinary action or claims for redress, or bad publicity).

3 Whether, considering 1 and 2, notification is reasonably likely to alleviate more harm than it would cause.

9.3.5 This three-step process has some safeguards built in.

9.3.6 The decision maker has to have the relevant facts, so wilful blindness or failure to investigate in good faith will invalidate the result.

9.3.7 Attention to context is required. Information, including its sensitivity, changes according to its context. For example, a name is an apparently simple piece of information, but consider how different a name seems when it is found in the context of a phone book, an honours list, or a register of sex offenders. The first context is neutral, the next positive, the third decidedly negative for the person whose name it is. When considering whether to notify breaches, the decision maker must pay attention to the precise context of the information, and of the occurrence, discovery and response to the breach.

9.3.8 The test of 'reasonably foreseeable harm' forces the decision maker to look beyond the immediate result of the breach, but does not require that any possibility, however remote or improbable, be given weight.

9.3.9 The second factor – consideration of the harms that notification itself may cause – requires a focus on harms *to the data subject* (or others, such as his or her family members). Without this directed focus the decision maker may wrongly place weight on the readily foreseeable harms to the persons/organisation responsible for the breach.

9.3.10 A further safeguard is to require that the decision maker give a public explanation. This guards against self-serving reasoning and ensures that decisions will be exposed to scrutiny. In matters such as whether to notify in a particular case of privacy breach, reasonable people can disagree. But someone has to decide. A decision that is explained in the open, is subject to media and parliamentary analysis, and is exposed to public opinion will be more likely to earn legitimacy.

9.4 Applying the principles to this case

9.4.1 As Privacy Commissioner, I am required by the *Information Privacy Act* to exercise my functions with reference to the objects (section 5) of the Act, which include transparency.

9.4.2 I am acutely aware that a decision not to recommend that the 90 identifiable persons be notified must be carefully explained by anyone, but especially by a Privacy Commissioner.

9.4.3 The circumstances of this case are exceptional, such that it is neither necessary nor desirable to notify. Having investigated, reviewed the relevant LEAP audit data and considered the context both of the information and the breach, I have decided that –

- the potential for reasonably foreseeable harm to arise from the breach for any of the 90 relevant data subjects is slight;
- the potential for harm to result from notification is significant for a substantial proportion of the data subjects; and
- notification is not reasonably likely to alleviate more harm than it would cause.

9.4.4 The basis for these conclusions follows, by reference to the principles set out above.

9.4.5 The information is sensitive in each of the 90 cases, but its sensitivity varies greatly. The information about some identifiable people relates to interactions with police in a context that would probably be regarded by most people as discreditable. Information about others among the 90 relates to their experience as victims, and although not discreditable it would probably be regarded as sensitive partly because, if disclosed, it would reveal a fact about the individual that he or she may have chosen not to share with others, including with those close to the individual. The individual may have his or her own reasons for this choice, for instance, perhaps as part of recovery and 'putting the incident behind them', as the saying goes. Consideration of the nature of the information indicates that the types of potential harm that would be reasonably foreseeable vary and depend on the information coming to the knowledge of persons who know the individual to whom it relates.

9.4.6 The LEAP audit data in the OPI file contains only a small amount of information for most of the 90. Often it is no more than their name and identifying information in the context of, say, a list of associates of a person in whom police have had an interest, or a list of persons with the same name as a person being looked up in LEAP on a given occasion. The information about each of the 90 is sprinkled randomly among 517 pages of A4 sized print-outs of screen data. None of the 90 persons is indexed, highlighted or otherwise presented in a way that calls attention to that particular person. The small proportion of the 90 identifiable persons who appear with the largest amounts of sensitive data relating to them are persons who share the same surname with Jenny or her husband and have a considerable history of interactions with police. The audit search string brought up their data 'unintentionally' because of the similarity of surnames and so their data appears randomly sprinkled throughout, rather than in one concentrated clump of data.

9.4.7 The extent of the unauthorised disclosure was limited. The evidence of those who had custody of the file before its return to OPI was that the people who had access to the LEAP audit data after the OPI file came into Jenny's possession and before it was returned were –

Jenny

Jenny's husband

A policeman friend of the couple

Kim Wells MP, Shadow Minister for Police and Emergency Services

Two of Mr Wells' staff

ABC TV journalist, Josephine Cafagna and Age newspaper journalist, Paul Austin.

9.4.8 During the course of the investigation I sought and received from the relevant persons assurances that during the time of their access to the OPI file they had not copied the LEAP audit data contained in it.

9.4.9 Jenny, her husband and their friend stated that they read the LEAP audit data searching for references to Jenny, her husband and police relevant to Jenny's concerns. They were not looking for data about persons unconnected to their concerns. The journalists stated that they had not read all the LEAP audit data in detail, being interested in the material relating to OPI and to Jenny's concerns.

9.4.10 The OPI file containing the LEAP audit data has been in the custody of OPI and OVPC since Mr Wells returned it to OPI on 5 August 2005. Data extracted from the LEAP archive for any audit continues to exist in the LEAP archive. It can be retrieved at any time through the use of the same search strings as were used in the original audit. It is good practice to limit the proliferation of sensitive personal data in digital or paper form. Accordingly, I have recommended to the Director, Police Integrity, that the search strings used for the original Jenny complaint audit be retained on the OPI file of Jenny's case, and that the paper copy of the audit data itself be destroyed. I have made the same recommendation to Victoria Police in relation to the two paper copies of the audit data that were created for the records of ESD and the Ombudsman Liaison Office attached to the office of the Deputy Commissioner (**Section** 5).

9.4.11 It is not likely that the eight persons who had access to the OPI file read all of the LEAP audit data in the detail necessary to have retained knowledge of the sensitive personal information about the 90 identifiable persons. On the basis of the assurances given and steps taken and recommended since the return of the OPI file, I conclude that the extent of the disclosure was limited and the risk of further unauthorised access, use or disclosure is small.

9.4.12 I am not aware of any relationship between any of the eight recipients and any of the 90 identifiable persons. That is, the eight are strangers to the 90. This is relevant because the potential harm of a privacy breach can be greater when an unauthorised recipient of sensitive data about another person knows that person. Harm may be greatest when the relationship is close.[6] Generally speaking, in privacy cases distance breeds indifference. The people who are most likely to change their attitudes, rethink their relationship or adjust behaviour towards a person whose privacy has been breached are those who know the victim of the privacy breach. The person whose privacy was breached may be adversely affected, not least because those close learn, not only the information itself, but also that the data subject has kept that information from them notwithstanding the closeness of the relationship. Doubts arise. Trust ebbs. 'What else haven't they told me?' a person thinks. This potential harm to relationships can be serious and needs to be considered in privacy cases. It is subtle and demands careful attention case by case. It has not been a relevant factor in relation to the 90 persons affected by the current decision not to recommend notification of breach. The fact that it has not been relevant in this case contributes to the conclusion that the potential for reasonably foreseeable harm from the breach to any of the 90 is slight.

9.4.13 In the circumstances of this case, none of the 90 is aware of the breach. This is because, notwithstanding the publicity and parliamentary debate about the matter, the names of Jenny and her husband have been kept secure so far. One of the consequences of the names not being public is that the identities of all persons in the LEAP audit data remain protected from public exposure and their privacy is preserved from breach beyond the eight recipients described above. It follows that the potential for reasonably foreseeable harm to any of the 90 is slight.

9.4.14 So far, the discussion has dealt with harms that might be done to the 90 by other persons reacting in certain ways to receiving knowledge of the sensitive personal information about the data subjects. Another important aspect of the potential harm done by privacy breach must also be considered. That is the internal suffering of the victim of the privacy breach caused just by knowing that his or her privacy has been breached.

9.4.15 If your privacy is breached you may feel indignant, humiliated or embarrassed. You may suffer anguish in anticipation of future harms flowing from the disclosure. You may be self-reproachful in the sense that you may wish you had told those close to you the information yourself, in your own way, rather than have them find out through the breach and wonder why you hadn't told them yourself. For present purposes, I will refer to this harm as the internal suffering caused by a privacy breach.

9.4.16 Privacy is intensely subjective. Different people have different levels of sensitivity to privacy breaches affecting them. But one objective factor for every person is that the victim of the privacy breach can only suffer the feelings described in the preceding paragraph if he or she becomes aware of the breach.[7] None of the 90 is aware that their data is among the LEAP audit data in the OPI file. For so long as the real names of Jenny and her husband remain secure, the 90 have no knowledge of a breach affecting them and so no cause to suffer the kind of harm just described.

9.4.17 This unusual situation of a high-profile breach relating to 90 persons who remain unaware that it relates to them is the main element of what makes the circumstances of this case exceptional.

9.4.18 I turn now to consider any harms that notification itself may cause.

9.4.19 If OPI attempts to notify the 90, two kinds of harm are reasonably foreseeable. First, fresh breaches may be caused by failed (even though well-intentioned) attempts to notify. Problems in notifying are foreseeable in this case because of: the large number; the repetition of names; spelling variations of two names; other aspects of the names that it would not be appropriate to detail in this Report; the uneven quality of LEAP data; the probability that some address and phone data will be out of date; the risk of misdirected mail; and the risk of correctly addressed mail being opened by persons who are in close relationships with the addressee but who may be unaware of the sensitive personal information until OPI's notification arrives.

9.4.20 Assume, for the sake of following my reasoning, that these problems could all be overcome and that every one of the 90 could be accurately traced and securely notified by OPI of the breach in order to see if they wished to make a complaint under the *Information Privacy Act*. A second type of harm is foreseeable and needs to be considered.

9.4.20 The act of notification will make the person aware for the first time that sensitive data relating to them was in OPI's file of Jenny's case. This case is high-profile because of the involvement of OPI and the ongoing problems of securing LEAP data. Significant public interests are involved and political debate has been vigorous. However, as has now been explained, the privacy breach has been limited. For the most part, the complainant, the journalists and the politicians have pursued their interests without worsening the breach. The extent of the disclosure of the LEAP audit data in the OPI file has been confined to eight people, not all of whom, if any, read it all. The original data is again secure. Copies are not likely to proliferate. To the degree that any of the 90, merely by becoming aware of the breach, undergoes the internal suffering described above, notification itself will have caused that harm.

9.4.21 This harm may be thought to be insignificant for some, such as those whose sensitive information is not regarded by them, subjectively, to be very private and their details appeared simply because they shared the same name as Jenny or her husband, rather than because they were the subject of specific investigation. But the suffering may not be insignificant for others, in particular those who appear in the audit data as victims of sexual crime, or as having been suspected or charged with an offence even though the offence did not proceed to a guilty verdict or even to a court hearing. These people, and their family members, can be expected to suffer, albeit to varying subjective degrees, once they know. If they are not notified, that harm will not be caused.

9.4.22 I have considered the option of recommending that only some of the 90 be notified. Apart from the practical difficulty of formulating workable criteria for deciding who among the 90 ought to be notified, and apart from the fact that the same problems of locating and securely informing the chosen ones would apply, the chief reason for rejecting this option is its unfairness. The result would be that some persons would be given the opportunity to make an enforceable privacy complaint and some would not. All of the 90 ought to be notified or none.

9.4.23 I have concluded, for the reasons stated, that notification is not reasonably likely to alleviate more harm than it would cause.

---

[1] 'Personal information' is defined in section 3 of the *Information Privacy Act 2000* (Vic) and the term was considered by VCAT in *WL v LaTrobe University* (General) [2005] VCAT 2592 (8 December 2005), a decision summarised in Privacy Aware vol 4 no 4 (Summer 2005-06) p 2.

[2] The categorisation adopted in the current context is consistent with types of information defined as 'sensitive personal information' in Schedule 1 *Information Privacy Act 2000* (Vic).

[3] Section 5.

[4] The issue of notification has received significant attention in privacy and data protection regulation, particularly in recent years in the wake of serious breaches of data security, most prominently in the US, by corporations that collect, use and often share consumers' personal data. Although the commercial context is different from disclosures of police database information, the attention given to the issue by various regulators is instructive. See, for instance, US Federal Trade Commission, Statement to the US Senate Committee on Commerce, Science and Transportation hearings on Data Breaches and Identity Theft, 16 June 2005 http://www.ftc.gov/05/2005/06/050616databreaches.pdf, at pp 10-12, for a discussion of notification principles; US Federal Reserve, Division of Banking Supervision and Regulation, Supervisory Letter SR 05-23, 1 December 2005, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, http://www.federalreserve.gov/boarddocs/srletters/2005/sr0523.htm; California Department of Consumer Affairs, Office of Privacy Protection, *Recommended Practices on Notification of Security Breach Involving Personal Information*, 10 October 2003, in particular Part III, http://www.privacy.ca.gov/recommendations/secbreach.pdf; Information and Privacy Commissioner, Ontario, Canada, *Identity Theft Revisited: Security is not Enough*, September 2005, in particular pp 17-22 on considering the interests of the individuals affected, http://www.ipc.on.ca/userfiles/page-attachments/idtheft.revisit.pdf

[5] For example, to inform a bank of a risk of identity fraud, or to cancel a credit card.

[6] Leaving to one side the special category of celebrities, which is not relevant here.

[7] This basic ingredient that the victim be aware of the breach in order to suffer humiliation, loss of dignity or injury to feelings can be seen in many privacy cases in jurisdictions with statutes older than Victoria's *Information Privacy Act 2000*. See, for example, the cases arising from the New Zealand *Privacy Act 1993* section 66 (1) (b) and the associated commentary in NZ *Privacy Law and Practice*, Volume 1 (Butterworths) paras 1066.4 to 1066.6. Note, however, that other types of harm may be suffered even if the victim is unaware of the breach, for instance discrimination against the victim of the breach by persons who learn a sensitive private fact, such as the victim's sexual orientation or criminal or medical record, without the victim being aware.

10 Conclusions and Recommendations

10.1 Data security

10.1.1 At the time of the loss of the file about Jenny's case, the data security of the then still newly born OPI was inadequate. Contributing factors were –

- Idiosyncratic, non-standard file formats inherited from the Police Ombudsman system that OPI was in the process of superseding.
- No location tracking of paper files on the files themselves.
- An electronic case management system that was not adequate in making associations, re-opening files, managing access and security permissions, ensuring appropriate links between electronic and paper files, and being audited.
- Individuals' distrust or intolerance of systems leading to 'work-arounds' that would get the immediate job done but leave an inadequate record.
- Use of informal or inconsistent means of receiving and dispatching correspondence and other work-related information.
- Lack of written procedures and structured training based on those procedures.
- In the absence of standard written procedures, lack of sufficiently precise written or verbal instructions given on a case-by-case basis by the staff with the specific case knowledge to the staff with general roles that were essential to the secure handling of personal information.
- Poor audit trails for key processes (exacerbated by the length of the period prior to the return of the file to OPI).

10.1.2 I invited OPI to respond to the reports of the independent experts on which the above conclusions were based. The Director, Police Integrity responded in January 2006 as follows.

- Secure OPI mail and records management facilities, with full-time mail staff dedicated to OPI, had been established from 14 June 2005. Records management staff, dedicated to OPI, report to the Manager Complaints through a Records Manager Team Leader.
- An interim OPI records management policy and mail dispatch procedure had been in place since August 2005, and OPI staff had been trained in both that month. Staff training was ongoing. The policies and procedures would be finalised in light of the OVPC Report and the report of OPI's own review of its information management system.
- Security-related requirements would be examined in the process of the OPI review. In advance of this, steps had been taken to further integrate the OPI Information Security Policy and its records management policy and procedures.
- Issues regarding migration of data, integration of systems, disposal schedules, information security and general management of electronic data were in the process of being addressed in the development, training and implementation of a new electronic case management system for OPI.
- The resources and placement of the records management unit within OPI would be addressed in the light of the government's response to OPI's review.
- Pending finalisation of the structure and resources for OPI records management a full-time OPI records manager had been appointed on 12 December 2005 until 30 June 2006, when the position would be reviewed.
- Systems were now in place requiring all file movements between Victoria Police and OPI to be by safe hand delivery.
- OPI mail had been separately processed since 18 July 2005.
- Mail for franking and general dispatch was now removed from the relevant OPI file before it enters the mailroom.

10.2 Complaints handling by OPI

10.2.1 OPI did not handle Jenny's complaints adequately. At the time of the handling of Jenny's Third Complaint and Fourth Complaint, OPI's complaints handling was adversely affected by two concurrent factors that had relevant impact on the facilities, processes and personnel involved.

10.2.2 One factor was the transition from facilities, processes and personnel that had been used by the Office of the Ombudsman during its longstanding police complaints oversight role, to the facilities, processes and personnel for the statutory functions of OPI.

10.2.3 The second factor was the significant internal changes being made during the same period to the Office of the Ombudsman itself.

10.3 Liaison between OPI and Victoria Police

10.3.1 At the time, liaison between OPI and Victoria Police did not work effectively in relation to Jenny's case and to the LEAP audit associated with OPI's handling of her complaints. In my view, steps that should improve liaison and oversight in relation to the security of personal information in LEAP have been taken by OPI and by Victoria Police.

10.3.2 Jenny's case, insofar as it relates to LEAP data security and LEAP audits, is simply an example of issues that long pre-date Jenny's case. Those issues require systematic attention by Victoria Police, OPI, OVPC to a limited extent, and others in Government.

10.4 Recommendations

10.4.1 Recommendations made throughout this Report are for the consideration of OPI, Victoria Police, or both. They are summarised below.

1. Destruction by OPI of paper copies of LEAP data when they are no longer needed, retaining only the search strings so that the data can be retrieved from the main LEAP archive if required again.
2. Responses to complainants be reviewed by at least one other OPI staff member besides the person who investigates the complaint and writes the response.
3. Investigation by Victoria Police/OPI of results of the fresh audit conducted during the OVPC investigation of access to LEAP data about Jenny in the period 1 September 2002 to 31 May 2005.
4. Conduct of an audit by Victoria Police/OPI of access to LEAP data about Jenny in the period 1 January 2002 to 31 August 2002.
5. Regular review of the effectiveness of liaison between ESD and OPI where their effective liaison is necessary - and appropriate, in light of OPI's independent oversight role - to the proper and fair handling of complaints from the public about the collection and handling of personal information.
6. Destruction by Victoria Police of paper copies of LEAP audit data when it is no longer needed - specifically in this case the copy in the files of the Victoria Police Ombudsman Liaison Office (Office of the Deputy Commissioner) and the copy in the Victoria Police Ethical Standards Department file - retaining only the search strings to allow retrieval from the main archive if required again.
7. Attach an appropriate flag to the data in LEAP about Jenny to ensure that future occasions of access to that data are swiftly brought to the attention of ESD and OPI for relevant scrutiny.
8. Encrypt all LEAP data flowing electronically across open systems between Victoria Police and OPI or Victoria Police and any other entity authorised to receive it for proper purposes.

10.5 Compliance Notice

10.5.1 Understanding the factors operating in the early period of OPI's existence and development out of the Office of the Ombudsman is not the same as excusing what happened in Jenny's case. But it is important in considering what ought to be done about it.

10.5.2 The focus of the OVPC investigation is to ensure consistent compliance in future by OPI with Information Privacy Principle 4 (Data Security).[1]

10.5.3 I have concluded that the period November 2004 to June 2005 was a period of rapid and tumultuous change in Ombudsman/OPI. In relevant ways it was unique in the lives of both organisations. It was a prelude to structural and operational separation of OPI from Office of the Ombudsman, a process that had begun and continues still.

10.5.4 I am satisfied that the weaknesses identified in the OVPC investigation as having resulted in a serious contravention of IPP4 by OPI have been recognised and that the weaknesses have been or are being strengthened by OPI with reasonable steps.

10.5.5 The proper focus for ensuring continuing compliance with IPP4 by OPI is to test that strengthening in future in a way that is proportionate, likely to be effective and has integrity.

10.5.6 Accordingly, I have served on the Director, Police Integrity and OPI a Compliance Notice under Part 6 of the *Information Privacy Act*. The text of the Compliance Notice is in the Appendix to this Report.

10.5.7 The Compliance Notice requires that OPI facilitate an independent expert audit, under the control of the Privacy Commissioner, of facilities and processes that were not adequate at the time of Jenny's case but which OPI has since strengthened or is in the process of strengthening.

10.5.8 The audit is timed to occur two years into the life of OPI, when its own systems ought to be fully installed and functioning. Any weaknesses OPI may have initially shared with the Office of the Ombudsman should by that time no longer apply. A report of the independent compliance audit is to be made public.

Paul Chadwick
Privacy Commissioner
February 2006

[1] See Section 1 'The Limits of Jenny's Case'.

Appendix 1
Compliance Notice

Section 44 *Information Privacy Act 2000 (Vic)*

to Director, Police Integrity, (Director) Office of Police Integrity (OPI)

for the purpose of ensuring compliance with
Information Privacy Principle 4 (IPP4, Data Security)
Schedule 1, *Information Privacy Act*

1 Matter described

1.1 IPP4 requires organisations covered by section 9 of the *Information Privacy Act 2000* to take reasonable steps to protect the personal information they hold from loss, unauthorised access and unauthorised disclosure. OPI's facilities and procedures for the security of complaints files were inadequate at the time in 2005 when OPI temporarily lost its original file of a complaint by a woman known as 'Jenny'.[1] Unauthorised disclosure and access to personal information resulted. A serious contravention of IPP4 occurred. I am satisfied that the Director has taken reasonable steps to strengthen OPI's relevant facilities and procedures. To ensure continuing compliance with IPP4, it is necessary that the adequacy of those facilities and procedures be independently audited. The outcome of the audit will inform any decisions by the Director and/or the Privacy Commissioner about whether there is a need for further steps.

2 Action specified

2.1 OPI and the Director are to facilitate an independently designed and conducted data security audit of OPI's –

1. computerised case management system of files of complaints by the public against police;
2. system for tracking movements of paper files among OPI staff;
3. separation of correspondence from paper files;
4. methods for dispatch of mail to complainants and materials to Victoria Police;
5. archiving of closed files;
6. management of flows between OPI and Victoria Police of electronic data and paper files containing personal information, in particular LEAP data; and
7. logs and audit trails (paper and electronic) relevant to 1-6 above.

2.2 The audit is to be designed and conducted by independent experts chosen by the Privacy Commissioner, who must ensure that the relevant personnel are accountable under appropriate, enforceable confidentiality provisions (the Independent Experts).

2.3 The audit is to include the tracking by the Independent Experts through the relevant OPI systems of at least one test sample complaint file chosen at random by the Privacy Commissioner from among OPI complaints files (the Sample File).

2.4 The Director may advise the Privacy Commissioner in writing that the Sample File randomly chosen relates to matters or persons of such a sensitive nature that it ought not be used as the Sample File, or that it ought be used only with appropriate arrangements to preserve its security. (For example, by the removal or masking of its sensitive contents, the contents being secondary to the purpose of the audit, which is to check OPI's files management, not to audit the contents of any given file.) Any such arrangements, which are to be agreed by the Privacy Commissioner and the Director, must be such as to preserve the integrity of the audit. Where such arrangements are not possible in the circumstances, alternative Sample Files are to be chosen, also randomly, by the Privacy Commissioner.

2.5 The Independent Experts will be under the direction of the Privacy Commissioner.

2.6 The costs of the audit are to be met by OPI.

2.7 The Privacy Commissioner is to seek the Director's comments on the audit findings prior to finalising the report. The final report is to be in a form that can be made public to provide appropriate transparency without undermining the security of OPI's data, systems or facilities.

2.8 The Director is to arrange for the prompt presentation to Parliament of the Privacy Commissioner's final report, unamended but with any accompanying statement the Director sees fit to make.

3 Period specified

3.1 The audit is to commence on a date between 1 November 2006 and 31 May 2007 chosen by the Privacy Commissioner.

3.2 The date is to be notified in writing, together with a draft timeline for the complete audit process, by the Privacy Commissioner to the Director at least two weeks in advance of the commencement date.

3.3 The Director may, within two weeks of receiving notification, suggest to the Privacy Commissioner a change of the commencement date where, in the Director's opinion, it would not be reasonably possible for OPI to facilitate the audit within the timeline from the date notified.

3.4 The Privacy Commissioner may accept the suggested alternative commencement date or, after consultation with the Director, fix another commencement date and if necessary adjust the timeline for the complete audit process. The audit must commence prior to 1 June 2007.

3.5 The Privacy Commissioner is to manage the audit as efficiently as circumstances permit, and with the least disruption to OPI's statutory functions as is consistent with the audit being thorough, fair and of integrity.

[Signed and served by the Privacy Commissioner]

[1] The file contained sensitive personal information related to a significant number of persons besides Jenny. The file was returned to OPI. For details see Office of the Victorian Privacy Commissioner, *Jenny's Case – Report of an investigation into the Office of Police Integrity under Part 6 of the Information Privacy Act 2000* (February 2006).

Victoria's Information Privacy Principles (IPPs)

Summary

1. Collection

Collect only personal information that is necessary for performance of functions. Advise individuals that they can gain access to their personal information.

2. Use and Disclosure

Use and disclose personal information only for the primary purpose for which it was collected or a secondary purpose the person would reasonably expect. Uses for secondary purposes should have the consent of the person.

3. Data Quality

Make sure personal information is accurate, complete and up to date.

4. Data Security

Take reasonable steps to protect personal information from misuse, unauthorised access, modification or disclosure.

5. Openness

Document clearly expressed policies on management of personal information and provide the policies to anyone who asks.

6. Access and Correction

Individuals have a right to seek access to their personal information and seek corrections. Access and correction will be handled mostly under the Victorian Freedom of Information Act.

7. Unique Identifiers

A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of an organisations operations. Tax File Numbers and Driver's Licence Numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. IPP 7 limits the adoption and sharing of unique identifiers.

8. Anonymity

Give individuals the option of not identifying themselves when entering transactions with organisations, if this would be lawful and feasible.

9. Transborder Data Flows

Basically, if your personal information travels, privacy protection should travel with it. Transfer of personal information outside Victoria is restricted. Personal information may be transferred only if the recipient protects privacy under standards similar to Victoria's IPPs.

10. Sensitive Information

The law restricts collection of sensitive information like an individuals racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.

The full text of the Information Privacy Principles forms schedule 1 of the *Information Privacy Act 2000* (Vic). To determine legal rights and responsibilities, use the full version, not this summary.

report 01.06

Office of the
Victorian Privacy
Commissioner

GPO Box 5057
Melbourne Victoria 3001
Australia
DX 210643 Melbourne

Level 11
10-16 Queen Street
Melbourne Victoria 3000
Australia

Local Call 1300 666 444
Local Fax 1300 666 445

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

An independent statutory office established by the Victorian Parliament under the Information Privacy Act 2000.