IN THE MATTER OF THE ROYAL COMMISSION INTO FAMILY VIOLENCE

ATTACHMENT DW-8 TO STATEMENT OF DAVID WATTS

Date of document: 31 July 2015
Filed on behalf of: the Applicant
Prepared by:
Victorian Government Solicitor's Office
Level 33
80 Collins Street
Melbourne VIC 3000

[redacted]

This is the attachment marked '**DW-8**' produced and shown to **DAVID WATTS** at the time of signing his Statement on 31 July 2015.

Before me: ... [redacted] .....

[redacted]

An Australian legal practitioner
within the meaning of the
Legal Profession Uniform Law (Victoria)

Guidelines to the Information Privacy Principles

Edition 3 – November 2011

privacy Victoria

Office of the
Victorian Privacy
Commissioner

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

GPO Box 5057
Melbourne Victoria 3001
Australia

Telephone +61 3 8619 8719
Local Call 1300 666 444
Facsimile +61 3 8619 8700
Local Fax 1300 666 445

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

The Privacy Commissioner acknowledges the work of Felicity Wright, Manager Compliance; Jason Forte, Policy & Compliance Officer; Scott May, Policy & Compliance Officer; Cherie Ford, Policy & Compliance Officer; Anna Pollock, Policy & Compliance Officer; Dr Anthony Bendall, Deputy Privacy Commissioner and all other staff who contributed to the development of these Guidelines.

Contents

Glossary of Terms and Abbreviations

The following is a list of common terms and abbreviations that appear in these Guidelines.

Term or Abbreviation	Meaning
ASIS	Australian Secret Intelligence Service
ASIO	Australian Security Intelligence Organisation
Biometrics	The automated use of physiological or behavioural characteristics to determine or verify identity. Biometrics are unique, measurable characteristics or traits of a human being. Finger-scanning or printing is a commonly used biometric. Voice recognition, photographs, and digitised signatures are others. Retina-scan and iris-scan are eye-based biometrics.
CCTV	Closed Circuit Television. A video monitoring and security system used to provide continuous traffic monitoring by the facility operator along the length of the facility and particularly at points of entry and tolling locations.
Cookies	Blocks of data shared between a web server and a user's browser. Cookies give the server information about a user's identity (or, at least, the computer's ID, or the client's ID), even if he or she is not the person actually using the computer at the time.
Data matching, data linking, data sharing, data cleansing	Data matching involves any of the following: - comparing personal information from two or more records to determine whether personal information from different records matches to the same individual; and/or - comparing personal information about an individual obtained from two or more records to gauge the accuracy of the personal information about that individual in each of the records, and to improve the accuracy of the personal information in all of the records; and/or - connecting two or more records of personal information to aggregate personal information about an individual. Some of these activities may also be referred to, or performed for the purpose of data sharing, data linking, or data cleansing.

Term or Abbreviation	Meaning
Encryption	The process of systematically encoding data before transmission and during storage so that an unauthorised party cannot decipher it.
E-government / E-commerce	"Electronic government". E-government refers to a government's use of information technologies (such as Wide Area Networks, the Internet, and mobile computing) to exchange information and services with citizens, businesses, and other arms of government. "E-commerce" is a similar concept pertaining to the activities of government, business or industry.
EU	European Union
Extranet	A private network that uses the Internet protocols and the public telecommunication system to securely share part of an organisation's information or operations with certain categories of user. An extranet can be viewed as part of an organisation's intranet that is extended to users outside the organisation.
FOI Act	*Freedom of Information Act 1982* (Vic).
Google	A popular search engine and a tool for finding resources online.
Information Privacy Act	*Information Privacy Act 2000* (Vic).
IPP	Information Privacy Principle. There are ten IPPs contained in the schedule to the *Information Privacy Act*. The IPPs are reproduced in Appendix 1 of these Guidelines.
ICT	Information and Communications Technology.
NPP	National Privacy Principle. There are ten NPPs contained in Schedule 3 of the *Privacy Act 1988* (Cth).
OECD	Organisation for Economic Co-operation and Development
SMS	Short Message Service. A service enabling recorded messages to be electronically communicated between mobile phones.
VCAT	The Victorian Civil and Administrative Tribunal. VCAT is the tribunal with jurisdiction to determine breaches of the IPPs in the *Information Privacy Act*.

Explanatory Note to Legal Citations

Victorian case notes of privacy complaints are also available at OVPC's website, http://www.privacy.vic.gov.au. Australian and New Zealand privacy cases referred to in these Guidelines can be found at the website for the Australasian Legal Information Institute, http://www.austlii.edu.au. Other cases from a number of overseas jurisdictions can be accessed through the World Legal Information Institute's Privacy Law Library at http://www.worldlii.org/int/special/privacy.

The usual format for referring to cases is to include the parties names or case name in italics, followed by the year the decision or case note was published, and then a reference to the decision maker (such as an acronym of the relevant privacy commissioner, court or tribunal) or publication source (such as in a law report series).

Designators for case notes of Privacy and Data Protection Commissioners	
HKPrivCmr	Hong Kong Privacy Commissioner
NSWPrivCmr	New South Wales Privacy Commissioner
NZPrivCmr	New Zealand Privacy Commissioner
PrivCmrA	Federal Privacy Commissioner of Australia
PrivCmrACD	Federal Privacy Commissioner of Australia Complaint Determinations
VPrivCmr	Office of the Victorian Privacy Commissioner
Designators for case reports of Courts and Tribunals	
AAT / AATA	Administrative Appeals Tribunal
AC	Appeal Cases (United Kingdom)
ALD	Administrative Law Decisions
ALN	Administrative Law Notes (in Administrative Law Decisions)
ALR	Australian Law Reports
CLR	Commonwealth Law Reports
FCA	Federal Court of Australia
FCAFC	Federal Court of Australia - Full Court
Fed Sup	Federal Supplement (USA)
FMCA	Federal Magistrates Court of Australia
HCA	High Court of Australia
NSWADT	New South Wales Administrative Decisions Tribunal
NSWADTAP	New South Wales Administrative Decisions Tribunal Appeal Panel
NSWCA	New South Wales Court of Appeal
NZHRRT	Human Rights Review Tribunal of New Zealand
NZLR	New Zealand Law Reports
SASC	Supreme Court of South Australia
VCAT	Victorian Civil and Administrative Tribunal
VR	Victorian Reports
VSC	Supreme Court of Victoria
VSCA	Supreme Court of Victoria - Court of Appeal

Preface to 3rd Edition of Guidelines to the Information Privacy Principles

The second edition of the Guide to the Information Privacy Principles was published in September 2006, after the 5th anniversary of the *Information Privacy Act*. The second edition was an accumulation of the work of the first five years of the office under the stewardship of Paul Chadwick, the first Privacy Commissioner. The Third Edition has merely updated the Second Edition, not re-written it. For this reason I have retained in this edition the Preface written by Paul Chadwick.

Another five years has passed since the second edition was published. Technology has continued to develop at an ever-increasing pace allowing for more and more gathering, matching and disseminating of information about individuals. Black Saturday happened in Victoria on 7 February 2009, requiring extensive data sharing in order to respond effectively to that emergency. These, and other events, have all added to the experience of Privacy Victoria, and the Victorian public sector, in interpreting and applying the Information Privacy Principles. This experience has been drawn upon for this latest edition, as well as the experience of other jurisdictions where similar principles are applied.

I hope this updated version informs and helps not only the Victorian public sector but others, both nationally and internationally involved in interpreting and applying these and similar principles and contributes in a small way to some consistency of approach. However, it must be remembered that these are only guidelines. They are not legally binding.

I thank the Policy and Compliance team who researched and updated the guidelines, in particular Jason Forte who co-ordinated the project, Megan Glyde for her meticulous proofing, Julie Bransden who created the Index and all other staff who assisted in the final production. Michelle Fisher, the original principal researcher and author of the second edition must not be forgotten as it is her hard work that provided the foundation for this updated guide.

HELEN VERSEY
Privacy Commissioner

October 2011

Victoria's *Information Privacy Act* (IP Act) is five years old on 1 September 2006. Over the four years the IP Act has been enforceable, its 10 Information Privacy Principles (IPPs) have been applied in diverse settings involving widely varying types of personal information. Because of the infinite combinations of information and of the circumstances of its collection, use, disclosure, quality and security, Parliament necessarily expressed the statutory standards broadly. Only time and use in practical situations can give the IPPs their patina of interpretation, their shades of meaning. This edition of the Guidelines shows that process in action.

The sheer size of this second edition mostly reflects the experience gained through applying the IPPs to circumstances brought by organisations and individuals to the Office of the Victorian Privacy Commissioner (OVPC) as enquiries and complaints. OVPC has also kept an eye on relevant developments in similar laws in other jurisdictions, partly because Victoria's IPPs are derived from a common set of international data protection standards, and partly because consistency is a desirable objective. Technologies and data flow across borders with ease. It will help if, within Australia at least, information privacy standards are as consistent as is practicable and commensurate with a decent common denominator, not the lowest one.

Most privacy enquiries do not become formal complaints, yet the detail of an apparently simple enquiry may shed light on an aspect of the application of the IPPs in one of the myriad settings in which personal information is collected and handled by state and local government organisations or their contracted service providers. In some common settings, questions of interpretation regularly recur, and the extra detail in this edition should assist the many who work with the IPPs day to day. Many complaints can be dealt with adequately by respondents, without the need for OVPC's formal involvement. And complaints may be conciliated with OVPC's assistance, without the need for hearing and adjudication by the Victorian Civil and Administrative Tribunal of the kind that tends to produce traditional case law. Complainants at times withdraw, so that their case produces no ruling, however useful such a ruling may have been for future guidance in similar cases. But, whatever its eventual resolution, every enquiry and every complaint requires consideration of how the IPPs may apply in the specific context.

This second edition of the Guidelines is to me a kind of bookend. It comes at the end of my five-year term as the first Victorian Privacy Commissioner. At the other end of the term is the first edition, which reads now so prospective in tone in that pre-enforcement period in August 2001-August 2002. Together, the first and second editions of the Guidelines to the IPPs bracket the many other materials produced by OVPC to animate Victoria's data protection law in its earliest years. The person who had day-to-day management responsibility for OVPC's complaint handling throughout the period was Helen Versey, Deputy Commissioner (Policy and Compliance), who is to become Acting Privacy Commissioner until my successor is appointed. It is fitting that she takes over now from me on this page the task of introducing these new Guidelines in greater detail.

I thank her, the principal researcher Michelle Fisher, Manager, Policy, and all the OVPC staff who contributed both to the freshly milled Guidelines and to their grist, the enquiries and complaints that require patient and discreet handling by any statutory regulator, but especially by a privacy commissioner's office.

PAUL CHADWICK
Victorian Privacy Commissioner

July 2006

Overview

Scope

1 These Guidelines are intended for people working with the Information Privacy Principles (IPPs) in the Victorian *Information Privacy Act 2000* (*Information Privacy Act*). The IPPs are relevant for all Victorian public sector employees, including those from Victorian government departments, local councils, statutory offices, government schools, universities and TAFEs. They can also be relevant for employees of private or community sector organisations, where those organisations are carrying out functions under a state contract with a Victorian public sector organisation.[1]

2 For further information about the types of organisations that are bound by the *Information Privacy Act*, and the organisations and activities that are exempt, see the following Information Sheets published by the Office of the Victorian Privacy Commissioner (OVPC):[2]

a *Who's covered by the Information Privacy Act?,* Information Sheet No. 01.06, April 2006; and

b. *Exemptions from the Information Privacy Act,* Information Sheet No. 02.06, 12 May 2006.

Whether Guidelines are legally binding

3 Under the *Information Privacy Act*, the Privacy Commissioner has the power to issue guidelines and provide advice on the operation of the *Information Privacy Act* and the IPPs.[3] These Guidelines are not legally binding, and do not constitute legal advice about how organisations are to comply in specific circumstances. (Specific advice is needed for those circumstances.) They are intended to indicate how the Privacy Commissioner interprets and applies the IPPs. These Guidelines indicate the matters the Privacy Commissioner may consider when advising organisations during consultations, when examining acts and practices during an audit, when dealing with complaints, or when conducting an investigation into an apparent breach of the IPPs.

4 The details of compliance with the IPPs and the Act are ultimately up to each organisation. Organisations should consult their privacy officer or unit as required, and may wish to seek independent legal advice where appropriate. Officers from the OVPC are available to take enquiries and provide guidance (✆ 1300 666 444).

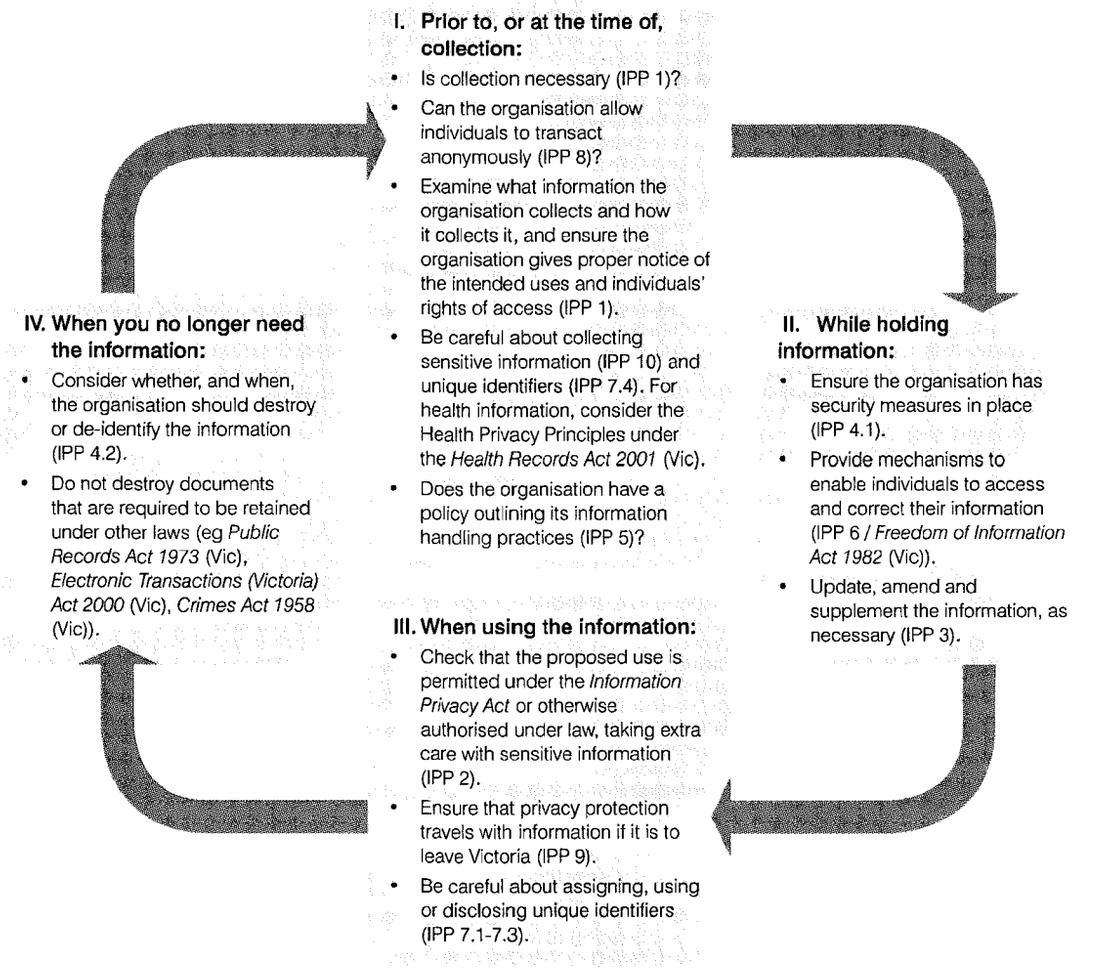
Considering the IPPs in context

5 These Guidelines should be read together with the full text of the IPPs (contained in the Appendix).

6 In practice, the IPPs often interact.[4] Information flows and impacts on privacy, as experienced day-to-day, are sprawling and untidy phenomena. In dealing with them in the context of the *Information Privacy Act*, it is better to assemble the facts of a case, identify the issues that those facts seem to raise, and then work through the IPPs to consider which apply and how.

7 Having an understanding of the particular data, laws and practices relevant to the information flows places an organisation in a better position to assess how the organisation can comply with the *Information Privacy Act*. The combinations of circumstances and the kinds of personal information arising daily throughout the Victorian public sector are vast and varied. These Guidelines cannot anticipate them all, and are an ingredient, not an all-solving formula, in decision-making under the *Information Privacy Act*.

Life cycle of IPPs



8 Getting familiar and comfortable with the IPPs will not only help an organisation understand them, but will slowly embed them as a reflex. Reflexive privacy protection offers the best kind of protection for an organisation and the privacy of the individuals involved. An organisation's privacy obligations commence before an organisation collects or obtains personal information and remain as long as it has possession or control over that personal information.

9 For instance, even before an organisation collects information, IPP 1 requires an organisation to consider whether it is necessary for its functions or activities that it collects the information at all. In the case of "sensitive information", IPP 10 obliges an organisation to look closely at issues of consent and legal authority. IPP 8 asks an organisation to consider whether it is lawful and practicable to collect the information anonymously.

10 Privacy remains relevant at every phase. The IPPs interact with each other. Examine the situation, identify the issues, and work though the IPPs to determine which apply and how, or which don't apply and why. These Guidelines detail and discuss ways that organisations can comply with the IPPs and embed privacy enhancive practices throughout their organisations.

Objects of the *Information Privacy Act*

11 The IPPs should be applied with the objects[5] of the *Information Privacy Act* in mind. They are:

a to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector;

b to promote awareness of responsible personal information handling practices in the public sector; and

c to promote the responsible and transparent handling of personal information handling in the public sector.

12 These objects and the IPPs together animate four longstanding themes in privacy and data protection law and policy:[6]

Openness and transparency
Individuals should be made aware of the information held about them and why it is held, and should be able to see it and correct it if necessary.

Proportionality
Organisations should only collect personal information as is necessary, and should minimise intrusion into privacy.

Purpose limitation
Generally, personal information should be used only for the purpose for which it was collected.

Individual participation
Individuals should have as much say as possible in what information about them is used for and who gets access to it.

13 The *Information Privacy Act* and the IPPs imply some shift in control from the collectors and users of personal information to the sources and subjects of it. It is not a total shift. As the objects say, it is a balancing of various public interests.

National consistency

14 The explanatory material accompanying the *Information Privacy Act* during its introduction into Parliament notes that the IPPs are adapted from the federal Privacy Commissioner's *National Principles for Fair Handling of Personal Information* (which were also relied upon in the drafting of the Commonwealth National Privacy Principles). The Victorian IPPs are to be interpreted, as far as possible, in a manner that is consistent with the National Privacy Principles:

> Some modifications to the National Principles have been made to reflect the responsibilities of public sector organisations to promote public interests and be accountable for the expenditure of public funds.... In adapting the National Principles under Victorian law it is intended that as much consistency as possible can be maintained with perceptions and practice already operating nationally.[7]

15 Accordingly, in applying the Victorian IPPs, organisations may wish to consider how the Commonwealth and other jurisdictions have interpreted privacy principles that were similarly based on the National Fair Handling Principles. Caution must of course be exercised where the wording and application of these principles differ, and where a contrary or inconsistent view has been expressed in Victoria – whether by the Victorian Privacy Commissioner or by a court or tribunal interpreting the Victorian law. These Guidelines include case law from other jurisdictions where relevant and analogous.

Distinguishing privacy from related concepts

Privacy and confidentiality

16 Often, individuals in the public sector are bound by duties of confidence – whether arising as a result of relationships, or imposed by statute,[8] or under a contract.

17 Confidentiality is a concept that is related to, but different from, privacy. An obligation of confidence is generally owed by the recipient of information to the provider of the information. Privacy is the right of the subject of the information, no matter who provided and who received the information. Confidentiality often deals with information other than personal information. Confidentiality is about controlling the disclosure of information, while privacy obligations go wider to encompass collection, quality and disposal.

> EXAMPLE:
>
> If Eva tells Norma in confidence that Anna has had an abortion, the relationship of confidence is between Eva and Norma, but it is Anna's privacy that is involved because it is her personal information being disclosed.

18 The *Information Privacy Act* will not override a duty of confidence, nor will IPP 2 (Use and Disclosure) provide any authority for disclosure of information that is already required to be held in confidence.[9]

Privacy and secrecy

19 Governments and corporations may have secrets, but not privacy. Privacy is a condition for individual human beings. Privacy is necessary to the preservation of dignity and autonomy. It provides for self-development and the flourishing of intimate relationships. Where privacy is respected, trust can grow. Privacy is a human right[10] and longstanding societal value.

20 Secrecy comprises techniques to prevent information coming to the knowledge of others. Secrecy may assist a person to maintain privacy and a company to maintain confidentiality. Governments may use secrecy to serve other public interests, such as: protection of national security; integrity of law enforcement investigations; and facilitation of "frank and fearless" advice, including contending and controversial options, prior to final decision. But secrecy can also be used to avoid detection of misdeeds or to avoid public accountability. In the *Freedom of Information Act 1982* (Vic) ("the FOI Act"), the Victorian Parliament has struck the balance between openness and secrecy, in the sense of the proper withholding of government information. The *Information Privacy Act* is the main legislative balance between openness and personal privacy.

21 The *Information Privacy Act* and IPPs should not be administered by the public sector in such a way as to avoid legitimate scrutiny and accountability or to impede the free flow of information in ways not required by the *Information Privacy Act* to protect the public interest in privacy.

Information privacy and FOI

22 The interaction of the *Information Privacy Act* and the FOI Act is discussed in the Privacy Commissioner's *Submission to the Victorian Ombudsman on his Review of the Freedom of Information Act 1982* (Vic), 9 August 2005:[11]

> Freedom of information and information privacy are closely related fields of administrative law. They both deal with information and how it ought to flow. Part V of Victoria's *Freedom of Information Act 1982* (FOIA) incubated one of the main data protection rights (access and correction of your own file) until in 2000 the Parliament created a full and separate data protection scheme in the *Information Privacy Act* (IPA).
>
> The IPA established the OVPC and a structure, based on international standards, for the responsible collection and handling of personal information by state and local government and their contracted service providers. The IPA cross-refers to the FOIA in several important respects (discussed later), allows exchanges between the Ombudsman and the Privacy Commissioner and both laws provide for appeals to VCAT.
>
> The FOIA is part of the mix of laws that provide Victorians with certain of the internationally recognised human rights,[12] as is the IPA, the main statutory protection in state legislation for the human right to privacy.[13] The two acts, and the rights they enshrine, are compatible, both requiring a balancing process when various public and private interests compete.

23 In Victoria, the FOI Act and the *Information Privacy Act* have a close interconnection in two ways:

a Part V of the FOI Act gives people the right to seek correction of their personal information and, to the extent that this is usually considered a privacy right, is a precursor to the *Information Privacy Act*; and

b Section 12 of the *Information Privacy Act* provides that the FOI Act is to remain the procedure for people to seek access to their personal information from those organisations that are subject to the FOI Act.[14]

24 But FOI and privacy laws differ in three important ways:–

c FOI is fundamentally about compelling disclosure. Privacy compels discretion.

d Under FOI, every person has a legally enforceable right to seek access to documents held by government, whether or not the documents relate to the requester.[15] Privacy only confers a right of access on the person who is the subject of the personal information. FOI includes mechanisms for addressing the privacy of third parties whose information is about to be disclosed to a requester.

e FOI deals mostly with access and correction. Privacy is wider and more subtle, also addressing collection, use, storage, quality, sharing and disposal of personal information.

25 The interaction of FOI and privacy, and the operation of IPP 6, is discussed further in the OVPC's Information Sheet 05.08, *Freedom of Information and the Information Privacy Act*, July 2008, and also in these Guidelines under IPP 6.

Overview Notes

[1] See *Outsourcing and Privacy: A guide to compliance under the* Information Privacy Act, OVPC, Edition 1, May 2011, available at http://www.privacy.vic.gov.au.

[2] Available at http://www.privacy.vic.gov.au.

[3] *Information Privacy Act 2000* (Vic) s 58.

[4] For instance, data flowing across borders (IPP 9) will involve some use or disclosure (IPP 2). Collection (IPPs 1 and 10) may involve consideration of whether anonymity is an option (IPP 8) or whether a unique identifier is necessary (IPP 7). Collection of identifiable data may involve undertaking to destroy or de-identify the data after a set period (IPP 4.2). Misuse or unauthorised disclosure of data will usually invoke both IPP 2 (use and disclosure) and IPP 4.1 (safeguarding the security of data against unauthorised disclosure or use). Inaccurate or misleading data will involve the data quality principle (IPP 3) and may lead to the exercise of correction rights under *Freedom of Information Act* procedures (s 12, *Information Privacy Act*).

[5] Section 5 of the *Information Privacy Act 2000* (Vic).

[6] See, for instance, the Second Reading Speech to the *Information Privacy Bill 2000* (Vic), Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000, page 1907 (John Brumby, Minister for State and Regional Development). The IPPs, like most modern data protection and information privacy standards, can be traced in part at least to the OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980). Victoria's heritage in this regard was noted in the discussion paper released early in the development of the then Data Protection Bill, when the Minister remarked that the Victorian data protection principles "reflect the ideas of the OECD guidelines". (Victoria, Department of State and Development, Multimedia Victoria, *Information Privacy in Victoria: Data Protection Bill*, Discussion Paper, page 22, July 1998, available at http://www.egov.vic.gov.au.)

[7] Note to clause 14 in the Explanatory Memorandum accompanying the *Information Privacy Bill 2000* (Vic).

[8] For example, see s 70, *Sex Offenders Registration Act 2004* (Vic); ss 106P and 141, *Fair Trading Act 1999* (Vic); s 30H, *Corrections Act 1986* (Vic). Note, sometimes such statutory restrictions are referred to in legislation as provisions relating to the "disclosure of information" – eg, s 92, *Road Safety Act 1986* (Vic); s 464ZGK, *Crimes Act 1958* (Vic); and s 127A, *Police Regulation Act 1958* (Vic) – or as "secrecy" obligations – see, eg Division 3 of Part 9, *Taxation Administration Act 1997* (Vic); s 33, *Emergency Services Telecommunications Authority Act 2004* (Vic); ss 30 and 36, *Corrections Act 1986* (Vic); s 87, *Sex Work Act 1994* (Vic); ss 155 and 243, *Accident Compensation Act 1985* (Vic), s 128, *Housing Act 1983* (Vic).

[9] Section 6 of the *Information Privacy Act 2000* (Vic) provides that the Act gives way to the extent of any inconsistency with other Victorian statutes. Note, unlike the *Information Privacy Act*, the Victorian *Health Records Act 2001* expressly preserves the confidentiality of information at the point of collection (HPP 1.7), use and disclosure for investigation of unlawful conduct or to a law enforcement agency (HPP 2.2(i) and (j)), and access (s 27 and HPP 6.1(e)).

[10] The right to privacy is recognised in s 13 of the Victorian *Charter of Human Rights and Responsibilities Act 2006*, which states: "A person has the right (a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and (b) not to have his or her reputation unlawfully attacked." The explanatory note to section 13 comments that it is modelled on the right to privacy contained in Article 17 of the *International Covenant on Civil and Political Rights*. See also the Office of the Victorian Privacy Commissioner's Information Sheet 03.08, *Privacy and the Charter of Human Rights and Responsibilities*, June 2008.

[11] Available at http://www.privacy.vic.gov.au.

[12] *International Covenant on Civil and Political Rights* (ICCPR) Article 25.

[13] ICCPR Article 17. Other laws make important contributions, among them the *Surveillance Devices Act 1999* and the *Health Records Act 2001*.

[14] This means, in practice, that IPP 6 in Victoria affects only those organisations that are not subject to the *Freedom of Information Act 1982* (Vic), such as contracted service providers to government. For further guidance, see paras 6:8-6:18. Also see the Office of the Victorian Privacy Commissioner's Information Sheet 01.10, *Accessing and Correcting Your Personal Information*, January 2010.

[15] The right of access is contained in s 13 of the *Freedom of Information Act 1982* (Vic).

Key Concepts

KC:1 The *Information Privacy Act* and the IPPs use some key words and phrases. The starting point for interpreting words and phrases is section 3 of the *Information Privacy Act*. If the word or phrase is not defined, then the next checkpoint is the dictionary to find the word's ordinary, everyday meaning. In some cases, the meaning of key terms is considered by tribunals and courts, and case law should be consulted as appropriate.

KC:2 In working out the meaning of any provision of the *Information Privacy Act* or IPPs, the interpretation that would promote the purpose or objects of the Act is to be preferred. Consideration can also be given to certain materials beyond the Act itself, such as the Explanatory Memorandum that accompanied the *Information Privacy Act* when it was considered by Parliament, and relevant Parliamentary debate.[16]

KC:3 The *Information Privacy Act*, like other privacy laws and anti-discrimination laws,[17] is generally regarded as beneficial legislation.[18] This means that the provisions of the *Information Privacy Act* should be interpreted in a manner favourable to those individuals whose privacy is to be protected. Moreover, the interpretation and application of Victorian statutes needs to accord with relevant aspects of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) which provides that:

a all statutory provisions (including those contained in the *Information Privacy Act*) must be interpreted in a way that is compatible with human rights, so far as it is possible to do so consistently with the statute's purpose;[19] and

b it will be unlawful for a Victorian public authority to act in a way that is incompatible with a human right, or to fail to give proper consideration to a relevant human right when making a decision.[20]

Personal information

KC:4 The starting point for determining whether the *Information Privacy Act* applies is to decide whether the information in question is "personal information" within the meaning of section 3 of the *Information Privacy Act*. If the information does not fall within this definition, then the *Information Privacy Act* and its IPPs do not apply.

KC:5 The definition of personal information is:

> information
>
> or an opinion
>
> (including information or an opinion forming part of a database),
>
> that is recorded in any form
>
> and whether true or not,[21]
>
> about an individual
>
> whose identity is apparent,
>
> or can reasonably be ascertained
>
> from the information or opinion
>
> but does not include information of a kind to which the *Health Records Act 2001* applies.[22]

Living natural persons

KC:6 The *Information Privacy Act* defines "individual" to mean a natural person. Corporations and other types of "legal persons" do not have privacy rights under the *Information Privacy Act*, only humans do.

KC:7 Some data protection laws make it explicitly clear that privacy protection applies only to "living persons" or "natural living persons".[23] Most laws in Australia (including the *Health Records Act 2001* (Vic)) extend privacy protection, in whole or in part, to deceased persons for periods of 5-10 years or more after death.[24] Access and correction rights under the Victorian *Freedom of Information Act 1982* also extend to information concerning deceased persons.[25]

KC:8 Although the Victorian *Information Privacy Act* does not expressly refer to "living persons", it is apparent from policy documents released during the early drafting of the legislation that the intention was for the *Information Privacy Act* to protect the privacy of living persons only:

> The law will not apply to information about legal persons (such as a company) or people who are no longer living.[26]

KC:9 It is important to bear in mind that information about a deceased person may include personal information about the living. Coronial records, for example, may include information about the deceased person's family, friends, employer and colleagues, and relevant medical and police officers involved in the coronial inquiry. The privacy of living relatives and other individuals will continue to be protected by the *Information Privacy Act*.

Recorded

KC:10 Unlike the *Health Records Act 2001* (Vic) and the *Privacy Act 1988* (Cth), the *Information Privacy Act* requires personal information to be "recorded". When the *Information Privacy Bill* was first introduced into Parliament, the definition of "personal information" was similar to that used in these other laws (ie, "whether recorded in a material form or not"). The definition was amended prior to Parliament passing the *Information Privacy Act*, with the following explanation:

> The amendments relate to the definition of personal information. They are necessary because they apply not merely to verbal and conversational exchanges of information but to personal information that is recorded in any form.
>
> The amendments are necessary to clarify that the bill will apply only to information recorded in some form, whether, for example, it is held in physical files or on electronic databases. It is not practicable or desirable for the bill to regulate conversations in which personal information is discussed. That was the unintended interpretation of the definition. In other words, if in a telephone conversation between two parties personal information had been discussed but no notes were held of that discussion, it would be inappropriate for that discussion to be subject to the Act.
>
> The advice I received was that a technical interpretation of clause 3 could have meant that telephone conversations could fall within the ambit of the Act. That is not the intention of the legislation. It is meant to relate to information that is held on physical files or electronic databases, not information that may or may not be discussed orally across a telephone line.[27]

KC:11 The Act will nevertheless apply to conversations about information that has already been recorded, as well as to conversations that are subsequently recorded (for example, as suggested above, where notes are taken).[28] The *Information Privacy Act* will not apply where the only record of the information is in someone's mind.[29]

In any form

KC:12 Personal information need not be merely words on paper. The words may be in stored messages (for example, emails, SMS and voicemail messages), captions on screens or in posters or, other signage. The personal information may not be words at all, but images (especially photos), sounds (voice on tape) or be latent in a material item but reasonably ascertainable (for example, DNA in human tissue).

Examples of personal information

KC:13 Almost any recorded information that is associated with an identifiable living natural person can be personal information. It can include correspondence, audio recordings, images, alpha-numerical identifiers, and combinations of these.

KC:14 The following information, in its context, has been regarded as "personal information" by the Victorian Civil and Administrative Tribunal (VCAT) and/or the Victorian Privacy Commissioner:

a an individual's name and address: *Duggan v Moira Shire Council*, Unreported, VCAT Reference No. G394/2004 (Senior Member Preuss, 9 February 2005); *Complainant P v Local Council* [2005] VPrivCmr 2; *Complainant D v Minister* [2003] VPrivCmr 4; *Complainant H v Local Council* [2004] VPrivCmr 2;

b publication of an individual's name on an online register as the holder of a sensitive trade activity: *Complainant E v Statutory Entity* [2003] VPrivCmr 5;

c an individual's name and unlisted telephone number: *Whitfield v Greater Bendigo City Council* [2005] VCAT 1756;

d an individual's change-of-name and new address details: *Complainant B v Statutory Entity* [2003] VPrivCmr 2;

e an individual's mobile telephone number: *Complainant K v Local Council* [2004] VPrivCmr 5;

f an individual's work telephone number: *Complainant M v Tertiary Institution* [2004] VPrivCmr 7;

g a photograph of an individual: *Smith v Victoria Police* [2005] VCAT 654;

h an individual's fingerprints: *Complainant AB v Victoria Police* [2006] VPrivCmr 3;

i a digital (CCTV) recording of events in a classroom involving a teacher and students: *Ng v Department of Education and Training* [2005] VCAT 1054;[30]

j surveillance footage of an individual and the surveillance report of that footage: *Complainant X v Contracted Service Provider to a Department* [2005] VPrivCmr 6; *Complainant AE v Contracted Service Provider to a Statutory Authority* [2006] VPrivCmr 6;

k computer copies of an individual's correspondence and academic papers: *Complainant W v Public Library* [2005] VPrivCmr 5;

l records created as a result of workplace monitoring of an individual's emails: *Complainant L v Tertiary Institution* [2004] VPrivCmr 6; *Complainant AR v the Department* [2010] VPrivCmr 3;

m an individual's bank account and leave details: *Complainant I v Department* [2004] VPrivCmr 3;

n letters to and from a named individual: *Dodd v Department of Education and Training* [2005] VCAT 2207; *Complainant AT v Local Council* [2011] VPrivCmr 2; *Complainant AQ v Contracted Service Department to the Department* [2010] VPrivCmr 2;

o a letter sent by facsimile about an individual's hearing before a professional registration board: *Towie v Victorian Government Solicitor's Office* [2005] VCAT 1810;

p correspondence containing information about an individual's concerns about an entity and information about the individual's character: *Complainant J v Statutory Entity* [2004] VPrivCmr 4;

q a publication referring to a land dispute between the local council and an individual: *Complainant Z v Local Council* [2006] VPrivCmr 1;

r an individual's prior dealings with police: *Complainant C v Department* [2003] VPrivCmr 3;

s disclosures made to a child protection officer about the custody and welfare of an individual's grandson: *Creely v Department of Human Services* [2004] VCAT 1746;

t the identity of an individual's child involved in an incident being investigated by a department: *Complainant AA v The Department* [2006] VPrivCmr 2;

u a student's candidature for a PhD: *Complainant F v Tertiary Institution* [2003] VPrivCmr 6;

v individuals' membership of an association and their attendance at meetings: *Complainants R, S, T, U and V v Local Council* [2005] VPrivCmr 4;

w the results of an individual's criminal record check: *Complainant Q v Contracted Service Provider to a Department* [2005] VPrivCmr 3;

x digital recording of a telephone call in which the individual took part and was named: *Complainant AP v Organisation B* [2010] VPrivCmr 1; and

y non-work related material transferred by an employer to a corporate computer: *Complainant AO v Organisation* [2009] VPrivCmr 4.

KC 15 For further guidance on determining when images are regarded as personal information and the kind of factors to address when taking pictures, see the OVPC's Information Sheets:

a *Images and Privacy*, Information Sheet 01.03, January 2003; and

b *Mobile Phones with Cameras*, Information Sheet 05.03, August 2003.

KC:16 Be aware that there may be other laws regulating surveillance activities, notably the *Surveillance Devices Act 1999* (Vic). Although the *Surveillance Devices Act* does not generally prohibit video surveillance in public spaces,[31] the *Information Privacy Act* may still apply to what can be done with the footage or in relation to the manner in which the footage is collected, where identified or identifiable persons are filmed.[32]

Whether identity is apparent or can be reasonably ascertained

KC:17 Whether an individual's identity is apparent or can reasonably be ascertained will depend on both the information and the circumstances in any given case.

KC:18 An individual's identity is "apparent" when one could look at the information collected and know or perceive plainly and clearly that it was information about the individual. In *WL v La Trobe University* [2005] VCAT 2592 (see Case Study KC-1), VCAT commented (at para 18) that one's identity would be apparent if the information mentioned the person's name or was a photograph of the person, and would also encompass situations where the information was of a "singular nature":

> One could also conceive of situations where information which did not include one's name or photograph would, because of the singular nature of the information, mean that it could be no one else but a particular person, and in that way reveal one's identity. In that case the identity would be capable of being clearly perceived by looking just at the information; it would be apparent, for example, if the information was about "the lady who wears a crown and rules the British Empire", one would know plainly from the information that it was a reference to Queen Elizabeth II. Her identity is apparent from the information.

KC:19 In *WL v La Trobe University*, VCAT also considered the meaning of "reasonably ascertained" (discussed in Case Study KC-1). The respondent submitted that the definition in the *Information Privacy Act* excluded information that requires cross-referencing with other known information to ascertain an individual's identity, and that the *Information Privacy Act* required identity to be ascertained *from* the information in question. The Tribunal rejected this proposed limitation, finding instead that "reasonably ascertained" must allow some use of extraneous material in order to give the phrase some meaning beyond what is captured by "apparent":

> Just what is meant by "reasonably be ascertained from the information" is not so clear. Does it mean ascertained solely from the information without reference to anything else? One would think it might not because, as I said earlier, there will be cases where there is a string of information which must inevitably lead to the identity of a particular person, depending on the context, without the information revealing a person's name or photograph.
>
> If such information can all be put together from what is actually contained in the information and from no other source and identifies the person, it would seem that the identity of the person would be "apparent" from the document. The use of the word "ascertained" must allow for some resort to extraneous material unless it is to be regarded as mere surplusage...
>
> It may well be that "reasonably ascertained" from the information recognises the use of some extraneous material or information. Support for this view can be found in a decision of the Supreme Court of Victoria in *Bailey v Hinch* [1989] V.R. 78. A similar, but not identical, provision was considered...[33]

KC:20 VCAT cautioned (at para 52) that the legislation requires an element of reasonableness about whether the person's identity can be ascertained, and this will depend upon the circumstances of each case.

CASE STUDY KC-1: Identity not "reasonably ascertainable"[34]

A university (in collaboration with other research institutions) conducted a pilot of a longitudinal study on health and relationships. The pilot was carried out by a contractor (a research foundation), and interviews were conducted by telephone. As part of the pilot, the applicant's partner was interviewed and a number of very personal questions were asked, involving information about the applicant and her partner.

The applicant was concerned that, although she did not participate in the survey, she was very much a part of the information elicited and her publicly listed telephone number was used by the researcher to interview the applicant's partner. It was argued that the applicant's identity could be reasonably ascertained by the researcher from the questions and answers provided by her partner, in conjunction with cross-matching her telephone number with electronic white pages in order to ascertain her name and address.

The university argued that the applicant's identity was not reasonably ascertainable because (i) it could not be assumed that the applicant's contact phone number was the same as that of her partner who had been interviewed (ie, that he lived there permanently); (ii) there was nothing in the partner's answers to home ownership that could link him to the address associated with the applicant's telephone number; (iii) the contractor kept names and telephone numbers on a separate database from the interview answers and questions; (iv) the contractor does not provide contact details to the university, but only provides the interview answers in de-identified form; and (v) as the applicant complained to the university soon after the interview, the contractor was able to strip her contact details from the database (although it would have been more difficult to do so at a later date).

VCAT accepted that the identity of the applicant could not be reasonably ascertained:

> Even allowing for the use of external information, the legislation requires an element of reasonableness about whether a person's identity can be ascertained from the information and this will depend upon all the circumstances in each particular case. Here, the alleged process of ascertainment would require inquiries from different databases, cross-matching and then cross-matching with an external database and even then the making of any possible connections would not identify with certainty. Even on the most favourable view to the applicant, this is beyond what is reasonable.[35]

VCAT found that this process of cross-matching research databases with external databases would "involve taking more than moderate steps".[36] Accordingly, VCAT was not satisfied that the complaint was about "personal information" within the meaning of the *Information Privacy Act*.

KC:21 The interpretation of "reasonably be ascertained" should take account of techniques such as email, unique machine addresses for every computer connected to the internet (IP addresses), "cookies" and other monitoring software, increasingly powerful online search engines, social media, biometrics,[37] smart cards,[38] reverse phone directories, video surveillance in public and workplaces, electronic databases of some public register data and other information services. Like the other uses of a reasonableness test in the IPPs, "reasonably" will qualify the operation of "ascertained" in practice.[39]

KC:22 In examining whether identity is apparent or may reasonably be ascertained, it is appropriate to consider how information from other sources may be used in conjunction with the recorded information or opinion to ascertain identity.[40] Consider whether identity *can* reasonably be ascertained, not whether anyone – the organisation holding it[41] or a third party[42] – intends to try.

KC:23 Biometrics (such as fingerprints and iris scans) and tissue samples (such as hair, blood and bodily samples) may, in some circumstances, enable a person's identity to be reasonably ascertained.[43] If the information is collected by an entity that has the means to analyse and identify an individual, then these sources of data may be regarded as "personal information". A sample of hair may be identifiable in the hands of a forensic scientist but would not normally be identifiable in the hands of a member of the public. Where the biometric is used to uniquely identify an individual, IPP 7 will be relevant.

Anonymised, de-identified and coded information

KC:24 In some instances, organisations may take steps to remove from information the elements that may lead to the identification of an individual. Instead of identifying material, such as a name, a number may be substituted. This is known as de-identification and coding. It aims to provide privacy protection by concealing the identity of an individual to whom the information relates, but to provide the information that will assist, for instance, in compiling demographic data. In some cases, it may be useful to code information that has been collected anonymously, for instance by assigning an identifier that indicates the gender and age of an individual without having collected further information that would otherwise render the person identifiable.

KC:25 The *National Statement on Ethical Conduct in Human Research* (jointly developed by the National Health and Medical Research Council, the Australian Research Council and the Australian Vice-Chancellor's Committee) provides a useful taxonomy for distinguishing identifiable data, coded data, and non-identifiable data – see Extract below. The authors of the taxonomy explain that they avoid the use of the term "de-identified" because it is ambiguously used to refer to data that is unidentifiable, as well as data that has identifiers removed but is still identifiable.

EXTRACT: National Statement on Ethical Conduct in Human Research, October 2007, page 29[44]

What are data?

Data are pieces of information, for example:

- what people say in interviews, focus groups, questionnaires, personal histories and biographies;
- analysis of existing information (clinical, social, observational or other);
- information derived from human tissue such as blood, bone, muscle and urine.

Data identifiability

Data may be collected, stored or disclosed in three mutually exclusive forms:

- **individually identifiable data**, where the identity of a specific individual can reasonably be ascertained. Examples of identifiers include the individual's name, image, date of birth or address;
- **re-identifiable data**, from which identifiers have been removed and replaced by a code, but it remains possible to re-identify a specific individual by, for example, using the code or linking different data sets;
- **non-identifiable data**, which have never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified. A subset of non-identifiable data are those that can be linked with other data so it can be known that they are about the same data subject, although the person's identity remains unknown.

This National Statement avoids the term "de-identified data", as its meaning is unclear. While it is sometimes used to refer to a record that cannot be linked to an individual ('non-identifiable'), it is also used to refer to a record in which identifying information has been removed but the means still exist to re-identify the individual. When the term "de-identified data" is used, researchers and those reviewing research need to establish precisely which of these possible meanings is intended.

Tissue and data

With advances in genetic knowledge and data linkage, and the proliferation of tissue banks of identified material, human tissue samples should always be regarded as, in principle, re-identifiable.

KC:26 Although the taxonomy refers to anonymous data as a sub-set of non-identifiable data, there may be times when anonymous data that is linked may become re-identifiable. For example, anonymous data that is linked and aggregated about the same person can lead to the creation of a profile from which a person's identity becomes reasonably ascertainable. This is especially likely when the person comes from a small community, in which the particular combination of data in the profile would relate to only one or a very few individuals.

KC:27 Finally, it should be remembered that coded or potentially re-identifiable information will, of course, remain identifiable to the entities in possession of the key or the means to generate the key. The ability to re-identify information may also arise where identifying information has been retained, such as where backup tapes are routinely kept as part of disaster recovery processes.

KC:28 The definition of personal information is very broad. When in doubt about whether information fits the definition, err on the side of treating information as personal information and consider the IPPs.

Distinguishing sensitive information from delicate information

KC:29 In privacy law and policy, the term "sensitive information" can confuse because it is commonly used in two ways:

a It is used in a technical way to mean one or more of the categories of information defined as "sensitive information" at the start of the IPPs.[45] This is how it is used in IPP 10 and IPP 2.1(a)(i).

b It is also often used to mean personal information of an especially delicate nature.

KC:30 "Sensitive information", in a technical sense, is not always delicate information, yet delicate information may include information that is not technically regarded as sensitive under the *Information Privacy Act*. For example, membership of a professional or trade association may not be considered "delicate" but, under the *Information Privacy Act*, it is defined as "sensitive information". Conversely, personal information such as a person's financial affairs or even address can sometimes be very delicate, yet it does not fall within the technical definition of "sensitive information".

KC:31 Financial records may be a very delicate issue for an individual, but completely innocuous to a bank or to strangers. A victim of domestic violence or an undercover police operative might consider their home address to be a delicate and highly confidential item of information. The fact that a person is employed in a certain profession can be delicate (eg brothel manager), and public exposure of that fact could pose a risk to personal safety or to relationships with persons to whom the worker has chosen not to reveal their work, such as parents or grandparents.

KC:32 Many organisations routinely deal with particular types of delicate information. This familiarity can breed a kind of insensitivity to that type of data, and carelessness may follow. Organisations should always be aware that what may seem routine or innocuous to the organisation may not be to the subject of it or to persons who know that person in other contexts in their life.

KC:33 A useful test for determining whether information is delicate was provided by Chief Justice Gleeson in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63 at para 42:

> Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.

KC:34 While some categories of information are easily identifiable as delicate or sensitive (such as those listed in the definition of "sensitive information" in the *Information Privacy Act*), other information may be regarded as delicate where the disclosure "would be highly offensive to a reasonable person of ordinary sensibilities".

KC:35 In applying the IPPs in specific cases, it is invariably important to consider the nature of the personal information in the particular circumstances, at the particular time.

KC:36 As the former Privacy Commissioner Paul Chadwick explained in OVPC's guidelines for website privacy, even a name can be regarded as delicate information:

> Because information is itself so context-specific, the IPPs are necessarily flexible. One useful way to illustrate how dependent information is on context is to notice that your name means one thing in the White Pages, another thing on the Australia Day Honours List, and quite another thing again on a register of sex offenders. In the first context, it is neutral in the sense that it just connects you with a phone number and address. In the second context, it is favourable. In the third, it is very unfavourable. Yet it is the same information. It is the varying contexts that matter so much.[46]

KC:37 A final point to note when handling delicate information is that higher standards of protection than the *Information Privacy Act* requires may be appropriate, or even mandatory. The IPPs establish a minimum level of protection for the collection and handling of information. Organisations may provide more stringent protection. The *Information Privacy Act* recognises the need for more stringent protections in some cases by acknowledging other laws should prevail over the *Information Privacy Act*,[47] and by enabling Codes of Conduct to be issued under the *Information Privacy Act*.[48]

Consent

KC:38 The concept of consent is central to privacy. The indignity and lack of control that people feel as a result of an interference with their information privacy is often reflected in phrases such as, "I would have let you if you'd just asked first" and, "How did you get my number?"

KC:39 Consent is not the only basis by which information can be collected, or used. The IPPs include provisions for non-consensual collection and uses/disclosures. Consent is of particular utility to agencies to satisfy both their own information needs and their obligations under the *Information Privacy Act*. If an organisation needs to use or disclose someone's personal information, it may be easiest to simply ask for the individual's consent to do so.

KC:40 Consent is referred to in the following IPPs:

a IPP 2.1(b) – consent to use/disclosure;

b IPP 2.1(c) – research use/disclosure where it is impracticable to seek prior consent;

c IPP 7.2(b) – adopting another organisation's unique identifier with consent;

d IPP 7.3(c) – consent to use/disclosure of a unique identifier;

e IPP 9.1(b) – consent to the transfer of information outside Victoria;

f IPP 9.1(e) – transfer of information outside Victoria where it is impracticable to obtain consent or where the individual would likely give consent;

g IPP 10.1(a) – consent to the collection of sensitive information;

h IPP 10.1(c) – collection of sensitive information where an individual is physically or legally incapable of giving consent or cannot communicate that consent; and

i IPP 10.2(c) – collection of sensitive information for research and other specified purposes where it is impracticable to seek consent.

KC:41 Section 64 is also relevant where an individual's consent is required (for a collection, use, disclosure, transfer or for the exercise of an access request), but the individual lacks capacity to consent. This section is discussed further, under "Capacity".

Elements of consent

KC:42 The essential elements of consent are that the:

a individual has the **capacity** to consent;

b consent must be **voluntary**;

c consent must be **informed**;

d consent must be **specific**; and

e consent must be **current**.

KC:43 Assessing these factors will depend on the circumstances of each case.

Capacity

KC:44 An individual may not be capable of giving consent. Age, or physical or mental disability may prevent the person communicating. They may have limited understanding of English. He or she may not understand the general nature and effect of giving or withholding consent.[49] If an organisation is uncertain that the person has capacity, it should not rely on any purported consent.

KC:45 Capacity to consent (under IPPs 1, 2 and 9) and to make access and correction requests (under IPP 6) is addressed in section 64. Section 64 deals with situations where the person is incapable of understanding the general nature and effect of consenting or making an access request, or is unable to communicate their consent or make the access request, by reason of age, injury, disease, senility, illness, disability, physical or mental disorder (s 64(3)). Where a person is incapable of consenting or making a request for access or correction, an authorised representative may do so on his or her behalf.

KC:46 Where the personal information concerns a child or young person, for instance, he or she may be able to exercise their rights under the *Information Privacy Act* independently of a parent or guardian if he or she has sufficient understanding and intelligence to give valid consent (the "Gillick test"[50]). This is not to say that a child can veto an organisation's decision to disclose information about them, such as when a school decides to disclose a child's educational or other records to the child's parents and this disclosure is reasonably expected. (See the OVPC's Information Sheet 02.02, *Privacy and School Reports*, May 2002.)

KC:47 The *Information Privacy Act* defines a child as being a person under the age of 18 years, but it does not state when a child is incapable of giving consent or exercising their right of access and correction. The Health Services Commissioner's Information Sheet No. 5, *Minors, Privacy Laws and Consent*, provides useful guidance to assist organisations in determining the capacity of children and young people and incorporates consistent advice from the Federal Privacy Commissioner. See the Extract.

EXTRACT: Victorian Health Services Commissioner, Minors, Privacy Laws and Consent, Information Sheet No.5[51]

Capacity to consent

Determining the competence of a minor to consent can be complex. A minor is capable of giving informed consent when he or she achieves a sufficient understanding and intelligence to enable him or her to understand fully what is proposed. This test comes from the English case of *Gillick v West Norfolk AHA* (1986) AC 112 which has been applied for many years when providing health services to minors.

A child's consent may be overridden by a court order on the basis of the "child's best interests".

Privacy rights

The *Health Records Act* 2001 (HRA) defines a child as being a person under the age of 18 years but does not specify the age individuals may be considered capable of giving consent. A child, like any other person, has a right to the privacy of their information. They can also exercise a right of access to their health information depending on their capacity to consent.

A parent's right to make decisions about their child's health information ceases once the child is 18, when the child becomes legally entitled to make their own decisions, or earlier if they have the capacity to give informed consent (as per the *Gillick* test above).

The *Privacy Act* does not define nor does it prescribe the age individuals may be considered capable of giving consent on their own behalf. Guidelines issued by the Federal Privacy Commissioner on the application of the *Privacy Act* in the private health sector state that:

> determining competence can be complex, such that the health service provider must have regard to the maturity of the young person and their understanding of relevant circumstances. In certain circumstances, young persons will have attained sufficient competence (maturity and understanding) to make their own decisions. Conversely there will be older teenagers who lack such competence. Nevertheless their views must be considered too. Health service providers will need to deal with each case subject to its circumstances.

KC:48 When dealing with individuals who may not have the capacity to make their own decisions, organisations should refer to the helpful guidance issued by the New South Wales Privacy Commissioner.[52] That guide includes the following checklist to assist agencies in making decisions about what happens to the person's information where they are unable to make decisions, or rely on others to act on their behalf:

Checklist for alternative decision-making

Relevant requirements

☐ What are the IPPs or complaints mechanisms that are relevant to the information handling conduct?

The person's capacity

☐ Does the person have capacity to exercise their entitlements under the IPPs and the [privacy law] (including the complaints mechanism) in relation to the conduct? If not, please see "alternative decision-making" below.

Alternative decision-making

☐ Can the person express a view about the conduct at the present time?

☐ Has the person been given an opportunity to express their views or opinions about how their personal information is handled?

☐ How has the person been provided with support that is appropriate to their capacities and their cultural and linguistic background to enable them to be involved in decisions about the conduct?

☐ Has the person previously expressed a view or wish about the conduct of which the agency is aware or could reasonably make itself aware?

☐ Is there any reason why the person's current wishes or previously expressed wishes cannot or should not be followed now?

☐ Is it possible to seek the views or consent of the person's representative?

☐ If so, how was the person's representative identified?

☐ Have the views or consent of the representative been considered?

☐ Have all other relevant criteria been assessed and considered before making a final decision about what happens to the person's information?

KC:49 A list of persons who can act as "authorised representatives" for individuals who lack capacity is set out in section 64(6). They include parents of children under the age of 18 years, guardians under an enduring power of attorney, and others empowered in various ways to perform functions in the best interests of the individual – except where the representative is acting inconsistently with an order made by a court or tribunal. For example, a court order directing a parent not to contact a child is likely to be inconsistent with that parent purporting to exercise an access request on behalf of the child. The list in section 64(6) does not give priority to any one category of authorised representative.

KC:50 An authorised representative is only permitted to exercise a power to consent or request access or correction where this is "reasonably necessary for the lawful performance of functions or duties or exercise of powers in respect of the individual by the authorised representative" (ss 64(1) and (2)). The scope of these functions, duties or powers may be specified in a court order (such as a parenting order made under the *Family Law Act 1988* (Cth)) or in a document authorising the representative to act on the individual's behalf, such as in an enduring power of attorney document. Or they may be listed in other legislation, such as in the case of administrators under the *Guardianship and Administration Act 1986* (Vic) or agents under the *Medical Treatment Act 1988* (Vic).

KC:51 OVPC has released general guidance which discusses how children, parents and guardians are able to make privacy complaints under the *Information Privacy Act*.[53]

Voluntary

KC:52 An individual must be free to exercise genuine choice. Consent must be given without coercion or threat and with sufficient time to understand the request and, if appropriate, obtain advice. Likewise, an organisation should not suggest that it has obtained consent if the "consent" is one obtained through the operation of law. Giving "notice" that a collection, use or disclosure is to occur is not the same as obtaining "consent".

KC:53 In many circumstances, an individual does not have an effective or real choice over whether or not to give consent. For example, voluntary consent may be difficult to obtain from a job applicant or employee who is asked to undergo a criminal record check, a medical examination, drug testing or a psychological assessment. That is not to say that these checks cannot be undertaken, where they are necessary, relevant to the position to be filled, and are not unreasonably intrusive. An applicant that applies for a job with the prerequisite of a police check could be said to have impliedly consented to the collection of that person's criminal history.[54] See Case Study KC-2 where the Privacy Commissioner considered that purported consent was not voluntary.

CASE STUDY KC-2: Purported consent not voluntary[55]

The complainant was an employee of the respondent organisation and made a bullying claim against co-workers. The complaint documentation consisted of a letter outlining the outcomes the employee sought, and a chronological list of all of the bullying incidents alleged to have occurred. The complainant met with a staff member of the organisation who explained the complaint process and advised that a full copy of the complaint documentation would be provided to each of the alleged bullies. The complainant agreed to this in the belief that there was no other choice, but later attempted to withdraw her consent as she was anxious about the information contained in the complaint documentation. The organisation advised that the documentation had already been forwarded to the alleged bullies.

The Privacy Commissioner decided that the complainant's consent could not be relied upon, as under IPP 2.1(b) individuals must be provided with a real choice about what will happen with their personal information. The complainant was merely told that the disclosure of her complaint documentation to the alleged bullies was part of the complaint investigation procedure and that there was, in effect, no other option.

Informed

KC:54 The individual must have full knowledge of all relevant facts, including:

a the personal information to be collected or used or disclosed;

b the purpose or purposes it will be put to;

c who will get the information, to whom it may be passed on, and what use the recipient(s) will make of the information;

d the consequences of giving consent, or of failing to give consent.

KC:55 Incorrect or misleading information may render the consent invalid.

Specific

KC:56 Consent must be specific enough in all the circumstances. If the information given is too broad or vague, the consent may not be specific enough to be regarded as valid consent for the particular collection, use or disclosure the organisation makes. Broadly worded consent statements asking individuals to agree to any use and disclosures of their personal information may raise issues with IPP 1 (Collection) and why it is necessary or lawful for that particular personal information to be collected. The level of specificity will depend on factors including:

a the nature of the personal information;

b the proposed use or disclosure;

c the recipient and its proposed use or disclosure; and

d the recipient's level of accountability.

KC:57 Generally, the more privacy-invasive the proposed use or disclosure, the more specific the required information and consent should be.

Current

KC:58 Consent has a use-by date.

KC:59 Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. It is good practice to inform the individual of a specified period for which the consent will be relied on in the absence of a material change of circumstances that the organisation knows or ought reasonably to know.

KC:60 Organisations should make it clear to the individual that he or she is entitled to change his or her mind and revoke consent. Information on how the individual can do this should be provided. There may be examples where Parliament has enacted legislation that expressly deals with the revocability of consent. For instance, a statute may state that consent is irrevocable, or the law may set conditions around the timing and effect of any withdrawal of consent.[56]

Bundled consents

KC:61 Bundled consents refer "to the practice of bundling together consent to a wide range of uses and disclosures of personal information without giving individuals an opportunity to choose which uses and disclosures they agree to and which they do not."[57]

KC:62 The then Australian Privacy Commissioner raised concerns about bundled consents in *OPC v Employment Services Company* [2005] PrivCmrA 13, an own motion investigation into a company that assessed job applicants' qualifications and placed them with employers for a fee. A wide range of information was collected (including tax file numbers, credit card details and copies of passports) and the collection statement asked job applicants to consent to a broad range of uses and disclosures of their information which may not have been necessary. The Federal Privacy Commissioner took the view that:

> ...broad or "bundled" consent forms diminish individuals' freedom of choice, effectively coercing individuals to hand over their personal information and to agree to a variety of uses and disclosures in exchange for a service.

KC:63 If the use of bundled consents is contemplated, organisations should consider whether individuals are:

a given a reasonable opportunity to *freely* elect to refuse consent to one or more proposed uses or disclosures;

b sufficiently informed about each of the proposed uses or disclosures, including the purpose for use or disclosure, the identity or type of organisation who will receive the information, and any further use or disclosure the recipient is to make of the information;

c informed of any law that requires the individual to consent to any one or more of the proposed uses or disclosures, and which of these proposed uses and disclosures are not compulsory; and

d advised of the consequences (if any) of failing to consent to any one or more of the proposed uses or disclosures.

Implied consent

KC:64 "Consent" is defined in the *Information Privacy Act* to mean express consent or implied consent.

KC:65 As a general rule, and depending on the nature of the personal information, seek express consent in writing. Implied consent can be obtained where consent can reasonably be inferred from a person's conduct or actions. The test is objective.

KC:66 Be careful not to make assumptions about implied consent not based on fact. It is risky to infer consent from a person's mere failure to state his or her lack of consent. The person may not have heard, understood or had sufficient information on which to decide to refuse.

KC:67 Consent should not be inferred in a particular case just because:

a most people have consented to the same use or disclosure;

b the benefits of consenting, as the organisation sees them, mean that the individual would probably consent if asked;

c the individual has given consent in the past; or

d the disclosure is to a spouse or family member.

KC:68 Implied consent involves difficult judgments. If a complaint results, implied consent may be difficult to establish and the party relying on the consent bears the onus of establishing it. It is far better practice to obtain express consent and avoid the pitfalls inherent in implied consent.

Opting in versus opting out of direct marketing

KC:69 Organisations may at times engage in direct marketing to, for instance, raise funds or to inform clients or consumers of various products or services related to the organisation's activities or functions. This may be permitted under the *Information Privacy Act* where it is carried out with individuals' consent.

KC:70 However, unlike the private sector provisions of the Commonwealth *Privacy Act 1988,* which allow organisations to make first contact with consumers and provide consumers with the ability to opt out of receiving further direct marketing,[58] there are no equivalent direct marketing provisions in the Victorian *Information Privacy Act*. On the contrary, the policy underlying the Victorian *Information Privacy Act* is less tolerant of direct marketing than the *Privacy Act 1988* (Cth). The Explanatory Memorandum to the *Information Privacy Bill* suggests that secondary use of public register information for direct marketing may be an interference with privacy:

> While public register information should be able to be used for the, or one of the, legitimate purposes for which it was collected, it is intended that the Act will in most cases treat uses outside those purposes as interferences with personal privacy.
>
> For example, it may be an interference with the privacy of an individual for a person to search through the names, addresses and other information held on the Land Register in order to identify and market products or services to a section of the Register that meets a particular socioeconomic profile. In these circumstances, the organisation using that information may contravene the Act.[59]

KC:71 Accordingly, when proposing to use information for the purpose of fund-raising or marketing, organisations should generally seek individuals' prior consent to that use. Organisations that are likely to need to use personal information to raise funds or market goods or services should consider seeking consent at the time of collection.

Purpose

KC:72 The purpose of an action is the reason for which it is intentionally done.

KC:73 In *Ng v Department of Education* [2005] VCAT 1054 at paras 88-89, VCAT took a narrow view of the meaning of "purpose", suggesting that the term be regarded as synonymous with the intent with which personal information was collected. This involves a subjective enquiry into the motive underlying the collection, rather than an objective enquiry into the effect the collection practice would have. VCAT cautioned against taking an objective view of "purpose" as that would result in too wide a purpose and one that would frustrate the intention of the *Information Privacy Act* to limit and constrain the use of personal information.

KC:74 Unless an organisation knows what it intends to do with the personal information it collects, it cannot readily assess or assert its necessity (IPP 1.1) or even perhaps its lawfulness and fairness (IPP 1.2).

KC:75 Purpose is expressly referred to in the following IPPs:

a IPPs 1.3 and 1.5 – collection notices to inform individuals of the purposes for which their information is collected;

b IPP 2 – distinguishing primary purpose from secondary purposes for using and disclosing information;

c IPP 4.2 – determining whether information is no longer needed for any purpose;

d IPP 5.2 – documenting in your privacy policy what, and for what purposes, information is held, used and disclosed;

e IPP 7.4 – requiring individuals to provide a unique identifier to access services when the provision of services is tied to the purpose (or a directly related purpose) for which the identifier was assigned;

f IPP 10.2(a)(ii) – collecting sensitive information about a person's ethnic or racial origin without consent for the purpose of providing government funded targeted welfare or educational services, where there is no reasonably practicable alternative for collecting the information for that purpose.

KC:76 Determining the purpose also helps an organisation ascertain the required standard of data quality (IPP 3), and whether additional steps should be taken to secure the data (IPP 4.1).[60]

"Function creep"

KC:77 "Function creep" refers to situations where personal information collected for one stated reason is later used for other purposes, perhaps quite unrelated to the purpose of collection. The term takes on a pejorative meaning in circumstances where individuals might not have willingly given up their information or tolerated the introduction of a new potentially intrusive practice had they known what uses would eventually be made of their information. This is particularly so where the secondary uses were not originally envisaged and are privacy-invasive, or where assurances had been given that functions would not creep and that the eventual uses would not occur. Function creep undermines the transparency objective of the *Information Privacy Act*, and is destructive of public trust in government. The *Information Privacy Act* is intended in part to build trust.[61]

KC:78 Organisations should consider what other, secondary purposes the information may be used for, beyond what the individual might reasonably expect. These secondary purposes may be quite legitimate and, by anticipating them in advance, organisations may be able to more readily comply with the *Information Privacy Act*. For instance, personal information collected in providing an educational or welfare service may be useful for later research. Anticipating this use allows organisations to seek prior consent to that use, obviating the need to establish later whether obtaining consent is "impracticable" (under IPP 2.1(c)).

KC:79 In other cases, using information for unrelated purposes may be incompatible with the primary purpose for collection, or may require decision makers to be advised of the competing public interests so that the appropriate balancing is undertaken and the need for additional safeguards is considered. For instance, it has already been recognised that allowing commercial use of enrolment information is incompatible with compelling individuals to enrol to vote.[62] Where people lack confidence that their data is to be used in accordance with assurances given, or believe inadequate safeguards exist to balance competing interests, the quality of the information they provide may suffer.[63]

KC:80 There are many good reasons for making secondary use of information already collected. However, transparency and proper limits are required to maintain individuals' willingness to supply their information fully and accurately and to maintain trust that personal information is used responsibly and legitimately

Necessary

KC 81 Necessity is referred to in the following IPPs:

a IPP 1.1 – collection must be necessary for one or more of an organisation's functions;

b IPP 2.1(c) – use/disclosure necessary for research, or compilation of statistics, in the public interest;

c IPP 2.1(d) – use/disclosure necessary to lessen or prevent a serious threats to individuals or the public;

d IPP 2.1(e) – use/disclosure as a necessary part of an organisation's investigation into suspected unlawful activity;

e IPP 2.1(f) – use/disclosure reasonably necessary to enable a law enforcement agency to carry out specified functions;

f IPP 7.1 – assigning a unique identifier necessary to enable an organisation to carry out its functions efficiently;

g IPP 7.2(a) – adopting another organisation's unique identifier necessary to enable an organisation to carry out its functions efficiently;

h IPP 7.3(a) – use/disclosure of a unique identifier necessary to fulfil obligations to another organisation;

i IPP 9.1(c) – transfer of personal information outside Victoria is necessary for the performance of a contract to which the individual is a party, or for implementation of pre-contractual measures at the individual's request;

j IPP 9.1(d) – transfer of personal information outside Victoria is necessary for the conclusion of a third-party contract concluded in the interest of the individual;

k IPP 10.1(c) – collection of sensitive information is necessary to lessen or prevent a serious threat to any individual where the data subject is physically or legally incapable of giving consent or physically cannot communicate that consent;

l IPP 10.1(d) – collection of sensitive information is necessary for the establishment, exercise or defence of a legal or equitable claim;

m IPP 10.1(a) – collection of sensitive information is necessary for research of statistics relevant to government funded targeted welfare or educational services.

KC 82 In *Ng v Department of Education,*[64] VCAT accepted that "necessary" does not mean essential but rather (as suggested by the High Court of Australia in a 1999 case)[65] "subjected to the top scale of reasonableness".

KC 83 International human rights jurisprudence provides a useful interpretation of what is "necessary" in a democratic society:

> the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable", or "desirable".[66]

KC 84 The High Court of Australia has held that "necessary" does not mean unavoidable, essential or indispensable. The Court noted that the term has been (perhaps unhelpfully)[67] interpreted to mean "reasonably appropriate and adapted" and suggested that an assessment of necessity involve consideration of what is proportionate,[68] or involve "close scrutiny, congruent with a search for 'compelling justification'".[69]

KC 85 Under the *Charter of Human Rights and Responsibilities Act 2006* (Vic), issues of necessity and proportionality are also relevant to the conduct of public sector organisations where their acts and practices have an impact on privacy and other human rights recognised under the Charter.[70]

KC:86 What is clear is that "necessary" requires more than what may be administratively convenient or desired. In an era in which government administration has access to very powerful information and communications technologies, for which individuals' personal information is a fuel, it is important to guard against a temptation – however understandable it may be – to read down the test of necessity.

KC:87 The concept of necessity is discussed further in these Guidelines, as it arises in the context of each of the relevant IPPs.

Reasonable, reasonably

KC:88 Variations of "reasonableness" appear in the definition of "personal information" and throughout several of the IPPs at:

a IPP 1.2 – not collecting personal information in an unreasonably intrusive way;

b IPPs 1.3 and 1.5 – taking reasonable steps to notify individuals of the identity of the collecting organisations, the purposes for which the information is collected, the usual disclosures etc;

c IPP 1.4 – collecting information about an individual directly from that individual, where reasonable and practicable to do so;

d IPP 2.1(a) – use/disclosure of information for reasonably expected secondary purposes that are (directly) related to the primary purpose of collection;

e IPP 2.1(c) – use/disclosure for research in the public interest, where the disclosing organisation reasonably believes the recipient will not further disclose the information;

f IPP 2.1(d) – use/disclosure where the organisation reasonably believes it is necessary to lessen or prevent serious (and imminent) threats to an individual's life or their (or the public's) health, safety or welfare;

g IPP 2.1(g) – use/disclosure to a law enforcement agency where the organisation reasonably believes the disclosure is reasonably necessary for that agency to carry out specified law enforcement functions;

h IPP 3.1 – taking reasonable steps to ensure personal information is accurate, complete and up to date;

i IPP 4.1 – taking reasonable steps to protect personal information from misuse, loss or unauthorised access, modification or disclosure;

j IPP 4.2 – taking reasonable steps to destroy or permanently de-identify information after it is no longer needed for any purpose;

k IPP 5.2 – taking reasonable steps to let a person, upon request, know the organisation's information handling practices;

l IPP 6.1(b) – denying access to information where that access would have an unreasonable impact on the privacy of other individuals;

m IPP 6.3 – where reasonable, considering the use of mutually agreed intermediaries to provide sufficient access to meet the needs of both parties, where the organisation is not required by IPP 6.1 to provide access;

n IPP 6.5 – taking reasonable steps to correct information that an individual has established to be inaccurate, incomplete or out of date;

o IPP 6.6 – taking reasonable steps to include a statement with the information claiming it is inaccurate, incomplete or out of date, where the individual and the organisation disagree about its data quality;

p IPP 9.1(a) – transferring personal information outside of Victoria where the organisation reasonably believes the recipient is subject to a substantially similar privacy law, binding scheme or contract;

q IPP 9.1(f) – transferring personal information outside of Victoria where the organisation has taken reasonable steps to ensure it will not be handled by the recipient inconsistently with the IPPs;

r IPP 10.2 – collecting sensitive information without the individual's consent for specified government educational or welfare purposes where there is no reasonably practicable alternative to collecting for that purpose.

KC:89 The precise application of the term "reasonable" will differ according to the context in which it is applied. This means that it will depend on the particular organisation and the circumstances surrounding the personal information.

KC:90 To be reasonable is to be fair, proper and moderate. The High Court has considered that what is reasonable is a judgment of fact and deciding what is reasonable will depend on each particular case,[71] and may be influenced by current standards.[72] A reasonableness test implies the application of reasoned and objective judgment to the circumstances. It implies taking a balanced view.

Practicable

KC:91 The IPPs refer to the term "practicable" at:

a IPP 1.3 – giving notice at or before the time of collection or, if that is not practicable, as soon as practicable after;

b IPP 1.4 – only collecting information directly from individuals if it is reasonable and practicable to do so;

c IPP 2.1(c) – use/disclosure of information for research and statistical purposes where it is not practicable to seek prior consent;

d IPP 6.8 – responding to access requests as soon as practicable;

e IPP 8.1 – allowing individuals to transact anonymously wherever it is lawful and practicable to do so;

f IPP 9.1(e) – transfer of information outside of Victoria for the individual's benefit where it is impracticable to obtain the individual's consent or, where it is practicable to obtain consent, the individual would be likely to give it;

g IPP 10.2(a) – collection of sensitive information for specified research and statistical purposes where there is no reasonably practicable alternative to collecting the information for that purpose, and it is impracticable to seek the individual's consent to the collection.

KC:92 Practicable means capable of being done or feasible. The word also incorporates an element of reasonableness.

KC:93 When the reasonableness or practicability of doing something is at issue, cost is one consideration but it is not the only one or even the primary one. Like other pieces of legislation that have an impact on Victorian public sector agencies, the *Information Privacy Act* means changes may need to be made. Processes and procedures need to be assessed and where necessary amended, time and attention spent, and costs incurred. This is only fair and proper. The fact that the *Information Privacy Act* requires such measures does not, and cannot, make compliance "not reasonably practicable". But resources are not unlimited either. Each case will require analysis and balancing according to the particular circumstances.

Key Concepts Notes

[16] Section 35 of the *Interpretation of Legislation Act 1984* (Vic) addresses the principles for interpreting statutes and includes a list of sources that can be used to aid statutory interpretation.

[17] *IW v City of Perth* (1997) 191 CLR 1.

[18] *WL v La Trobe University* (General) [2005] VCAT 2592 at paragraph 9 (8 December 2005, per Coghlan DP); *GA v Commissioner of Police, NSW Police* [2005] NSWADT 121 per Deputy President Hennessy commented (at para 16) in relation to the NSW privacy law: "One of the purposes of the PPIP Act, as evidenced by its long title, is to 'provide for the protection of personal information, and for the protection of the privacy of individuals generally'. That protection is not absolute. The PPIP Act places limits on the protection of personal information so that potentially competing objectives in other legislation... are not usurped.... The PPIP Act is beneficial legislation and, in the words of Brennan CJ and McHugh J in *IW and the City of Perth* (1997) 191 CLR 1 at 12: '...It is to be given "a fair, large and liberal" interpretation rather than one which is "literal or technical". Nevertheless, the task remains one of statutory construction. Although a provision of the Act must be given a liberal and beneficial construction, a court or tribunal is not at liberty to give it a construction that is unreasonable or unnatural...'"

Also see *MT v Director General, NSW Department of Education & Training* [2004] NSWADT 194 per Judicial Member Montgomery at para 171:

> A proper function of the purposive approach is to give effect to the identified legislative purpose. I agree that with [sic] the Commissioner's submission that in the absence of clear and unambiguous language to the contrary, the protection of privacy as a fundamental human right justifies a construction of privacy legislation that is consistent with the legislature's intention to minimise exceptions to the general statutory restrictions on interfering with individuals' privacy...

Further, see *KD v Registrar, NSW Medical Board* [2004] NSWADT 5 and *MG v Director General, Department of Education and Training* [2004] NSWADT 137.

[19] Section 32, *Charter of Human Rights and Responsibilities Act 2006* (Vic).

[20] Section 38, *Charter of Human Rights and Responsibilities Act 2006* (Vic).

[21] Not having to assess whether the information is true speeds the process and widens the scope. But if you find that information is personal information and is not true, the data quality principle (IPP 3) will need considering.

[22] The *Health Records Act 2001* (Vic) protects the privacy of health information. Health information is also part of the Commonwealth *Privacy Act*'s definition of sensitive information.

[23] See, for example, the data protection laws in Ireland, Sweden and the United Kingdom, discussed by Douwe Korff [consultant to the European Commission (EC)] in *EC Study on Implementation of the Data Protection Directive: Comparative Summary of National Laws*, September 2002, pages 33-35, available at http://www.garanteprivacy.it.

[24] For example, see the *Health Records Act 2001* (Vic), s 3 ("personal information") and s 95; the *Privacy and Personal Information Act 1998* (NSW), s 4(3)(a); the *Information Act 2003* (NT), s 4 ("person") and s 155; and the *Personal Information Protection Act 2004* (Tas), s 3 ("personal information").

[25] *Freedom of Information Act 1982* (Vic), ss 5 ("record"), 33 (document affecting personal privacy), and 39 (amendment of record).

[26] Victoria, Department of State and Development, Multimedia Victoria, *Information Privacy in Victoria: Data Protection Bill*, discussion paper, July 1998, p 12, available at http://www.egov.vic.gov.au.

[27] Victoria, Legislative Assembly, *Parliamentary Debates*, 5 September 2000, 498 (John Brumby, Minister for State and Regional Development).

[28] See, for example, *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77, where the Appeal Panel applied *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192 (at para 21) to find that information conveyed to an organisation verbally and held only in the mind could not be caught by the privacy legislation "provided it was never reduced to a written record".

[29] Although there is New Zealand case law to suggest that information stored in someone's mind is "personal information" if it is readily retrievable (*Reporter seeks access to unwritten information held by government ministry* (Case Note 37930) [2002] NZPrivCmr 10 (1 June 2002); *Woman seeks access from former employer to content of verbal reference* (Case Note 210106) [2010] NZPrivCmr 14 (1 June 2010)), that has not been the case in Australia. In *Vice Chancellor, Macquarie University v FM* [2005] NSWCA 192 (10 June 2005), the NSW Court of Appeal decided that information obtained visually or aurally and not otherwise documented is not to be regarded as being "held" under the NSW privacy law. The Court suggested that, to find otherwise, would make a nonsense out of having to comply with the other principles in the Act, such as the obligations to ensure information is accurate and up to date, and to dispose of information securely.

[30] Also see para 39 of the judgment, *Ng v Department of Education and Training* [2005] VCAT 105, where VCAT remarked that CCTV recordings in the street may likewise be regarded as personal information.

[31] The *Surveillance Devices Act 1999* (Vic) prohibits surveillance of private activities and private conversations, unless carried out with the parties' consent or pursuant to a warrant. Due to the way the terms "private activity" and "private conversation" are defined under this Act, surveillance is not prohibited where: (i) an activity is conducted outside of a building or in a place where an individual should reasonably expect he or she may be seen by another person; or (ii) where a conversation is carried on in circumstances where an individual should reasonably expect he or she may be overheard by another person.

[32] In August 2010, the then Victorian Attorney-General tabled the report of the Victorian Law Reform Commission, *Surveillance in Public Places: Final Report*. The report recommends that surveillance laws be modernised and that responsible use of surveillance devices in public places be promoted by greater regulation. At the time of publication, neither the former nor current Victorian governments had formally responded to the report. The full report is available at http://www.lawreform.vic.gov.au.

[33] *WL v La Trobe University* [2005] VCAT 2592, paras 44-45 and 47.

[34] *WL v La Trobe University* [2005] VCAT 2592.

[35] *WL v La Trobe University* [2005] VCAT 2592 at para 52.

[36] *WL v La Trobe University* [2005] VCAT 2592 at para 42.

[37] A biometric identifier is a form of identification that relates to a person's biomedical information. Common biometric identifiers include blood, fingerprints, DNA and iris scans. Biometrics include photographs, including where these are used in conjunction with facial imaging software in real time.

[38] A smart card is any type of card that has an embedded microchip. The degree of sophistication can vary, but most smart cards are capable of storing significant amounts of data which can be modified with the use of a smart card reader. Common smart cards include building access cards, e-tags and public transport stored value cards, such as the Victorian myki card.

[39] The concept of "reasonableness" is discussed later in this Key Concepts section – see paras KC:88-KC:90.

[40] For example, in *Complainant AH v Department* [2007] VPrivCmr 3, the Privacy Commissioner considered whether a Department representative, upon visiting a small rural community and disclosing details about the purpose of his visit (namely to investigate a serving staff member, the complainant, currently on sick leave) identified the complainant. The Privacy Commissioner decided that, although the complainant's name was not specifically mentioned, the Department had disclosed personal information about the complainant as the information could be reasonably ascertained within the small rural community.

[41] *Information Privacy Act* s 4 states that an organisation "holds" personal information if the information is contained in a document that is in the possession or under the control of the organisation, whether alone or jointly with other parties, regardless of whether the document is situated in or outside of Victoria.

[42] "Third party" is defined in *Information Privacy Act* s 3 as meaning any person or body other than the organisation holding the information and the individual to whom the information relates.

[43] There are differing views amongst privacy offices about whether tissue samples are "personal information", as distinct from information derived from analysing a sample. See, for example, the discussion by the Australian Law Reform Commission and the Australian Health Ethics Committee in their joint report, *Essentially Yours: The Protection of Human Genetic Information*, March 2003 (tabled June 2003), Chapter 8. The law in this area is currently unsettled. Note, though, that there is an international commitment to protect the privacy of human genetic data and the biological samples from which that data is extracted, recently acknowledged by Australia and other nations in the United Nations Educational, Scientific and Cultural Organisation's *International Declaration on Human Genetic Data*, adopted unanimously and by acclamation on 16 October 2003, available at http://unesdoc.unesco.org. Also refer to the Office of the Victorian Privacy Commissioner's publications on:

- *Submission to the Victorian Parliament Law Reform Commission on its Inquiry into Forensic Sampling and DNA Databases*, July 2002, esp. pages 3 and 37-38;
- *Supplemental Submission to the Victorian Parliament Law Reform Commission on its Inquiry into Forensic Sampling and DNA Databases*, September 2002, esp. pages 1-2;
- *Submission to the Australian Law Reform Commission and the Australian Health Ethics Committee joint inquiry into Protection of Human Genetic Information*, December 2002, esp. pages 2-3 and 27;
- *Submission to the Forensic Procedures Review Committee on its Review of Part 1D of the Crimes Act 1914* (Cth), September 2002, esp. pages 4-5 and 5-16; and
- *Submission to Further Independent Review of Part 1D of the Crimes Act 1914* (Cth); January 2010.

[44] Australia, National Health and Medical Research Council and others, *National Statement on Ethical Conduct in Human Research*, October 2007, page 29. Pages 25-26 are available from http://www.nhmrc.gov.au.

[45] Schedule to the *Information Privacy Act 2000* (Vic). The meaning of "sensitive information" is discussed further in these Guidelines in the section dealing with IPP 10.

[46] Office of the Victorian Privacy Commissioner, *Website Privacy – Guidelines for the Victorian Public Sector*, May 2004, page 7.

[47] Section 6, *Information Privacy Act 2000* (Vic).

[48] Part 4, *Information Privacy Act 2000* (Vic).

[49] Refer to Privacy NSW's *Best Practice Guideline, Privacy and people with decision-making difficulties*, February 2004, available at http://www.lawlink.nsw.gov.au.

[50] The Gillick test comes from the English House of Lords case of *Gillick v West Norfolk AHA* (1986) AC 112, which has been applied in Australia for many years in relation to determining when minors are capable of giving informed consent to a particular action or arrangement. In Gillick, their Honours said: "A minor is, according to this principle, capable of giving informed consent when he or she 'achieves a sufficient understanding or intelligence to enable him or her to understand fully what is proposed.'"

[51] This Information Sheet is available at http://www.health.vic.gov.au/hsc.

[52] Privacy NSW, *Privacy and people with decision-making disabilities*, Best practice guide, February 2004, updated 2005, available at http://www.lawlink.nsw.gov.au/lawlink/privacynsw.

[53] See Office of the Victorian Privacy Commissioner Information Sheet 04.09, *Children and Privacy Complaints: A Guide for Parents and Guardians*, May 2009.

[54] See Office of the Victorian Privacy Commissioner Information Sheet 02.09, *Job Applications, Referee Checks and Privacy*, April 2009; Office of the Victorian Privacy Commissioner Information Sheet 03.09, *Handling Criminal Records in the Public Sector*, April 2009, both available at http://www.privacy.vic.gov.au. For further consideration of the difficulty of obtaining meaningful consent in the workplace, see the Victorian Law Reform Commission's report, *Workplace Privacy*, Final report, September 2005, paras 2.23-2.24, 2.31, 2.46, 3.2, 3.103, 3.114, 3.144, available at http://www.lawreform.vic.gov.au.

[55] *Complainant AU v Public Sector Agency* [2011] VPrivCmr 3.

[56] See, for example, Sections 464ZGC-464ZGF of the *Crimes Act 1958* (Vic), which expressly allow a volunteer to withdraw his or her consent to the taking or retention of a genetic tissue sample. The withdrawal of consent after the sample has already been taken is limited, however, in that police may apply for a court order to retain the sample and any related material and information (such as a DNA profile that can be compared against DNA profiles derived from tissue samples found at crime scenes).

[57] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Privacy Sector Provisions of the Privacy Act 1988*, page 85, March 2005, http://www.privacy.gov.au/law/reform/review.

[58] The National Privacy Principles in Schedule 3 of the *Privacy Act 1988* (Cth) contain at NPP 2.1(c) specific provisions to deal with use and disclosure of non-sensitive personal information for the secondary purpose of direct marketing.

[59] Explanatory note to Clause 11 in the Explanatory Memorandum to the *Information Privacy Bill 2000* (Vic).

[60] For instance, information collected for a financial or delicate purpose may indicate tighter security requirements.

[61] See, for instance, the Second Reading Speech introducing the Information Privacy Bill, where the then Minister for State and Regional Development said, "The protection afforded to privacy is a key aspect of the democratic balance between governments, business and individuals. Communities which compromise on privacy compromise on freedom. This creates an environment of mistrust and caution in which citizens are unwilling to volunteer information and the free flow of information is hindered." (Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000, John Brumby, Minister for State and Regional Development, 1905 at 1906.)

[62] Both the Victorian and Commonwealth electoral laws have been amended in recent years to prohibit the use of voters' information for commercial purposes. See Section 37, *Electoral Act 2002* (Vic) and Sections 91B and 189B, *Commonwealth Electoral Act 1918* (Cth).

[63] Providing false information is a privacy-protective method used by individuals to preserve their privacy on the internet (Wallis Consulting Group, *Community Attitudes Towards Privacy 2007*, commissioned by the Office of the Privacy Commissioner, Australia, June 2007, page 64, available at http://www.privacy.gov.au.)

[64] *Ng v Department of Education* [2005] VCAT 1054 at para 77.

[65] *Pelechowski v Registrar*, Court of Appeal (NSW) (1999) 198 CLR 435.

[66] *Silver and others v the United Kingdom*, European Court of Human Rights, 25 February 1983, para 97; *Handyside v the United Kingdom*, European Court of Human Rights, 4 November 1976, para 48.

[67] See Kirby J's comments at para 202, 205 and 247, *Mulholland v Australian Electoral Commission* [2004] HCA 41.

[68] For further elaboration on the proportionality test, *Mulholland v Australian Electoral Commission* [2004] HCA 41 see Gleeson CJ at paras 33-39, and Kirby J at paras 249-251.

[69] *Mulholland v Australian Electoral Commission* [2004] HCA 41 per Gleeson CJ at paras 39-40.

[70] *Charter of Human Rights and Responsibilities 2006* (Vic). See especially sections 7 (when human rights may be limited), 32 (interpreting laws in manner compatible with human rights) and 38 (obligations on public authorities to consider relevant human rights).

[71] See, for instance, *Jones v Bartlett* [2000] HCA 56 (Gleeson CJ at para 57-58).

[72] *Bankstown Foundry Pty Ltd v Braistina* [1986] HCA 20 (Mason, Wilson and Dawson JJ at para 12).

IPP 1: Collection

1.1 Collection is a fundamental part of the *Information Privacy Act* and goes to the heart of information privacy protection. It is essential that organisations get it right.

1.2 The first step should always be, "what information is necessary to carry out this function or activity?" with the corollaries, "can the purpose be achieved without collecting personal information?" and "can the information be anonymous or de-identified?"

1.3 The best privacy safeguard is to not collect personal information that is not needed. If an organisation unnecessarily collects personal information, it will then have to comply with all the other IPPs in relation to that information. The unnecessary collection may breach IPP 1.1, and later there may also be a risk of a breach of data security (or another IPP) for data which did not need to be collected and held in the first place. What an organisation does not have, it does not spend funds or resources on, nor make mistakes with.

1.4 The purpose of collection governs use and disclosure (IPP 2) which starts from the assumption that information is used or disclosed for the primary purpose it was collected. Collect wrongly, and the organisation may be inconvenienced or worse by not being able to use the information in the way it envisaged.

1.5 IPP 10, on collection of sensitive information, supplements IPP 1, and the two are best considered together. IPP 10 is intended to provide safeguards additional to IPP 1 by limiting the circumstances in which sensitive information is collected.[73] IPP 10 is discussed in more detail later in these Guidelines.

1.6 In general, where an organisation has possession or control of personal information, it has collected it and the IPPs must be complied with.

1.7 Section 4(1) of the *Information Privacy Act* states that an organisation holds personal information if the information is in the possession or under the control of the organisation, whether alone or jointly with other persons or bodies, irrespective of whether the document is situated in or outside of Victoria.

1.8 Broadly put, the basic standards are:[74]

a Collect only what is needed.

b Do it lawfully, fairly, directly and not unreasonably intrusively.

c Tell people it is being collected and why.

IPP 1

Information collected prior to 1 September 2001

1.9 The collection principles (IPP 1 and 10) do not apply to information already collected by organisations prior to the *Information Privacy Act* coming into force (1 September 2001).[75] In contrast, the other IPPs do apply to information already held at that date.[76]

1.10 For example, in *Complainant AB v Victoria Police* [2006] VPrivCmr 3, it was recognised that IPP 1 was not breached by police in failing to give notice to firearm licence applicants of the usual uses and disclosures of fingerprint information, as the fingerprints had been taken in 1995. (Police undertook, however, to review the information provided to firearm licence applicants to ensure that the ongoing use of fingerprint data is clearly explained.) Notwithstanding that the year of collection pre-dated the *Information Privacy Act*, the use/disclosure being made of the data was subject to the *Information Privacy Act* (and in this case was found to be within IPP 2).

1.11 The Privacy Commissioner similarly did not have jurisdiction over a collection practice in *Complainant A v Local Council* [2003] VPrivCmr 1, which involved the collection prior to the commencement of the *Information Privacy Act* of an individual's banking information.

1.12 When the Act was introduced, it was recognised that organisations were not able to retrospectively collect information in accordance with IPPs 1 and 10, but organisations were expected to deal with all information they hold (no matter when it was collected) in accordance with the remaining IPPs.[77]

Unsolicited personal information

1.13 Victorian public sector organisations do not always request, seek or actively gather the personal information they hold. An organisation may have a general function to receive information that is not specifically solicited, such as a regulator whose function it is to receive inquiries or complaints, or ministers whose function it is (often delegated to departments) to respond to letters from members of the community raising issues about the laws within their portfolios. Or an organisation may ask for particular types of personal information, but be provided with far more than was sought.

1.14 Unsolicited personal information has been included in:

a petitions sent to Parliament or to Councils (eg, *Complainant H v Local Council* [2004] VPrivCmr 2);

b letters of complaint or expressions of concern about the conduct of persons or bodies (eg, *Complainant J v Statutory Entity* [2004] VPrivCmr 4, *Complainant AF v Local Council* [2007] VPrivCmr 1);

c email inquiries or requests for information (eg, *Golden v Ministry of Economic Development* [2005] NZHRRT 13[78]); and

d resumes submitted otherwise than in response to a job advertisement or other such invitation (see *Job applicant alleges that department contacted former employer – (Case Note 19740)* [2002] NZPrivCmr 5[79]).

1.15 The IPPs will apply to personal information, whether solicited or not. Victoria does not expressly exclude unsolicited information from the meaning of collection (as the NSW and New Zealand privacy laws do),[80] nor does the *Information Privacy Act* limit the application of the collection principle to solicited information (as do the Commonwealth and Tasmanian privacy laws).[81]

1.16 Unsolicited personal information may contain the personal information of the provider, or even the personal information of third parties. The supply of information may be completely unsolicited and be quite unnecessary to the organisation's functions and activities.

1.17 Usually, organisations cannot destroy the information or send back the original and keep no copy, as a private sector organisation might well do, because most Victorian public sector organisations are subject to the *Public Records Act 1973* (Vic), which requires that records be handled and disposed of in prescribed ways for archives purposes.[82] To the extent that the *Public Records Act* compels retention of unsolicited personal information unnecessary for an organisation's functions and IPP 1 forbids collection of such information, the two laws are inconsistent and the *Public Records Act* prevails.

1.18 The receipt of unsolicited information may trigger the notice requirements in IPPs 1.3 and 1.5, even though the organisation may not intend to use the information about the sender or any third party referred to in the unsolicited communication. However, in some cases, it may be reasonable not to give notice – see the section on "reasonable steps for giving notice" at paras 1:94-1:96. In *Little v Melbourne City Council (General)* [2006] VCAT 2190, the Tribunal found that Council was not required to give notice under IPP 1.3 relating to an unsolicited letter sent by the Complainant to Council.

IPP 1.1: Necessary for one or more functions or activities

1.19 IPP 1.1 prohibits organisations from collecting personal information unless the information is necessary for one or more of the organisation's functions or activities.

1.20 Accordingly, an organisation should be quite clear about the need and the function/activity. Both elements are required.

Necessity

1.21 Necessity is assessed in a practical way. Does the organisation need the personal information in order to discharge the function effectively? Consider whether anonymous information would be sufficient. Can the function be discharged through anonymous transactions? If so, forms and practices should be adapted to avoid excess collection.

1.22 See, for instance, OVPC's Information Sheets discussing whether it is necessary to collect identifying information:

a *Personal Information in Complaint Handling*, Information Sheet 03.05, 1 September 2005;

b *Objectors, Submitters and Privacy*, Information Sheet 01.05, 7 July 2005;

c *Confirming Identity and Privacy: A Guide for Organisations*, Information Sheet 07.08, December 2008; and

d *Job Applications, Referee Checks and Privacy*, Information Sheet 02.09, April 2009.

1.23 Also see the Information Sheet 03.09, *Handling Criminal Records in the Public Sector,* for guidance on ensuring criminal record checks are only done when necessary and relevant.

1.24 This principle is aimed at ensuring that organisations only collect information that is necessary for their purposes and not excessive.

1.25 It is important that the reason the organisation "needs" the information (that is, the purpose for collection) be closely tied to the organisation's function or activities. The collection should be for a specific purpose and the type and extent of information collected should be limited to what is necessary to achieve that purpose (that is, carry out that activity or function).

1.26 In *Ng v Department of Education* [2005] VCAT 1054, the Department installed CCTV cameras in a computer classroom to minimise vandalism and monitor student use of the computers. VCAT considered whether CCTV monitoring of a classroom was necessary for the Department's function. While noting that it could be argued that the education system in Victoria operated for more than a century without the need for video surveillance, VCAT took a "more relaxed meaning of necessity" and suggested the test:

> ...is the collection in question here reasonably required or legally ancillary to the accomplishment of the Department's functions?[83]

1.27 VCAT found that the operation of CCTV was reasonably required and ancillary to the Department's function in operating a school system in monitoring the computer rooms. Because the CCTV system could be turned on and off, rather than record constantly, VCAT accepted that the system was "reasonably adapted to the attainment of the Department's functions in providing education in computer subjects" and accordingly there was no breach of IPP 1.1.[84]

1.28 IPP 1.1 acts to limit the collection of unnecessary information, and this includes information about individuals who are of no concern to the organisation. For example, in *Complainant X v Contracted Service Provider to a Department* [2005] VPrivCmr 6, a contractor was engaged to conduct surveillance for use in assessing a compensation claim. However, the contractor surveilled the wrong person and accordingly the Privacy Commissioner concluded that the information about that wrong target was not necessary for one or more of the organisation's functions.

Employment

1.29 Collecting unnecessary information is common when assessing an individual's suitability for employment. For example, in *Man objects to pre-employment screening (Case Note 218236)* [2011] NZPrivCmr 4, the New Zealand Privacy Commissioner considered that collecting information about a person's personal credit history when that person applied for employment and before they had accepted a position was not a necessary collection, as the position was not one in which there was a significant financial risk to the organisation. The OVPC Information Sheet 02.09, *Job Applications, Referee Checks and Privacy*, April 2009, discusses in more detail the ways in which an organisation can ensure it only collects information necessary for assessing suitability for employment.

Incidental collection

1.30 In some cases, organisations may collect incidental information about a person or a third party that may not be strictly necessary to carry out its functions or activities. In *Complainant AE v Contracted Service Provider to a Statutory Authority* [2006] VPrivCmr 6, for example, surveillance was carried out on the Complainant's wife in relation to her claim for compensation due to an injury. The surveillance also captured information about the complainant, who argued that his information was not necessary for the contracted service provider's function of assisting the statutory authority to assess the merits of his wife's claim. The Privacy Commissioner accepted that surveillance may, when carried out lawfully and appropriately, inevitably capture information about someone other than the person who is the subject of the surveillance. In some cases, information about the third party may be relevant information about the person surveilled (such as where a third party driving a car is indicative of the fact that the subject of the surveillance was not driving). The Privacy Commissioner suggested the following test to assist in determining when collecting incidental information about third parties during surveillance might be regarded as inappropriate:

> The test the Privacy Commissioner applied when assessing whether the information collected about the complainant is relevant information was whether a reasonable person would find sufficient connection between the subject of surveillance and the other party, the complainant.

1.31 For a further discussion of the meaning of "necessary", see paras KC:81-KC:87.

Function or activity

1.32 In state and local government, functions and activities often have a basis in law. An organisation's functions or activities may be specifically listed in the statute that established the organisation. The functions or activities may be broadly expressed in statute, but more refined in regulation, ministerial directive or other sources. An organisation should check these sources so that it has a clear understanding of the organisation's functions and activities – sometimes over time organisations can lose sight of the legal basis underpinning their functions.

1.33 Organisations should be as clear and specific as possible about the function or activity that the information is needed for.

IPP 1.2: Lawful, fair, not unreasonably intrusive

1.34 IPP 1.2 requires that collection must be by lawful and fair means and not in an unreasonably intrusive way.

Lawful

1.35 Collection must be according to law and not contrary to law. This includes criminal and civil law, statute and common law.

1.36 The *Information Privacy Act* will not permit collection of information where that collection is prohibited by another law. This includes statutory restrictions against collecting particular information (eg, DNA profiles from bodily samples collected during roadside drug testing)[85] or collecting information in particular circumstances (eg, monitoring of private conversations or activities without consent or a warrant).[86]

1.37 IPP 1.2 may also be breached where an organisation lacks power or authority under law to collect personal information or exceeds its power.

Fair

1.38 The concept of fairness has been examined by courts in the context of exercising their discretion to exclude unfairly collected evidence. The High Court of Australia has suggested the term should be viewed in context and in accordance with community values:

> The term "unfairness" necessarily lacks precision; it involves an evaluation of circumstances... [F]airness is a concept broad enough to adapt to changing circumstances as well as evolving community values.[87]

1.39 Information may be regarded as having been obtained unfairly where it was collected by trickery, deception or under duress. The High Court has also suggested that information may be seen as unfairly obtained where it was collected in circumstances in which the individual would not have ordinarily given up their information had proper procedures been followed.[88]

1.40 A government agency may not be collecting fairly if, for instance, it knowingly accepts personal information from persons whom the agency knows are under the mistaken belief they must compulsorily provide it. Individuals may be required by law to provide certain information to obtain some benefit or entitlement, or to exercise some right or privilege – for example, to obtain a licence for a profession, or to volunteer in child-related areas of work. The legislation may set out the type of information which must be provided and, in some cases, may make it a criminal offence to provide false or misleading information. In such contexts, agencies that collect more than necessary and compulsorily should consider carefully whether they are collecting unfairly.

1.41 In drafting forms, organisations should take care to distinguish compulsory information (required by law to be provided) from other information which is not compulsory to be provided but which the organisation regards as necessary. Organisations should remember that information can be provided by consent, but they should indicate to individuals when provision of information is optional.[89]

1.42 The term "computer says no" is shorthand for situations in which computers are pre-programmed to deny the person using the computer the ability to proceed until the person provides the information for certain specified fields on the screen. When designing forms for electronic transactions, organisations should avoid a "computer says no" situation by ensuring that the program does not require fields to be completed with unnecessary personal information before the transaction can progress or be finalised (see Case Study 1-1).

CASE STUDY 1-1: Computer system set up to require unnecessary information before processing application[90]

This case involved a complaint to the Federal Privacy Commissioner by a woman who had attempted to open a deposit account with a Banking Institution. The complainant was required to complete an application and objected to providing information about her marital status, as she believed this information to be unnecessary for opening the account. The Banking Institution informed the complainant that their computer system did not allow applications for deposit accounts to be opened without completing the field for "marital status".

After the complainant wrote to the Bank, the Bank said it would change its system, although it would take some time. In the meantime, they would record her status as "single" and note that this may not reflect actual marital status. The complainant was dissatisfied with the bank's response, and wrote to the Federal Privacy Commissioner.

The Bank acknowledged that it was not necessary to collect marital status information as the complainant's marital status had no bearing on her eligibility to open an account. In consultation with the Federal Privacy Commissioner, the Banking Institution undertook to change its computer system so that applicants would no longer be required to disclose their marital status. The Bank agreed to provide the Federal Privacy Commissioner with quarterly reports on the progress of its implementation program.

1.43 It may also be an unfair collection if an organisation misrepresents what will be done with the information once collected, such as claiming the information will be treated securely and confidentially when it is intended or proposed that the information be passed on to others (see Case Study 1-2).

CASE STUDY 1-2: Failure to disclose use[91]

A company, prior to a meeting with one of its employees, had promised complete confidentiality. The organisation later disclosed the employee's personal information (opinion) to others within the organisation, leading to the employee's dismissal. The employee had been promised confidentiality and had not been informed of the use to which the information supplied would be put or the subsequent disclosures.

The New Zealand Privacy Commissioner found a breach of Principle 3 of the *Privacy Act 1993*, which is similar to IPP 1. The New Zealand Privacy Commissioner stated that an important element in the assessment of "unfairness" is whether a complainant would have responded differently had he or she known that the information would be disclosed.

1.44 Similarly, it may be unfair if an organisation initiates monitoring or collection of information for one purpose, giving assurances or undertakings that the information will not be used for any (or certain specified) purposes, and then make such a use/disclosure, especially where:

a individuals might have objected to the collection had they known its eventual use;

b less intrusive alternatives were available but had not been considered; or

c additional safeguards would have been sought in respect of the secondary use.

1.45 For instance, installing CCTV to protect an organisation's property from theft or vandalism while undertaking not to use the technology to surveil workers in the workplace may later be held to have been an unfair collection if the CCTV footage is subsequently used to monitor employee performance or in disciplinary proceedings, and:

a employees (individually or collectively) might have objected to the appropriateness of using surveillance to monitor their performance, had they known the undertaking would not be kept;

b other less intrusive means for monitoring workers' performance were available but had not been considered; or

c additional safeguards would have been sought to protect workers' interests, such as giving notice before the footage is used to take adverse actions against an employee.

1.46 In *Ng v Department of Education*, VCAT found that there was no breach of IPP 1.2 as there was no apparent unlawfulness and because Ng was aware that surveillance was underway and later impliedly consented to its use for assessing her performance in the classroom. VCAT did not appear to address the question of fairness at the time of collection. Had it done so, factors relevant to an assessment of fairness may have included:

a departmental guidelines (although not binding), which expressly forbade the use of CCTV use for monitoring individual work performance; and

b public notices and staff briefings which gave the impression that the CCTV would only be used to detect vandalism and graffiti and not for purposes related to teachers' employment.

1.47 Implied consent to a later use of the CCTV footage to assess performance does not affect whether the footage was collected fairly in the first place.

1.48 It is vital to ensure that collection notices (IPP 1.3) and privacy polices reflect the organisation's intention when it collects information (see IPP 5).

1.49 Collecting information or monitoring individuals without notice and without their consent or knowledge, as in the case of covert surveillance, will be regarded as unfair in most circumstances. There are some situations in which the use of covert surveillance may be justified and not considered unfair, depending on how it is conducted. Examples of such instances of covert surveillance include where it is:

a expressly authorised under law by a decision maker required to take privacy interests into account, such as where a judge grants a covert warrant; or

b carried out with prior notice that covert surveillance may be used for limited and specified purposes, such as might permit an employer to investigate suspected unlawful activity or misconduct of a serious kind, or allow an insurer to investigate a suspected fraudulent compensation claim.

1.50 Additional safeguards are generally required to ensure that less intrusive options are considered, that there is an identified legitimate need justifying the use of this intrusive option, that the surveillance is limited in scope and duration, that the privacy interests of any person (including third parties) are taken into account, and appropriate oversight and accountability mechanisms are in place to deter and detect any misuse.

1.51 In practice, third parties may be affected by surveillance conducted on those with whom they live or work. Where the third party believes his or her privacy has been invaded, it will usually be appropriate to examine all the circumstances of the case and to ask, "Would a reasonable person find sufficient connection between the third party's information and the purpose underpinning the surveillance (eg, investigation of fraud) to assess properly the claim by the person who is the primary target of the surveillance?" If the answer is no, then the collection of the personal information of the third party may be unfair to that third party, allowing always for the likelihood that there will be collections of personal information of third parties that are merely incidental.[92]

1.52 Consideration should also be given to the degree, if any, to which other rights are affected by the collection practice, as Victorian public authorities are required to do under the relevant sections of the *Charter of Human Rights and Responsibilities Act 2006* (Vic).[93] For instance, although covertly obtained information may be permitted in some cases, the line between what is permissible and what is not may be crossed where other rights are unduly infringed.

1.53 For example, the crossing of this line in the use of covert and other tactics by police was discussed by Kirby J in the High Court case of *R v Swaffield; Pavic v The Queen*:

> Subterfuge, ruses and tricks may be lawfully employed by police, acting in the public interest. There is nothing improper in these tactics where they are lawfully deployed in the endeavour to investigate crime so as to bring the guilty to justice. Nor is there anything wrong in the use of technology, such as telephonic interception and listening devices although this will commonly require statutory authority. Such facilities must be employed by any modern police service. The critical question is not whether the accused has been tricked and secretly recorded. It is not even whether the trick has resulted in self-incrimination, electronically preserved to do great damage to the accused at the trial. It is whether the trick may be thought to involve such unfairness to the accused or otherwise to be so contrary to public policy that a court should exercise its discretion to exclude the evidence notwithstanding its high probative value. In the case of covertly obtained confessions, the line of forbidden conduct will be crossed if the confession may be said to have been elicited by police (or by a person acting as an agent of the police) in unfair derogation of the suspect's right to exercise a free choice to speak or to be silent. Or it will be crossed where police have exploited any special characteristics of the relationship between the suspect and their agent so as to extract a statement which would not otherwise have been made.[94]

Not unreasonably intrusive

1.54 In practice, it will often be the case that there are only fine distinctions to be made between a collection that is unnecessary (IPP 1.1) and a collection done in an unreasonably intrusive way (IPP 1.2).

1.55 To illustrate this point, a collection may be unreasonably intrusive where excessive or unnecessarily intimate information is collected, or where the collection occurs in a manner that unnecessarily intrudes into a person's home life or unreasonably interferes with a person's bodily integrity. Much will depend on the context and the need that is said to underpin the collection.

1.56 Collecting information in "ways not unreasonably intrusive" has to be assessed in all the circumstances. Asking an employer or neighbour or family member for information when the organisation could go directly to the person concerned may also be unreasonably intrusive, depending on the nature of the information and the circumstances of the relevant relationship. If collection occurs via a third party, IPP 1.4 and IPP 1.5 are relevant.

1.57 For example, confirming a person's identity can be achieved in differing ways. What might be unreasonably intrusive in one context may not be in another. Requiring an iris scan from individuals who visit a secure facility for the criminally insane may not be regarded as overly intrusive when done to ensure the wrong person is not mistakenly allowed to leave. Such a practice may be unreasonably intrusive if used to attend another facility, such as a library or public hospital.

1.58 Collecting information too soon, from too many people, may also be unreasonably intrusive. For instance, asking all job applicants to undergo criminal record checks or medical examinations may be overly intrusive when it is reasonable to limit the request to a preferred candidate. For further guidance, see OVPC's Information Sheet 03.09, *Handling Criminal Records in the Public Sector.*

1.59 The phrase "unreasonably intrusive way" in IPP 1.2 focuses the mind on the method used to collect information, and the necessity test in IPP 1.1 focuses minds on the type and on the amount of information collected.

1.60 In whatever way personal information is collected, the source and method should be able to be justified and explained.

IPP 1.3: Collection notices

1.61 IPP 1.3 requires organisations to take reasonable steps[95] to make individuals aware of the following matters:

a the identity of the organisation and how to contact it;

b the fact that he or she may access that information;

c the purposes for which the information is or was collected;

d the names (or types) of organisations or individuals to whom the information is usually disclosed;

e any law requiring the collection; and

f the main consequences (if any) if the person does not provide any or part of the information sought.

These factors are explained in OVPC's Information Sheet 02.11, *Collection Notices*, March 2011.

1.62 Giving notice is essential for promoting transparency about an organisation's collection and handling of personal information, and for ensuring individuals are aware of their rights and obligations in respect to giving up (and later accessing) their information.

1.63 Prior notice gives individuals the opportunity to consider whether they will proceed with their interaction with government, knowing what information is to be collected and how it is to be used. For example, prior notice that successful job applicants will be required to undergo a criminal record check should be given at the time applications are initially sought. (See OVPC's Information Sheet 03.09, *Handling Criminal Records in the Public Sector,* April 2009.)

Timing for giving notice

1.64 Notice of the matters listed in IPP 1.3 must preferably be given before or at the time of collection. If that is not practicable, notice can be given as soon as practicable after the information is collected.

1.65 The notification details do not necessarily have to be explained every time particular personal information is collected, nor explained at the same level of detail. Some matters, such as the identity of the organisation, may be obvious from the context. Sometimes, the organisation will have already taken steps to notify an individual when the same or similar information was collected on a previous occasion.

1.66 In other cases, it may be impossible to give prior notice, such as where emergency services are being delivered. Where prior notice is not practicable, organisations should nevertheless take reasonable steps to give notice after the time of collection. (See the earlier discussion relating to "practicable" at paras KC:91-KC:93 and the discussion about taking reasonable steps to give notice at paras 1:94-1:96.)

Form of notice

1.67 The notification requirements can be achieved in a variety of ways. Notification can be prepared in advance (paper, online, telephone scripts) and staff should be trained to ensure familiarity with their obligations under the *Information Privacy Act*. Privacy notices on forms and websites will assist. Sometimes a simple explanation at the time of collection will be sufficient.

1.68 Further examples of types of notice are detailed in OVPC's Information Sheet 02.11, *Collection Notices*, March 2011.

Multi-layered (or "short") notices

1.69 Information can be provided in layers, from full explanation to brief refresher as individuals become more familiar with how the organisation operates and what it does with their personal information. Brief privacy notices on forms or signs could be supplemented by longer notices made available online or in brochures.

1.70 In some cases, such as where CCTV surveillance is conducted, it may be sufficient to post brief information on a sign, such as the identity and address of the organisation conducting the surveillance, a brief reference to why surveillance is underway, and a website where individuals can find more complete details about IPP 1.3 matters. Organisations should ensure that individuals are able to locate and understand the prescribed notification details easily.

1.71 More information on multi-layered notices can be found in OVPC's Information Sheet 02.11, *Collection Notices*, March 2011.[96]

Distinguishing notice statements from privacy policies

1.72 An organisation's privacy policy (which must be available to all who ask for it – IPP 5) will often be useful but may not be comprehensive enough to adequately inform individuals of the prescribed matters in IPP 1.3. Notice statements under IPP 1.3 address a specific collection practice (such as assessing an application for employment, or collecting personal information on a council planning application form) compared to privacy policies under IPP 5, which address all of the organisation's information collection and handling practices (not limited to collection and use). For further guidance on distinguishing collection statements from privacy policies, see OVPC Information Sheet 02.11, *Collection Notices* and Information Sheet 01.11, *Drafting and Reviewing a Privacy Policy*, March 2011.

IPP 1.3(c): Purposes of collection

1.73 IPP 1.3(c) requires organisations to inform individuals of the purposes for which information is collected.

1.74 The primary purpose will be what is strictly necessary to discharge the function or undertake the activity. The primary purpose needs to be clearly stated and must be more specific than a general reference to some broad power. Primary purpose needs to be more specific than, for example, "administering revenue laws" or "licensing" or "oversight of planning" or "peace and good order". A narrower primary purpose does not prevent the organisation from using or disclosing the information appropriately for related secondary purposes. Sometimes there may be several purposes; for example, several purposes may be laid out in statute. Each of these may be regarded as a primary purpose for the purposes of applying IPP 1.

1.75 Where there has been a long-standing practice of collecting information (especially one that pre-dates the introduction of privacy laws), it may be difficult to work out what the primary purpose is, or that purpose may have changed over the years. This is often the case with public registers. If it is difficult to be specific, an organisation should consider whether it is necessary to collect the information at all (IPP 1.1). For further guidance about ascertaining the purpose of public registers, see OVPC's publication, *Public Registers and Privacy – Guidance for the Public Sector*, August 2004, pages 1-12 and, for other issues relating to the giving of notice, see pages 12-19.

1.76 If secondary purposes are known in advance, they too should be explained to the subject. See the earlier discussion (at paras KC:72-KC:80) relating to "purpose" and "function creep".

IPP 1.3(d): Usual recipients of the information

1.77 IPP 1.3(d) requires the organisation to ensure individuals are aware of the individual or organisation, or the types of individuals or organisations, to whom the information is usually disclosed. The effect of this principle is to ensure individuals are made aware of where their data is likely to flow.

1.78 This principle allows organisations to either list the individuals or organisations by name, or by type. For example, a notice might state that information is usually disclosed to the "State Revenue Office and Australian Taxation Office" or the "Victorian Electoral Commission and Australian Electoral Commission", or the notice might say information is disclosed to "state and federal taxation authorities" or "state and federal electoral commissions".

1.79 Where the information is usually shared for specific purposes, the notice should also refer to these. For example, the notice might say information is usually disclosed to "state and federal electoral commissions for the purpose of updating the joint electoral roll".

1.80 When an organisation collects personal information with the intention of publishing it or disseminating it (eg, online), it should make this intention clear at the time of collection. Online publication is effectively disclosure to the world, potentially with few limitations or controls over possible uses.

CASE STUDY 1-3: Online publication of submission to council without prior notice[97]

A Local Council called for submissions relating to an amendment to a local law. Any person affected by the amendment was able to make a submission pursuant to s 223 of the *Local Government Act 1984* (Vic). The complainant submitted a letter regarding the local law to the Council, which contained the complainant's name and address, as well as general comments regarding his neighbours, who were also identifiable.

The Local Council held a Special Council Meeting at which it considered the submissions it received relating to the local law. The complainant's letter was considered as part of this process. At some point after the meeting, the Council published the minutes of the meeting on its website, attaching all of the submissions to the minutes, including the complainant's. This meant that the complainant's name and address were now publicly available and could be found by using a search engine.

The complainant complained to the Local Council, requesting that his letter be removed from the minutes. The Local Council responded stating that the minutes of meeting were required to be made available to the public as a matter of course. In addition, Council stated that s 223 submissions were required to be made available for public inspection in accordance with the procedures specified in the Act. The Local Council felt that it had acted appropriately and therefore would not remove the complainant's letter from its website.

The Privacy Commissioner considered the notice that was given to the complainant at the time of collection. In particular, it was important to take reasonable steps to ensure that an individual knows the purpose for which information is collected and to whom and how it is usually disclosed, particularly if information is intended to be disclosed to the world at large (ie, online). While the notice given to the complainant stated that submissions would be considered at a Special Council Meeting, the notice did not state that such submissions would subsequently be published on the Council's website.

The complaint was resolved at conciliation with the Council agreeing to amend its collection statement and privacy policy.

1.81 Where lawful and practicable, consider offering individuals an opportunity to restrict the publication of their details, such as where they are concerned that disclosure may pose a risk to their personal safety. Some laws expressly offer this option to restrict publication or disclosure.[98] An organisation may have a discretion in other cases.

CASE STUDY 1-4: Online publication of delicate information without prior notice[99]

The complainant held a licence in relation to a sensitive trade activity under a statutory scheme. When she registered with the Statutory Entity who administered the scheme, she was unaware that her name would be included on the register that subsequently became available on the internet. Online Google searches led to results that associated her name with another related and more sensitive trade activity, also regulated by the Statutory Entity. She felt humiliated about being wrongly identified with the more sensitive trade and was concerned about the risk of harm that may result from being identified and then located.

The Statutory Entity removed the register from the internet and later worked with Google and with an internet archive to remove any cached copies of the information that were still accessible to searchers.

IPP 1.3(e): Compulsory collection

1.82 Where an organisation has the power to obtain information compulsorily, that power should be made clear to the person. The notice statement should specify which law is being invoked as a basis for collection. This makes the organisation's legal authority transparent and allows individuals to check the scope of that authority. It also serves as a check for the organisation that the collection is lawful and not excessive or intrusive (IPPs 1.1 and 1.2) and that the collection is authorised despite any inconsistent obligation under the IPPs or *Information Privacy Act* (s 6). (See the earlier discussion about unreasonably intrusive collection at paras 1:54-1:60.)

1.83 If the information is required under law for one purpose but not for other purposes, the distinction should be made clear.

Optional information

1.84 Where the person has an option not to provide certain details (such as email address, phone number, age or even name), that should be made clear. Such information may still be regarded as necessary to an organisation in that it assists it in effectively and efficiently carrying out its functions or activities. However, there may be instances where an individual does not wish to participate or take advantage of all of the organisation's activities and so may prefer to withhold certain information.

1.85 Organisations are reminded that they should not seek information (even by consent) that is unnecessary to their functions or activities, or that is unduly intrusive or unfair. An organisation cannot rely on an individual's consent to sanction a breach of IPPs 1.1 or 1.2.

IPP 1.3(f): Consequences for individuals who do not provide their information

1.86 IPP 1.3(f) requires organisations to give notice of the main consequences (if any) for the individual if they do not provide all or part of the information being collected.

1.87 Organisations should be careful not to overstate the consequences for individuals who do not provide all or part of the requested information. For instance, there may be a legal obligation to provide certain information in order to engage in a profession or activity, or to qualify for a benefit or service. But some individuals may not be required to provide all or any of the information in certain circumstances.

IPP 1.4: Direct collection

1.88 IPP 1.4 requires organisations to obtain information about an individual only from the individual, where it is lawful and practicable to do so.

1.89 This preference for direct collection enables individuals to have some measure of control over what is collected, by whom and for what purposes. It provides individuals with an opportunity to refuse to participate in the collection, or to provide their information on conditions or with reassurances about how it is to be used. Direct collection also makes it more likely that the information organisations collect will be relevant, accurate and complete (IPP 3), as firsthand information is less likely to suffer from the data quality problems usually associated with second-hand information.

1.90 Nevertheless, there will be many circumstances where it would not be practicable to collect information directly from the individual. This may occur, for instance, where an individual discloses information about their family circumstances when applying for financial assistance or welfare benefits.

1.91 As a result of indirect collection, organisations may end up collecting a considerable amount of information about individuals without those individuals' knowledge. In many circumstances, particularly where the information can be used to affect their interests, these individuals may want to know that their information has been collected, that they can find out what is known about them, and that they can be informed about where their information will flow. That is what IPP 1.5 requires.

IPP 1.5: Notice of indirect collection

1.92 IPP 1.5 requires organisations to take reasonable steps to make an individual aware of the matters in IPP 1.3 if they collect personal information from someone else, unless doing so would pose a serious risk to the life or health of any individual.

1.93 There will be times when an organisation collects information about an individual from another individual, organisation or source. As with IPP 1.3, this principle promotes transparency about who is collecting individuals' information and why, and ensures they are aware of their rights of access and obligations in relation to compulsory acquisition of their data.

"Reasonable steps" for giving notice

1.94 In assessing whether it is practicable to give an individual (including senders of unsolicited communications) notice as required by IPP 1.3, or what reasonable steps should be taken under IPP 1.5 to make identifiable individuals (who may be the subject of unsolicited personal information sent by another person) aware of the matters in IPP 1.3, factors to consider include:

a whether the organisation intends to respond to the sender (or third party) in any event, for example, to acknowledge receipt of the letter;

b whether notice is likely to have already been received by the sender, for instance in previous correspondence or where the sender appears to be responding to information the organisation had made available and that information already contains a notice statement;

c whether the information will be indexed in a way that allows retrieval by reference to an individual who was not the sender (eg, persons named in an unsolicited letter);

d the number of people likely to have access to the information;

e whether and how the organisation is likely to use or disclose the information (as distinct from simply acknowledging receipt, filing and storing it in compliance with the *Public Records Act 1973* (Vic));

f the likely effect on the individual, in particular any adverse effect, of any future use or disclosure of the information;

g the nature of the particular information;

h the effect on the privacy of any other individual; and

i the degree of difficulty in making contact with relevant individuals and making them aware, having regard to consideration of the above factors, to all the circumstances and to the objects of the *Information Privacy Act*.

1.95 Having followed the above steps, the organisation may decide that, for the time being, it is not necessary or practicable to give (further) notice, or it is not reasonable to take steps to give notice. Further efforts to give notice under IPP 1.3 or 1.5 should be taken if at any time the organisation proposes to use, disclose, transfer, give access to, correct, update or complete the unsolicited personal information.

1.96 All the other IPPs would of course continue to apply.

Automated collection, monitoring and surveillance

1.97 The *Information Privacy Act* applies to personal information, whether collected by manual or by automated means. Automated collection of personal information may occur through the use of technologies such as anti-virus software,[100] video surveillance,[101] use of "cookies",[102] or email technologies.[103]

1.98 Automated collection and monitoring may result in organisations collecting vast amounts of data, some of which may be sensitive information (as defined in the *Information Privacy Act*) and some of which may not relate to the organisation's functions or activities (such as personal emails or documents) – see Case Study 1-5.

CASE STUDY 1-5: Unnecessary collection of information through use of anti-virus software[104]

The complainant was a member of a Local Library and regularly used the Library's computer facilities. On one occasion, he inserted his floppy disk into the Library's computer to utilise the word processing facilities and noticed the library's virus-scanning software ran a check on the files on his disk. A dialogue box then presented him with an alert to the effect that his files had been copied and "cured".

Being concerned that the library was copying and retaining a copy of the personal information contained in his files, the complainant contacted the library to ask whether their anti-virus software could clean files without copying them. The next time he used the library's facilities, he was presented with a different alert that advised simply that the file was cured.

After a complaint was lodged, the Library advised the Privacy Commissioner that the anti-virus software copied files to a temporary drive (on the library's network) to prevent any loss of data during the curing process. Copies were accessible only by staff administrators and only until the end of the day, as any copied files were automatically deleted when the computers were shut down.

The Library also reported that its investigations revealed that copies of files could be made at the original location (in this case, on the complainant's floppy disk) so that no personal information was collected or held on the library's computer system.

The Library changed its system and assured the complainant that no copies of files or documents would be made other than at the original location; the software would replace an infected file with a cured file; and if unable to cure a file, the file would remain on the disk but the system would not allow it to be opened, and a message would advise the user of this fact.

1.99 When automated systems are being set up or operated, organisations should take steps to ensure that:

a the collection or monitoring fulfils a legitimate purpose that relates to the organisation's functions or activities – this may include using automated technologies to secure an organisation's equipment from damage (eg, from viruses);

b the personal information collected is kept to the minimum necessary to achieve that purpose and proportionate to the apprehended "risk" – avoid, for instance, universal and continuous monitoring where that is unnecessary;

c the least intrusive method of collection or monitoring is adopted – for instance, avoid accessing the content of email or other documents where this is not necessary; limit any collection of unrelated personal information or sensitive information where possible and, where this is not possible, put safeguards in place to ensure inadvertently collected information is not used or disclosed; and

d the information collection and handling practices are made transparent and documented, with proper notice given to individuals about who is responsible for the collection or monitoring, the purposes for which the information is used or disclosed (including anticipated secondary uses or disclosures – refer to the earlier discussion of "Function creep" at paras KC:77-KC:80), and the fact that individuals may seek access to their information. In many cases, it may be preferable to seek an individual's consent or authorisation prior to monitoring or automatically collecting their information.

1.100 For further guidance on how to comply with the *Information Privacy Act* when using automated technologies, such as email and virus filtering tools, see the "Lessons Learned" section of OVPC's June 2006 audit report, *Deakin University – Electronic Mail Policies*, Privacy audit 02.06. The Privacy Commissioner has also released Information Sheet 04.10, *Privacy in the Workplace*, which will be relevant for organisations implementing monitoring in the workplace.

1.101 Organisations are reminded that they may have other legal obligations relevant to their use of automated technologies for monitoring and collection of personal information, including laws relating to:

a the monitoring of telecommunications and stored communications (such as email) under the *Telecommunications (Interception) Act 1978* (Cth);

b the monitoring or recording in relation to the input or output of information from a computer under the *Surveillance Devices Act 1999* (Vic);

c the conduct of video and audio surveillance, as well as the use of tracking technologies (such as GPS)[105] under the *Surveillance Devices Act 1999* (Vic); and

d the unauthorised access to, and impairment or modification of, computer functions and electronic communications (and other related computer offences) under the *Crimes Act 1958* (Vic).

IPP 1 Notes

[73] Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000 (John Brumby, Minister for State and Regional Development), page 1907 – Second Reading Speech for the *Information Privacy Bill*. Also see the Explanatory Memorandum for the *Information Privacy Bill*, clause note for Principle 10.

[74] The full text of the IPPs are contained in the Appendix at the end of these Guidelines.

[75] Section 15(1), *Information Privacy Act 2000* (Vic).

[76] Section 15(2), *Information Privacy Act 2000* (Vic). Note the Federal *Privacy Act 1988* differs in this regard, in that it imposes fewer obligations on private sector organisations when dealing with information already held prior to 21 December 2001 (when the private sector privacy provisions commenced) – see ss 16C and 16D of the *Privacy Act 1988* (Cth).

[77] Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000 (John Brumby, Minister for State and Regional Development), page 1909 – Second Reading Speech for the Information Privacy Bill. Also see the Explanatory Memorandum for the *Information Privacy Bill*, note to clause 15.

[78] The case related to an email to the Ministry of Economic Development asking for the names of the board members and the chair of the Accounting Standards Review Board. The Ministry's email reply (including the original email inquiry) was copied to the Institute of Chartered Accountants of New Zealand.

[79] The New Zealand Privacy Commissioner found that the receipt of a job application and curriculum vitae in response to the Department's job advertisement did not constitute "unsolicited material".

[80] Section 4(5), *Privacy and Personal Information Protection Act 1998* (NSW); and Section 2, *Privacy Act 1993* (NZ).

[81] IPP 2 in Section 14, *Privacy Act 1988* (Cth); and section 11, *Personal Information Protection Act 2004* (Tas). Also note that, under the New Zealand legislation, organisations are not required to give notice where notice had been given on a previous occasion or where the lack of notice would not prejudice the interests of the individual concerned: Principle 3(4) in Section 6, *Privacy Act 1993* (NZ).

[82] *Public Records Act 1973* (Vic), s 12 and related Standards issued by the Public Records Office. See also Office of the Victorian Privacy Commissioner Information Sheet 05.09, *Public Records, Recordkeeping Systems and the Information Privacy Principles*, July 2009.

[83] *Ng v Department of Education* [2005] VCAT 1054 at para 84.

[84] *Ng v Department of Education* [2005] VCAT 1054 at para 85.

[85] Analysing samples obtained during roadside drug testing to derive a DNA profile is prohibited by s 58B, *Road Safety Act 1986* (Vic).

[86] See ss 6 and 7, *Surveillance Devices Act 1999* (Vic).

[87] *R v Swaffield; Pavic v The Queen* [1998] HCA 1 per Toohey, Gaudron And Gummow JJ at para 53 and Kirby J at para 131, respectively.

[88] *R v Swaffield; Pavic v The Queen* [1998] HCA 1 per Toohey, Gaudron And Gummow JJ at paras 54 and 71.

[89] For more guidance on the drafting of forms, see the Office's publications: *Public Registers and Privacy: Building Permit Data*, Report 01.02, August 2002, paras 126-127 and Recommendations 3-4 (at paras 160-161); and *Public Registers and Privacy – Guidance for the Public Sector*, August 2004, pages 16-18.

[90] *D v Banking Institution* [2006] PrivCmrA 4.

[91] *Case Note 29987* [2003] NZPrivCmr 4.

[92] See *Complainant AE v Contracted Service Provider to a Statutory Authority* [2006] VPrivCmr 6, which involved the incidental collection of information during surveillance. This case is discussed at para 1:30.

[93] See especially s 38 of the *Victorian Charter of Human Rights and Responsibilities Act 2006*, which requires public authorities to act in a way that is compatible with human rights and to give proper consideration to relevant human rights when making decisions.

[94] *R v Swaffield; Pavic v The Queen* [1998] HCA 1, Kirby J stated (at para 155, footnotes omitted).

[95] For a discussion of "reasonable steps", see paras 1:94-1:96.

[96] See also the Office of New Zealand Privacy Commissioner, *Questions and Answers about Layered Privacy Notices*, available at http://www.privacy.org.nz.

[97] *Complainant AT v Local Council* [2011] VPrivCmr 2. See also *Complainant AL v Local Council* [2009] VPrivCmr 1.

[98] See, for example, the silent voter provisions in the *Electoral Act 2002* (Vic), s 31. For a discussion of suppression mechanisms in the public register context, see Office of the Victorian Privacy Commissioner, *Public Registers and Privacy – Guidance for the Public Sector*, August 2004, pages 13-14.

[99] *Complainant E v Statutory Entity* [2003] VPrivCmr 5.

[100] *Complainant W v Public Library* [2005] VPrivCmr 5.

[101] *Ng v Department of Education* [2005] VCAT 1054.

[102] For a description of "cookies" and related technologies in the privacy context, see Privacy Victoria, *Website Privacy – Guidelines for the Victorian Public Sector*, May 2004, pages 15-17.

[103] *Complainant L v Tertiary Institution* [2004] VPrivCmr 6.

[104] *Complainant W v Public Library* [2005] VPrivCmr 5.

[105] "GPS" stands for Global Positioning System, a navigational system that uses satellite technology to provide precise information about location and speed in air, sea, and land travel. See Office of the Victorian Privacy Commissioner Information Sheet 02.08, *Privacy and Global Positioning System Technology*, June 2008.

IPP 2: Use and disclosure

2.1 IPP 2 reflects the reality that in any society, privacy requires a balancing of various, but not always competing, public interests. The starting point for information privacy laws is that privacy is a community expectation. That expectation is to be balanced – in multiple contexts involving many types of information – with the public interest in flows of information.

2.2 If primary purpose is well considered at the time of collection, the basic rule of IPP 2.1 is relatively straightforward: Use and disclose personal information only for the primary purpose.

2.3 But there are eight other instances where disclosures might be permitted beyond the primary purpose. These are contained in IPPs 2.1(a)-(h). Seven of these envisage use or disclosure without consent. Together they are a major part of the balancing foreshadowed in the objects of the *Information Privacy Act* and found in all the major international instruments on privacy.

2.4 In effect, IPP 2 makes lawful a range of uses and disclosures for purposes that may be unrelated to the purpose of collection or the primary use or disclosure.

What is "use" and "disclosure"?

2.5 **The terms "use" or "disclosure" are not defined in the *Information Privacy Act*.**

2.6 The *Macquarie Australian Dictionary* defines "use" as "employ for some purpose". However, the term "use" should be interpreted broadly in relation to personal information, and particularly in light of technological developments.

2.7 The term "disclose" has been interpreted by Courts in Australia to take its ordinary dictionary meaning, "opening something up to view or revealing it".[106]

2.8 Accidents or careless actions that result in unauthorised disclosures may be better considered under IPP 4 (Data Security). However, the types of information, and the settings for its use, are so diverse that it will often be the case that a disclosure will be relevantly considered under both IPP 2 and IPP 4. (See paras 4:17-4:21 for a discussion of the relationship between unauthorised disclosures and security breaches.)

Oral disclosure of recorded information

2.9 As noted earlier (at paras KC:10-KC:11), the *Information Privacy Act* does not apply to personal information unless it is recorded.

2.10 However, the *Information Privacy Act* will apply to oral disclosures of personal information as long as the information in question exists, or existed, at one time in a recorded format, including but not limited to visual formats.

2.11 IPP 2 will apply to all disclosures of recorded personal information no matter how the disclosure occurs. For example, a verbal disclosure of recorded personal information, or showing someone a document, are disclosures under IPP 2.

2.12 See the earlier discussion (at paras KC:10-KC:11) about "recorded" information applying to conversations that have either already been recorded or are contemporaneously recorded (for example, where notes are made after a telephone call, or where the document being discussed is about to be handed over or posted).

Disclosure by allowing others to view information

2.13 Personal information can be disclosed even though it remains in the possession or control of its original collector. The act of sending the original or a copy to another person is not a necessary element of a disclosure, although it will be a common one.

2.14 A disclosure can occur by permitting a person to read material displayed on a computer screen (for example, at a reception counter or in an office). This is a particular risk for organisations with the increasing proliferation of hand-held technology devices.

Intra-organisation uses and disclosures

2.15 Of the many organisations within the Victorian public sector, some are closely related or may fall under the same portfolio department. Entities within the Victorian public sector should not assume that, because one part of the organisation collected some personal information, this can disclosed to any other part of the organisation without regard for IPP 2.

2.16 Departmental portfolios are commonly comprised of distinct business units, statutory agencies and independent statutory offices. For example, the Department of Human Services has various business units, panels, commissions, boards and other entities carrying out many functions in diverse areas (for example, child protection and public housing).

2.17 Generally, these individual entities will be separate "organisations" under section 9 of the *Information Privacy Act*. They will have different functions, which will affect what personal information is necessary to collect (IPP 1.1). The entities may also be subject to specific statutory/other authorities to obtain information and may have obligations of confidentiality affecting the entity's authority to collect information under IPP 1 or disclose the information.

2.18 A disclosure by one body or entity will constitute a collection by the recipient body. Organisations, and entities within a departmental portfolio, should ensure they comply with both IPPs 1 and 2 when they share personal information.

2.19 This approach to intra-organisation uses and disclosures is consistent with the decision of the New South Wales Administrative Decisions Tribunal in *KJ v Wentworth Area Health Service* [2004] NSWADT 84 when Judicial Member Montgomery considered (at 49-50) the disclosure principle of the *Privacy and Personal Information Protection Act 1998* (NSW):

> The *Privacy Act* does not clearly define what is meant by a public sector agency. In my view, the expression should be given a broad interpretation, consistent with the principle that personal information should be dealt with in an open and accountable manner. For example a statutory body that is administratively part of a larger public sector agency can constitute an agency in its own right. What constitutes a public sector agency will be a question of fact to be determined on a case by case basis.
>
> While generally speaking the expression "disclosure" refers to making personal information available to people outside an agency, in the case of large public sector agencies consisting of specialised units, the exchange of personal information between units may constitute disclosure.

IPP 2.1: Primary purpose

2.20 IPP 2.1 permits use and disclosure for the primary purpose for which the personal information was collected. This creates a nexus with "collection notices" (IPP 1.3) – as organisations should have already explained the primary purpose of collection to the individual.

2.21 For further discussion of purposes, see the earlier sections on "purpose" at paras KC:72-KC:80 and IPP 1.3 (notification of purposes of collection) at paras 1:73-1:76.

2.22 For instance, in *Complainant H v Local Council* [2004] VPrivCmr 2, the Privacy Commissioner found that Council's public disclosure of petitioners' names and addresses in its minutes was in accordance with the primary purpose of collection, namely to facilitate the democratic process in government decision-making.

CASE STUDY 2-1: Council prosecution of information received in a report a primary purpose[107]

The complainant was a trained food safety officer working in a restaurant. The Local Council was responsible for enforcing food safety laws. The complainant wrote an unsolicited letter to Council, expressing concerns about the way the restaurant was complying with food safety laws. The complainant requested that Council make this clear to the restaurant proprietor.

Council prosecuted and fined the restaurant proprietors for breaches of the food safety laws. The complainant believed his letter was used in evidence in the prosecution, and if he had been informed it would be used in this way, would have tried to persuade Council not to put his letter before the courts.

In relation to IPP 2, the Privacy Commissioner commented:

> "IPP 2 requires organisations to use and disclose personal information for the primary purpose for which they collect it....arguably, the use of the letter in the prosecution brief was for the primary purpose for which it was collected."

The complainant referred the complaint to VCAT. VCAT dismissed the complaint. Deputy President Coghlan stated:

> "This principle [IPP 2] in effect requires organisations to use and disclose information for the primary purpose for which it is collected. It is abundantly clear that Council used the information it collected and held for the purpose they collected it; ie for the purpose of investigating potential breaches of the *Food Act*... where the primary purpose of collection is the same purpose as its use, that in that circumstance Principle 2 cannot have been breached."[108]

2.23 In dealing with the issue of access by parents and guardians to school reports of students aged under 18, the Privacy Commissioner said:

> Education of a young person is not the exclusive preserve of schools. Parents and guardians have an important role. They need to know how the young person is getting on at school. Communication from schools to parents and guardians about the academic progress of a young person for whom they have responsibilities is in most cases part of the primary purpose of collecting the personal information that is in a school report.[109]

Using compulsorily acquired information – the general principle

2.24 The purpose for which information is compulsorily obtained will necessarily limit the extent and purpose for which that information can lawfully be used and disclosed: see *Johns v Australian Securities Commission* [1993] HCA 56. In that case, Justice Brennan of the High Court of Australia said:

> [W]hen a power to require disclosure of information is conferred for a particular purpose, the extent of dissemination or use of the information disclosed must itself be limited by the purpose for which the power was conferred. In other words, the purpose for which a power to require disclosure of information is conferred limits the purpose for which the information disclosed can lawfully be disseminated or used...
>
> A statute which confers a power to obtain information for a purpose defines, expressly or impliedly, the purpose for which the information when obtained can be used or disclosed. The statute imposes on the person who obtains information in exercise of the power a duty not to disclose the information obtained except for that purpose. If it were otherwise, the definition of the particular purpose would impose no limit on the use or disclosure of the information. The person obtaining information in exercise of such a statutory power must therefore treat the information obtained as confidential whether or not the information is otherwise of a confidential nature. Where and so far as a duty of non-disclosure or non-use is imposed by the statute, the duty is closely analogous to a duty imposed by equity on a person who receives information of a confidential nature in circumstances importing a duty of confidence...
>
> It is therefore important to ascertain the purposes for which such information can be legitimately used or disclosed.[110]

2.25 In general, where an organisation has statutory powers to compel the provision of information to it, it should not disclose that information except for the purposes for which the powers were conferred or where otherwise required by law.

2.26 Where the statute or regulations conferring the compulsory powers provides clear authority for certain uses or disclosures, then the *Information Privacy Act* permits them. Use or disclosure will then be authorised or required by law, a permissible ground under IPP 2.1(f). (See paras 2:121-2:133 for a more detailed discussion of IPP 2.1(f).)

2.27 There will be a myriad of situations where individuals are compelled to provide their information in order to obtain a benefit, exercise a right, or comply with a legal obligation. Examples include:

a obtaining a driver's licence or registering a motor vehicle;

b registering a pet cat or dog;

c planning to renovate or build a house, or objecting to a planning proposal;

d applying for public housing;

e practising as a professional (eg, as a teacher, lawyer or doctor);

f seeking a licence to operate a child care centre;

g working in certain child-related areas;

h voting at state and local government elections; or

i complying with notices to produce documents or give evidence.

2.28 Organisations should carefully examine any laws underpinning the compulsory collection of information to ensure that any subsequent use or disclosure of that information is properly authorised. (See the discussion of IPP 2.1(f) relating to uses and disclosures that are authorised or required by or under law.)

IPP 2.1(a): Reasonably expected related secondary purposes

2.29 Personal information can be used and disclosed for purposes secondary to the primary purpose and related to it. An individual must also reasonably expect the organisation to use and disclose the information for the secondary purpose.

2.30 Clarity about the primary purpose is important, as it will determine what is or is not a secondary purpose. Examples of the relationship between primary and secondary purposes are illustrated below:

a From the *Emergencies and Privacy* Information Sheet 02.10:

Example: Local Council use for fire and flood protection:

Local Councils may collect information from ratepayers in relation to owners' properties, information such as the amenities, value, uses and upkeep of those properties.

Particularly in rural and outer-suburban areas, a related secondary purpose is the extent to which the property is a fire or flood hazard. Councils may employ fire protection and safety officers who inspect, monitor risk, prepare prevention plans and enforce bylaws (such as those regulating burning-off in the open)

Disclosure of this information to a relevant authority for the secondary purpose of safety against bushfire, flood or extreme weather is likely to be reasonably expected in this circumstance.[111]

b From the *Fences and Privacy* Information Sheet 04.08:

In the present context, councils collect personal information about property owners for the primary purpose of levying rates and charging for services provided by council. Rates are based on property values. Councils' database on ratepayers needs to contain a description of properties, their value, and the names and addresses of property owners.

Paying rates and dealing with fencing issues are part of the responsibilities of property ownership. In most circumstances, disclosure of the name and address of a property owner for the purpose of facilitating lawful fencing activity by a requester with a legitimate interest in that property owner's fence, will be a disclosure for a secondary purpose that the property owner would reasonably expect.[112]

2.31 Secondary purposes for use and disclosure must be related (or, in the case of sensitive information, directly related) to the primary purpose of collection *and* consistent with what an individual would reasonably expect.

2.32 This is a two part test:

a How is the secondary purpose *related* (or directly related) to the primary purpose?

b Would an individual whose information was collected *reasonably expect* the use or disclosure?

Related secondary purposes

2.33 The secondary purpose for which the information is used or disclosed has to be connected to or associated with the primary purpose. It must relate to the primary purpose for which it was collected. If sensitive information is involved, the secondary purpose has to be *directly* related to the primary. The organisation bears the onus of showing this relationship.

2.34 The Explanatory Memorandum suggests that a reasonably expected secondary use would be where information collected in delivering a government service is subsequently used to manage, evaluate or improve that particular service. So, quality assurance and program evaluation and development are likely to be regarded as reasonably expected secondary purposes.[113]

2.35 In *Ng v Department of Education* [2005] VCAT 1054, the Department installed a CCTV camera in the computer room of a school to minimise the risk of vandalism and to monitor student use of the computers. The CCTV footage was subsequently used during an investigation into the teacher's work performance in the classroom. In that case, VCAT found that the purpose of installing the CCTV camera was not the broad, objective outcome of having an "all seeing eye" taking visual recordings of any "relevant incident" that may need to be investigated, but the specific motive of collecting information about student misbehaviour and inappropriate conduct in the computer room where the CCTV was installed. However, use of the CCTV footage to assess the teacher's performance in managing inappropriate student behaviour was a secondary purpose "clearly related to monitoring the inappropriate behaviour itself."[114]

2.36 Other related secondary purposes have been found by the Privacy Commissioner or VCAT include the following:

a the secondary use by police of firearm licence holders' fingerprints in the investigation of crime was related to the primary purpose of collection, which involved assessing the person's suitability to hold a firearm and to ensure the ongoing possession and use of firearms was conditional on the need to ensure public safety and peace: *Complainant AB v Victoria Police* [2006] VPrivCmr 3;

b the secondary disclosure of a tertiary student's contact details to a debt collector after the student incurred a debt for a course was related to the primary purpose of collecting the information, that being the enrolment of fee-paying students: *Complainant M v Tertiary Institution* [2004] VPrivCmr 7.

2.37 In some cases, use or disclosure would not be related – despite what may seem at first glance to be an apparent link between the primary purpose and the disclosure. For instance, in *Duggan v Moira Shire Council* (2004, Unreported, VCAT), the Local Council submitted that the primary purpose of collecting the identity of a person who found a dog was related to the secondary purpose of informing the grateful owner of the finder's details so that the owner could thank the finder. VCAT rejected this, finding instead that the primary purpose was to collect the dog:

> I am unable to accept the submission that the secondary purpose was related to the primary purpose. The primary purpose of collection was to enable the Council to make contact with the [finder] to collect the dog, and if there were any difficulties in so doing, to get further particulars of the dog's whereabouts. I am not satisfied that the disclosure of the [finder's] name to [the owner] was related to this purpose.[115]

Reasonably expected

2.38 For a use or disclosure to be "reasonably expected", it is necessary to ask what an ordinary person, not expert in the workings of government but aware of the circumstances, would consider reasonable. The test used for interpreting reasonable expectation was described in *Complainant D v Minister* [2003] VPrivCmr 4 (see Case Study 2-2) as follows:[116]

> The test is an objective one. It is the reasonable expectation of an ordinary person, who is not necessarily expert in the workings of government, that is to be considered in the particular circumstances.

2.39 The expectations of the actual individual involved are a consideration, but they are not determinative.

> **CASE STUDY 2-2: Referral of ministerial correspondence reasonably expected**[117]
>
> A Minister disclosed personal information about a complainant to the organisation which was the subject of the complaint.
>
> The Commissioner considered the disclosure to be part of the primary purpose insofar as a Minister would typically refer matters to those with the requisite responsibility and/or capacity to assist on a matter. The Commissioner said that even if such a disclosure was not for the primary purpose, it was for a secondary purpose related to the primary purpose.
>
> The Commissioner reasoned that an ordinary person, although not expert in government administration, would reasonably expect that the Minister and his or her personal staff do not themselves deal with the detail of complaints and enquiries from the public. Rather, a person would reasonably expect that the Minister and his or her staff would refer the complaint (and the complainant's details) to those who can and should deal with them.

2.40 Organisations know more about government structures and processes than the "ordinary person". However, in considering reasonable expectations, organisations need to put themselves in an individual's place and consider what would be expected as reasonable by that ordinary person, who is not expert but aware of the circumstances.

2.41 A secondary use or disclosure might be reasonably expected where that use or disclosure is "inextricably linked" to the primary purpose of collection. In *Ng v Department of Education*, VCAT found that:

> the inextricable link between inappropriate behaviour by students and the quality of teachers' management of that behaviour is so close as to render it reasonably foreseeable by a reasonable teacher that footage taken for the one purpose should be used for the other.[118]

Reasonably expected due to individual's own actions

2.42 Where an individual discloses their own information in a public forum, for instance by talking to the media about a complaint they made about a public sector organisation, the individual ought reasonably to expect that the public sector organisation will respond to media inquiries and may, in responding, disclose the person's information in a proportionate manner. In *Complainant Y v The Department* [2005] VPrivCmr 7, the Privacy Commissioner stated:

> I consider that an individual who speaks willingly to a journalist (whom s/he knows writes articles for publication), about matters that are to be the subject of a public tribunal process, would reasonably expect that the organisation complained about may also respond in public... An organisation may communicate with a number of media organisations to ensure its reputation and interests are protected, if each has picked up on a story and appears likely to publish on it, regardless of the fact that the story was initiated through one alone. Similarly, a respondent organisation may need to disclose to correct what the respondent may regard as inaccurate or misleading information disseminated by media outlets other than the outlet to which a complainant first spoke. A complainant who knowingly takes his or her complaint to "the court of public opinion" reasonably expects that a respondent organisation will mount its defence in that same forum.

Examples of reasonable expectation

2.43 The extent to which personal information might reasonably be expected to be disseminated within an organisation will be affected by matters such as the size of the organisation and the functions of the individuals within the organisation (affecting their "need to know"). For instance, in *Complainant Q v Contracted Service Provider to a Department* [2005] VPrivCmr 3, the Privacy Commissioner accepted that it was reasonably expected that a Human Resources Manager could pass on the outcome of a criminal record check for a job applicant to two senior staff members with responsibility for supervision and management of the person's work. A person's reasonable expectation would be that the information would not flow outside the organisation, or to people within the organisation who did not have a "need to know".

IPP 2

CASE STUDY 2-3: Disclosure of petitioners' details reasonably expected[119]

A member of the public organised a petition and sent it to his local council. The Council invited him to attend the meeting in which it was tabled for discussion. The Council later posted the petition on its website as part of the minutes of the meeting. The petitioner was concerned that his personal details (name and address) were available on the petition and thus on the website.

In the Commissioner's view, the primary purpose for which the Council collected the personal information contained in the petition was to facilitate the democratic process in government decision-making.

The Council had discussed the petition at an ordinary meeting that was open to members of the public. Moreover, councils, like all government bodies, have a duty to be accountable and, where possible, transparent to the public. Accordingly, the minuting of the petition and its discussion, along with any arising decisions by Council were all related secondary purposes for which it was collected.

The assessment of whether a related secondary purpose is reasonably expected is an objective one: would an ordinary person, although not expert in government administration, reasonably expect that any personal information they put on a petition, circulated through the community and tabled at a public meeting, would ultimately be disclosed?

The Commissioner considered that a person would reasonably expect such a disclosure.

Sensitivity of information may affect reasonable expectation

2.44 The extent of later disclosure may also be affected by the manner in which the information was given to government, and by the sensitivity of the information itself. For instance, in *Complainant H v Local Council* [2004] VPrivCmr 2 (see Case Study 2-3), in addition to finding the disclosure in council minutes of petitioners' details was in accordance with the primary purpose of collection, the Privacy Commissioner found that the circumstances in which the information was gathered and presented to Council also created a reasonable expectation that it would be publicly disclosed. The Privacy Commissioner cautioned, however, that there may be cases where disclosure would not be appropriate where that disclosure would reveal sensitive or delicate information:

> An ordinary person, although not expert in government administration, would reasonably expect that to put their name to a petition that is to be circulated throughout the community to gather more signatures, with a view to having the petition tabled at a public meeting, would result in the disclosure of any personal information they elect to put on the petition.
>
> Only in the rarest of circumstances, such as a petition by persons who all have a particular illness petitioning for better health services, will disclosure not be appropriate. In the example given of illness, to disclose would reveal more about a person than just their name and address. In such cases it might be appropriate to keep private the actual names and addresses while disclosing the subject matter of the petition itself.

2.45 In *Complainant F v Tertiary Institution* [2003] VPrivCmr 6, a PhD student's ongoing candidature was reviewed by a Tertiary Institution review panel. Having received unfavourable comments from the panel, the student asked his Master's thesis supervisor to review a draft PhD thesis. Prior to doing so, the Master's thesis supervisor spoke to the PhD supervisor about whether the Master's thesis supervisor should be reviewing the thesis, and was advised not to review the thesis as the student's candidature had been terminated. The student complained about disclosure of information about his PhD candidature information to the Master's thesis supervisor. The Privacy Commissioner found that the disclosure was reasonably expected:

> It is necessary and appropriate that a PhD supervisor be able to give his or her opinion about whether a Masters thesis supervisor should proceed to review a PhD thesis where the candidate has already been requested by a Review Panel to withdraw as a candidate for a PhD. A person would reasonably expect, absent special circumstances, that two academics with a close working relationship, from within the same department, who both at varying points in time supervised the same student, might discuss that student's progression from a master's degree to a doctorate.

CASE STUDY 2-4: Disclosure of complaint details to employee complained of reasonably expected[120]

The complainants had a son at a local kindergarten, operated by a Local Council. The complainants wanted to complain about fee advice given to them by their son's kindergarten teacher. They were told to make a written complaint, which they did, and were told it would be kept confidential. The President of the kindergarten informed the complainants that they had shown the complainants' letter to the kindergarten teacher, about whom the complaint related.

The Privacy Commissioner considered the provisions of IPP 2 and stated:

> Where a person raises a complaint with an organisation about the actions of a particular individual within that organisation, it is often necessary to seek a response from the individual who is the subject of the complaint in order to afford natural justice. "Natural justice" requires that where an allegation is made about an individual, and as a result it is proposed that action be taken against the person being complained about, it is only fair that that person be given a right of response in order for the complaint to be properly and fairly investigated.
>
> In light of the particular circumstances of this complaint and despite the parties' conflicting version of events, the allegations against the teacher could not have been adequately addressed unless the teacher was given an opportunity to respond. Therefore, showing the complaint to the teacher was arguably part of the primary purpose of its collection, and in any event a related secondary purpose. A reasonable person in the complainants' position should reasonably expect that in the interests of natural justice, where s/he has complained about a specific conversation held with a certain individual, that this individual would have to be consulted about the issue in order to ascertain whether or not there was any basis to the complaint.

Limiting disclosure to what is sufficient

2.46 **When disclosing under IPP 2.1(a), the amount of information disclosed should not exceed what is sufficient to satisfy the related secondary purpose – see Case Studies 2-5 and 2-6. Excessive disclosure is not reasonably expected.**

CASE STUDY 2-5: Avoiding excessive disclosure when handling complaints[121]

Ms B complained that AC had misused his position in the Public Sector Body to obtain information about her, and other people, for a personal purpose. Following internal investigation and disciplinary proceedings, the Public Sector Body informed Ms B of the outcome of its investigation into AC as well as its findings about the wider allegations that other individuals' privacy had been breached.

The Privacy Commissioner found that it was reasonably expected that the Public Sector Body would provide sufficient information to Ms B to show that the investigation of her complaint and outcome were fair. This ensured that organisations deal properly with complaints and are seen to do so. However, the Privacy Commissioner considered that the disclosure of the results of the wider investigation appeared to involve more information than was sufficient to deal properly with Ms B's complaint. The Public Sector Body acknowledged to AC that its disclosure was excessive and undertook to review its policies concerning the release of information to people who complain about its staff.

CASE STUDY 2-6: Avoiding excessive disclosure when handling complaints[122]

See Case Study KC-2 for the fact scenario. In its response, the organisation argued that even if it had received the complainant's withdrawal of consent prior to distribution, disclosing the complaint documentation – in full – was a necessary part of the investigation process. Further, the organisation argued it was 'not reasonably possible' to edit the complaint documentation before distribution.

The Privacy Commissioner considered that the disclosure of the complainant's information in full to all of the alleged bullies was far more than what they needed to respond to the complaint about their own alleged behaviour. Disclosure of information should have been kept to the minimum necessary to investigate the matter and did not require the wholesale disclosure that had occurred in this instance. Similarly, the Privacy Commissioner considered that it was possible to edit the document provided in order to protect the complainant's privacy. She considered that an investigation process requires an organisation to collate the information provided in a complaint and reasonably determine what needs to be disclosed to each staff member.

Using notices to build an expectation

2.47 Notice statements outlining the secondary purposes for which the information is to be used or disclosed, given at or prior to the time of collection (under IPP 1.3), can assist in creating an expectation that information is to be used for related secondary purposes. However, more may be required to establish that the secondary use is "reasonably" expected. For instance, a secondary use or disclosure that breaches an undertaking of confidentiality cannot be said to be "reasonably" expected. Notice cannot be used to override other existing legal obligations.

2.48 Reasonableness requires that the related secondary use or disclosure is also proper and fair, and generally not incompatible with the primary purpose of collection. Organisations that give notice of their intention to use or disclose information contrary to what a person might reasonably expect may find that the willingness of individuals to transact with the organisation, or to provide complete and accurate information, may be compromised.

IPP 2.1(b): Consent

2.49 Consent is one of the exceptions to the basic rule that primary purpose governs use and disclosure. Where an individual has consented to other uses or disclosures, including unrelated or even incompatible ones,[123] an organisation may use or disclose the personal information accordingly. The elements of valid consent were discussed under Key Concepts at paras KC:42-KC:60.

2.50 Consent occupies no privileged position in IPP 2. Just because an individual does not provide consent to use or disclose personal information will not necessarily mean an organisation will be unable to use or disclose personal information. Other categories, such as disclosure authorised or required by or under law, may allow a disclosure to proceed irrespective of whether the individual's consent was sought or obtained.

2.51 For instance, in *Complainant Q v Contracted Service Provider to a Department* [2005] VPrivCmr 3, in completing a Victoria Police application form, the complainant consented to the disclosure of the results of a criminal record check to a named officer within the Respondent Organisation's human resources department. Although the complainant believed that in doing so, he was effectively limiting disclosure to that person only, the Privacy Commissioner found that the wider disclosure to two other senior staff who would supervise and manage the complainant's work did not amount to a breach of privacy as the disclosure fell within one of the other permitted uses in IPP 2 – that is, it was a reasonably expected related secondary disclosure under IPP 2.1(a).

Distinguishing consent from notice

2.52 Organisations must distinguish consent from notice. The law, administrative practice or the simple fact of government's unique role may mean that individuals have no real choice in a use or disclosure. In such circumstances, when the individual signs a form it is usually regarded as an acknowledgement that he or she has received notice. It is not "consent" in the proper sense of the word. (See the discussion of consent in "Key Concepts", especially paras KC:52-KC:53.)

"Opt-in" consent versus "opt-out" consent

2.53 If organisations want to use personal information in ways that do not fall within either the primary or related secondary purposes, it is open to them to seek consent from the individuals concerned.

What is "opt-in" and "opt-out"?

2.54 An "opt-in" consent model means that personal information cannot be used or disclosed for purposes (such as marketing) unless the person has given their prior consent to the particular use or disclosure.

2.55 An "opt-out" model is where individuals are told that their personal information will be used or disclosed in a particular way unless they take some action (for example, ticking a box) to say that they do *not* consent.

2.56 Opt-out models create uncertainty as to whether consent is validly given. Simple failure to tick a box, for example, may be due to the individual not reading that section of the form, rather than the person consenting to what is proposed.

Opting-in preferred approach for Government

2.57 Individuals can choose whether or not they engage with most private sector organisations, and whether they want to provide their personal information to them. However, often state and local government organisations collect information under law or to provide a service only government provides. People may have no choice but to provide the government organisation with their personal information.

2.58 As a result, the default position should be to require 'opt-in' consent for other uses and disclosures not otherwise permitted under IPP 2. (Also see the earlier section on "opting in to direct marketing" at paras KC:69-KC:71 and the discussion of consent at pages 19-25 of OVPC's report, *Public Registers and Privacy: Building Permit Data*, Report 01.02, August 2002.)

IPP 2.1(c): Research or statistics where impracticable to seek consent

2.59 The *Information Privacy Act* applies in the research and statistics context where a Victorian government organisation uses or discloses identifiable information obtained directly from the individuals concerned (that is, the research subjects), or where the information is obtained from other sources (such as records held by a public or private sector organisation).

2.60 The *Information Privacy Act* facilitates the conduct of research in a number of ways, not limited to the use/disclosure ground in IPP 2.1(c). For instance, using unidentifiable data, or relying on consent, are alternative ways that research can be carried out in compliance with the *Information Privacy Act*. These should be considered first by organisations intending to disclose to researchers, or to conduct research themselves. Both approaches are discussed in paras 2.61-2.64.

Research using unidentified data

2.61 Where the research or statistical data is aggregated or anonymised so that research subjects' identity cannot be reasonably ascertained, then the *Information Privacy Act* will not apply. Such data will not be considered personal information. See the earlier discussion about the meaning of "personal information", especially the sections on whether identity can be reasonably ascertained (paras KC:18-KC:23) and on de-identification and coding (paras KC:24-KC:28).

Research with consent

2.62 Personal information can be used and disclosed with the individual's consent (see paras 2:49-2:51). Research is routinely carried out with a subject's consent. Consent is foundational in human research and has been the preferred basis upon which such research is conducted.

2.63 For further guidance on "consent", see the earlier discussion of the term at paras KC:38-KC:71 and of consent as a basis for use and disclosure under IPP 2.1(b) at paras 2:49-2:58.

2.64 When an organisation is about to introduce a new initiative that involves the collection of personal information (eg, a pilot project that will trialled and later evaluated), the likelihood of using personal information for research purposes should be anticipated at the start. This allows organisations to seek consent or give notice, as appropriate, at the point of collection – saving the organisation from having to go back to the individuals later to seek their consent to research.

Non-consensual research under other IPP 2 grounds

Authorised by law

2.65 Research may also be carried out without consent where, for instance, it is authorised or required under law (IPP 2.1(f)). The disclosure by the Victorian Electoral Commission of electoral information for medical research under s 34 *Electoral Act 2002* (Vic) is an example. Note that the authorising legislation may itself impose some obligations or restrictions on how the information is used or disclosed. For example, the *Electoral Act* expressly forbids the disclosure of silent electors' information – whether to researchers or to others (like political parties, members or candidates).

Disclosure necessary to lessen/prevent serious threats to public health, public safety or public welfare

2.66 Another possible basis for conducting research lies in IPP 2.1(d)(ii), where an organisation reasonably believes that the use or disclosure of personal information is necessary in the context of lessening or preventing a serious threat to public health, public safety or public welfare. Research into preventing serious injuries or fatalities might fall into this category.

Research using sensitive information

2.67 If a researcher wishes to use sensitive information (eg, ethnic origin and criminal record), IPP 10 may be relevant. IPP 10 authorises collection of such information in limited circumstances, such as by consent or, in some situations, without consent where the research is relevant to government funded targeted welfare and educational services. Sensitive information is dealt with by IPP 10. See especially the discussion of using sensitive information by consent (paras 10:27-10:31) and in the context of research (paras 10:32-10:33 and 10:44-10:57).

Research in the public interest, where impracticable to seek consent

2.68 IPP 2.1(c) provides for the use and disclosure of personal information for research purposes, or for the compilation or analysis of statistics, in the public interest, other than for publication in an identified form, where it is impracticable to seek the individual's prior consent. In the case of disclosure, the organisation must reasonably believe that the recipient will not further disclose the information.

2.69 An organisation seeking to rely on IPP 2.1(c) needs to consider the following questions:

a Is the use or disclosure of identifiable information *necessary* for research or statistical work, by the organisation itself or by the proposed recipient of the information? Can the same research objectives be achieved with alternative sources of data, or data that has been de-identified or is anonymous?

b Will the research or statistical analysis/compilation result in publication of the information in a form that identifies any particular individual? If the data is to be de-identified prior to publication, how effective will that be? Consider, for instance, whether research subjects' identity can be reasonably ascertained where data is drawn from small communities.

c Does the organisation reasonably believe that the recipient of the personal information will not disclose the information? Have undertakings of confidentiality been sought? Where the disclosure is outside of Victoria, have appropriate privacy protection measures been attended to, in accordance with obligations under IPP 9 (see especially para 9:5)?

d If it is necessary to use identifiable data, can the research subjects' consent be sought? Or is it *impracticable* to seek the subjects' consent before their personal information is used or disclosed?

e Is the work *in the public interest*?

2.70 These two latter aspects – the impracticability of seeking consent, and research in the public interest – are discussed further below.

"Impracticable" to seek consent

2.71 Impracticability must be assessed in context, but generally it means more than mere inconvenience or some cost and effort for a public sector organisation.

2.72 Moreover, the *impracticability* of seeking consent should not be confused with the *undesirability* of seeking consent. IPP 2.1(c) does not permit consent to be waived where, for example, consent can be readily sought but organisations would prefer not to do so (for instance, out of a desire for a high or 100% rate of participation).

2.73 Useful guidance on interpreting the meaning of "impracticable" in this context can be found in the *CIHR Best Practices for Protecting Privacy in Health Research*, developed by a Privacy Committee comprised of representatives from privacy commissioners, research bodies, consumer groups and other stakeholders from across Canada. See Extract below.

EXTRACT: CIHR Best Practices for Protecting Privacy in Health Research, September 2005, pages 7 and 40:[124]

Seeking consent from individuals for the use of their personal data may be considered *impracticable* when there are difficulties in contacting or notifying individuals for reasons such as:

- the size of the population being researched;
- the proportion of prospective participants likely to have relocated or died since the time the personal information was originally collected; or
- the lack of an existing or continuing relationship between prospective participants and the data holder who would need to contact them (eg, a patient database that does not have a regular follow-up program to maintain a complete and accurate record of changes in registrants' contact information over time);

such that:

- there is a risk of introducing bias into the research because of the loss of data from segments of the population that cannot be contacted to seek their consent, thereby affecting the validity of results and/or defeating the purpose of the study; or
- the additional financial, material, human, organisational and other resources needed to obtain consent could impose a hardship or burden on the researchers or organisation so burdensome that the research could not be done.

Notification after use/disclosure and withdrawal

2.74 Where it is impracticable to seek consent before the research subject's data is used, it is still open to the organisation to notify the person after the use or disclosure. This provides individuals with an opportunity to withdraw from further participation in the research study (and possibly, but not necessarily, be able to withdraw their data), consistent with ethical research standards supporting revocation of consent and informing subjects of the implications of that revocation.[125]

Research "in the public interest"

2.75 IPP 2.1(c) makes clear that research and statistical work cannot be carried out without consent unless the work is justified by a public interest. European data protection instruments have suggested that research and statistics "in the public interest" involve "matters which affect society's essential interests and in which the state has responsibilities" such as containing epidemics, combating drug taking, investigating the scale and pattern of sexual assaults on minors, or developing aid to social groups in difficulty.[126]

2.76 The Australian Privacy Commissioner has also acknowledged the public interest in similar types of research, such as:

a monitoring the causes of, and circumstances surrounding, homicide in order to improve public understanding and provide a foundation for the formulation of public policy in areas such as family law, child protection and firearms regulation; identify characteristics that place individuals at risk of homicide; and provide indicators of the efficiency and effectiveness of existing preventative measures;[127] and

b research into the nature and extent of serious fraud in Australia and New Zealand, the appropriateness of sanctions imposed, designing prevention initiatives, and determining the cost of fraud to the community.[128]

Questions to ask to determine whether proposal is "in the public interest"

2.77 In assessing whether research or the compilation or analysis of statistics is "in the public interest", organisations should consider questions such as:

a Is the organisation conceiving of the public interest as being wider than its own needs?

b How is the wider community expected to benefit from the research or statistical analysis/ compilation? Will the community benefit, for example, through the:

i. gain in greater knowledge, insight or understanding within fields such as science and humanities;

ii. improvement of social welfare, public safety, or individual well-being or the minimisation of serious harm;

iii. enhancement of the delivery of government services or targeting of government funded welfare or educational services?

c. Are there any countervailing considerations or interests that should be taken into account in balancing the public interests in privacy and the conduct of the research? For instance:

i. Is there a cost to the community of not undertaking the research or statistical work?

ii. Are participants at risk of any harm (eg, physical, emotional, social, economic or legal harm)? If so, what is the seriousness and likelihood of this harm? Do participants have a view about what is an acceptable level of risk?

d. Will the research or statistical work lead to any particular benefit – or pose any particular risk – to participants from specific groups who may, for instance, be in a relationship of dependency or inequality or may otherwise be vulnerable?[129]

Making first contact with prospective participants

2.78 Various options are available under the *Information Privacy Act* to allow an organisation's information holdings to be used for the purpose of making first contact with prospective research participants. In some cases, prior consent may have already been obtained by the organisation, satisfying IPP 2.1(b). For example, individuals may have been given the option (at the time when their information was originally collected) of later being contacted to participate in research or surveys.

2.79 In other cases, participation can be sought without disclosing identified information, such as through the publication of notices seeking participants. Anyone responding to such notices or advertisements would then be participating by consent, consistent with IPP 2.1(b) and/or the primary purpose of collection (IPP 2.1).

2.80 Where prior consent has not been obtained, an organisation may be able act as an intermediary by using its information holdings to make first contact on behalf of the researcher. This may be in accordance with IPP 2.1(a) where the research is related to the organisation's functions or activities and is reasonably expected. (For instance, a school may initiate contact with students and their families about education-related research.) Here, the public interests in privacy and research are balanced by the organisation maintaining control over the information it holds and only disclosing identifiable details after consent has been obtained by those individuals wishing to participate in the research.

2.81 In some cases, there may be authorisation under law to disclose information to a researcher (IPP 2.1(f)). For example, section 34 of the *Electoral Act 2002* (Vic) expressly authorises disclosure of enrolment information in the public interest, including for medical research or the provision of a health screening program.

Research using data matching or data linkage

2.82 Researchers and statisticians sometimes use data matching or data linking when conducting their research or analysis. The Privacy Commissioner considered the concept of "data matching" in OVPC's *Data Matching in the Public Interest – A Guide for the Victorian Public Sector,* August 2009, and suggested the following definition of the term:

> Data matching... includes any/all of the following:
>
> - comparing personal information from two or more records to determine whether personal information from different records matches to the same individual; and/or
> - comparing personal information about an individual obtained from two or more records to gauge the accuracy of the personal information about that individual in each of the records, and to improve the accuracy of the personal information in all of the records; and/or
> - connecting two or more records of personal information to aggregate personal information about an individual.
>
> Some of the activities within the definition are sometimes referred to as "data sharing", "data linkage" and "data cleansing".[130]

2.83 Data matching may be conducted for the benefit of those whose information is involved, for example to identify beneficiaries of programs, or more usually to facilitate compliance action, for example, against tax evasion or breach of conditions for assistance. In the research context, data matching is often carried out to discover new trends or causal factors to health or safety issues.

2.84 Victorian government organisations should be aware that much of the data it holds was obtained compulsorily from individuals who, for instance, were seeking a benefit or entitlement, or exercising a right. Driver's licence data, ratepayer databases, and electoral roll information are all examples. As acknowledged in the *Data Matching in the Public Interest* guide, organisations may find it very useful to match these data sets, but it is important that there be a legitimate public interest involved:

> From the point of view of the public, these are three very different data sets in which their personal information is held (often compulsorily) to serve quite separate public purposes. At a minimum, when unrelated data sets are connected and compared – especially for reasons that may affect persons' legal rights and obligations – that activity needs to be:
>
> - clearly justified in the public interest;
> - authorised under law;
> - carried out transparently; and
> - supervised independently.[131]

2.85 When any data matching activity involving the use or disclosure of personal information is to be carried out, consideration should be given to the legislative obligations under the *Information Privacy Act* – notably, that the collector's activity is limited to what is necessary, fair, lawful and not unreasonably intrusive, and that the disclosing organisation has obtained consent under IPP 2.1(b), has lawful authority under IPP 2.1(f), or complies with the public interest and other requirements in IPP 2.1(c).

2.86 Consideration should also be given to whether the information can be meaningfully de-identified prior to use by, or disclosure to, the researcher. See paras KC:24-KC:28, 3:38-3:48 and 7:11-7:15 for further guidance about de-identification and data matching.

2.87 Significant data matching may require express legal authority, with transparency and oversight. Organisations are encouraged to refer to OVPC's Guide for *Data Matching in the Public Interest*[132] and/or to consult with OVPC for further guidance about specific projects or proposals.[133]

Role of research ethics committees

2.88 Research involving human subjects (or their data) may require prior ethics approval from the organisation that is conducting, or who will disclose, the data. Universities and other organisations may be required (due to their funding or other arrangements) to consider the national guidelines relating to the ethical conduct of human research. These obligations may exist where research is funded by, or carried out under the auspices of, the National Health and Medical Research Council, the Australian Research Council, or the Australian Vice-Chancellors' Committee.

2.89 In some cases, organisations will be required by state or federal privacy laws to seek ethical approval for research. For instance, statutory guidelines for health and medical research have been issued under the Federal *Privacy Act* and the Victorian *Health Records Act.*

2.90 However, unlike the Federal *Privacy Act* and the Victorian *Health Records Act*, binding statutory guidelines for research have not – and cannot – be issued under the *Information Privacy Act.* Ethics approval is therefore not required, but is generally advisable. A research ethics committee review may provide an opportunity for an organisation to consider the various elements in IPP 2 that might be relied upon to support a use or disclosure for research.

2.91 Notably, in the context of IPP 2.1(c), a research ethics committee can review a research proposal to determine whether the research is in the public interest, whether or not seeking consent is impracticable, and whether adequate safeguards have been set up to satisfy the disclosing organisation that the recipient will not further disclose the information. An ethics review may also be useful in assessing whether research involving data matching/linkage is the least intrusive option, especially if it is proposed to be conducted without consent.

2.92 An ethics review should be considered when research will involve collecting personal information directly from participants (such as through surveys or focus groups) or where the information is collected indirectly through observation (if the subjects are identifiable) or by accessing existing records or databases.

IPP 2.1(d): Necessary to lessen or prevent serious threats to health or safety

2.93 IPP 2.1(d) allows use or disclosure to occur where the organisation reasonably believes it is necessary to lessen or prevent:

a a serious and imminent threat to an individual's life, health, safety or welfare; or

b a serious threat to public health, public safety or public welfare.

Imminent

2.94 In IPP 2.1(d)(ii), note that the threat to public health/safety/welfare must be serious, but not necessarily imminent. This is in contrast to a threat to an individual's life/health/safety/welfare (IPP 2.1(d)(i)), which must be both serious *and* imminent.

2.95 "Imminent" in IPP 2.1(d)(i) is directed at emergency situations, where a threat to life or health could include a threat to safety (eg, bushfires). Disclosures for non-imminent threats are better dealt with by way of consent. A threat can remain 'imminent' over a period of time, for example, in the case of domestic violence where there is ongoing concern about harm to the victim, and disclosure is necessary to provide continued protection. "Imminent" is omitted from IPP 2.1(d)(ii) in order to capture threats to public health or safety that may be serious enough to warrant disclosure but not imminent in terms of time (eg, a outbreak of an infectious disease).[134]

2.96 In *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77, the Appeal Panel adopted the ordinary dictionary meaning of "imminent" as being "likely to occur at any moment; impending".

2.97 Note that an "imminent threat" may be a continuing one, for example in the aftermath of a disaster. See OVPC's *Emergencies and Privacy* Information Sheet 02.10.

> CASE STUDY 2-7: **Example of a "serious and imminent threat"**[135]
>
> M lodged a complaint with the Department of Human Services (DHS) in relation to an alleged child stealing racket, believing agencies in local government were acquiring child "clients" illegally. M alleged that after lodging this complaint, DHS provided a health provider with her residential address, and by doing so breached M's privacy. Although Member Proctor ultimately decided that, on the facts, the DHS did not provide M's address to the health provider, Member Proctor went on to consider whether disclosure of M's address would have been a breach of the Act had it occurred. In obiter, Member Proctor stated:
>
> 'Given my above finding, I do not need to rule on the issue of whether DHS disclosing the address was a breach of the (Information Privacy) Act. However, I will comment that MS (the employee of DHS alleged to have disclosed M's address) providing a person's address to a health provider, where the CEO of the health provider advised that the person had threatened to commit suicide would have led me to find that DHS reasonably believed disclosure was necessary to lessen or prevent a serious and imminent threat to M's life, health, safety and welfare.'

Use/disclosure is necessary to lessen or prevent a threat

2.98 It is not enough for an organisation to form a reasonable belief that there is a serious (and, in the case of an individual, imminent) threat. IPP 2.1(d) also requires that the organisation believe that it is *necessary* to disclose information in order to lessen or prevent the threat. In determining whether a use or disclosure might be regarded as necessary, consider the following:

a Is the use or disclosure motivated by an intention to lessen or prevent the threatened harm?

b Is the information being used or disclosed relevant to managing that threat?

c Where information is disclosed, is the recipient in a position to act on the information to lessen or prevent the harm from eventuating?

2.99 IPP 2.1(d) does not specify who can make use of the information or to whom it may be disclosed. In most cases, the recipient would need to be an appropriate agency that is in a position to lessen or prevent the particular threat. For instance, and depending on the circumstances, appropriate recipients would be the police, emergency services or health authorities.

2.100 The requirement for necessity was discussed in *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77, where the Appeal Panel considered an equivalent provision under the New South Wales privacy legislation and found that the disclosure was not "necessary" to prevent or lessen the threat of harm in that case – see Case Study 2-8.

CASE STUDY 2-8: Disclosure not "necessary" to prevent threat to individual's health, and threat not "imminent"[136]

A soccer coach used his position as a teacher at the soccer player's school to access her school records when he was alerted to possible health concerns that might prevent her from playing in the team's grand final game. After reading a medical report on her file, he approached the player and told her the club needed an indemnity from her parents in case she was injured. The next day, the player told the coach that on legal advice they refused to provide the indemnity. The coach then contacted the president of the soccer club to say he had become aware of the player's medical condition, that he did not think she was match fit, and that others had told him she would end up in a wheel chair if she played. The club president approached the player and her mother at a soccer training session to express his concerns for the girl's safety but, according to the club president, the conversation ended with the mother becoming abusive. The player did not play in the grand final.

The NSW Administrative Decisions Tribunal Appeal Panel accepted the earlier finding that the disclosure was not "necessary" to prevent or lessen a threat of harm, as a letter from the coach had stated that the player's health was not a reason to prevent her from playing soccer. The Appeal Panel accepted the earlier Tribunal's finding that the coach's disclosure to the club president was instead motivated by a concern to protect both himself and the club from any potential personal injury claims.

The Appeal Panel also found that the threat to the player's health or safety was not "imminent", as she had regularly played with her knees strapped and there was no evidence that an injury was "impending".

Public officials acting on information obtained in their private capacity

2.101 From time to time, public officials may come across information in their private capacity that leads them to believe or suspect that someone poses a serious risk to an individual's, or the public's, health, safety or welfare. Public officials may be tempted to use their privileged access to official information (such as criminal records or child protection files) to confirm their suspicions and decide to use or disclose the information in their private capacity. This situation may create difficulties for an organisation that has a function to protect the community from threats of harm but also has obligations to prevent sensitive information it holds from being used for personal reasons or disclosed to unauthorised persons.

2.102 The dilemmas associated with public sector employees accessing official information to confirm private suspicions was illustrated in the New South Wales case described in Case Study 2-9. (Other aspects of this case are discussed in the Guidelines' section on the relationship between unauthorised disclosures and data security breaches (at para 4:18)).

CASE STUDY 2-9: Use and disclosure of official information for personal reasons[137]

A president of a Scottish dancing school (M) used her official access privileges as a parole officer to check the Department's criminal history records relating to a dance instructor (NS) after she became concerned that he posed a serious threat to the children attending the dancing school. M discovered that NS had prior convictions for offences involving minors and was a "prohibited person" and therefore not permitted to engage in unsupervised work with children. M disclosed these facts to NS's parole officer, and he was arrested the next day for breaching his parole conditions. However, M went further and threatened NS with exposure unless he immediately telephoned every parent of students in the class and told them of his criminal history. M then disclosed the information to a number of parents at the school.

After NS was released from custody (about 4 months after his arrest), he was immediately re-arrested and charged with a new offence involving sexual assault of a minor, who had attended the Scottish dancing school. M used her access privileges again to find out who visited NS when he was in custody. M contacted one of NS's visitors and disclosed the fact that he had been re-arrested and charged with sexually assaulting a 10 year old student at the school.

The Tribunal in that case found that M had accessed the Department's database for a dual purpose – for her own private reasons, and as a parole officer to verify and inform appropriate persons of the risk in order to enable the agency to carry out its functions in supervising parolees. The Tribunal accepted that M's access and disclosure to NS's parole officer was permissible given her belief that it was necessary to prevent or lessen a serious and imminent threat to the children in NS's dancing classes. However, the disclosures to parents and the visitor, on the other hand, were unauthorised as M was acting entirely for her own private purposes, in her private capacity.

This case was later referred to by the New South Wales Administrative Decisions Tribunal Appeal Panel in *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77). The Appeal Panel commented (at para 58) that, "However well intentioned [the correction officer's] conduct may have been, it clearly involved a gross violation of the confidentiality of prisoner records."

2.103 Government employees, like any person in the community, should have a legitimate avenue for conveying to the appropriate authorities concerns about individuals whom they believe present a serious risk of harm. Organisations, particularly those involved in policing or protecting the community, should be able to consider information that a reasonable person would consider indicative of a serious risk of harm, regardless of the source of that information. Yet there is a well-documented risk that official information may be misused for personal gain and other reasons. It is for this reason that organisations must ensure there is proper oversight and clear guidance to staff about when access is regarded as appropriate.

2.104 As noted in the 2006 report into *Jenny's case*, unauthorised access or misuse of personal information by public officials may occur for a variety of reasons:

> The literature 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.[138]

2.105 Accordingly, organisations need to have security measures and procedures in place to enable them to, on the one hand, receive and act upon credible information of serious threats of harm and, on the other hand, deter and detect any misuse or unauthorised disclosure of information by employees using their access privileges. Organisations should provide their staff with guidance about when it would be appropriate to access information in response to concerns that the staff member has developed on the basis of information obtained in their private capacity. The *Information Privacy Act* is not intended to deter the vigilance and community commitment that trained professionals may exercise on the basis of information that comes to their notice in their private lives. The IPPs require care when acting on such information, so that all relevant interests are balanced, including the protection of a well-meaning staff member from later accusations of wrongful use of databases.

2.106 Factors relevant to determining whether the official's use or disclosure is necessary to lessen or prevent a serious harm might include:

a the reliability of the information obtained in the official's private capacity;

b the seriousness of the potential harms;

c the degree of vulnerability of the potential victims (including whether they are in a position to recognise the threat themselves); and

d the involvement of an appropriate authorised person.

2.107 An initial access to official information may be appropriate, provided that the official is authorised to access the information and believes that the access is necessary to assess a reasonably suspected threat of serious harm. Subsequent use of that information by an official acting in their private capacity, however, is unlikely to be authorised. Any use or disclosure within or outside of the organisation must be in accordance with the organisation's functions and in compliance with its legal obligations and its own specialised protocols. It is prudent for officials in circumstances such as these to ensure that they keep an accurate record of their activities and consult a supervisor. Both steps will usually assist if they are later called on to explain their actions, either because of a complaint or following an audit.

Anticipating the need to provide information during an emergency

2.108 Where a serious threat to public health or safety is involved, say, an infectious disease or large-scale evacuation, significant amounts of personal information could be at stake. Steps to ensure limited disclosure consistent with the circumstances, which may require prompt and effective action in an emergency, will need to be considered. Threats to health, safety or welfare in this context will generally require a fast and appropriate response from the organisation. Accordingly, it is advisable to have a policy in place before it happens, and tell people about it. That way the organisation can quickly and confidently handle a request for personal information in an emergency situation. Such a policy may include an escalation process for dealing with such disclosures and a guide for determining who makes the disclosures, what information is likely to be released, and to whom.

2.109 For guidance on developing a plan to respond to potential information requests by emergency services, see OVPC's *Emergencies and Privacy* Information Sheet 02.10.[139] This Information Sheet deals with the relevant IPPs in emergency contexts, establishing emergency policies and protocols, planning checklists and draft protocols for data sharing in an emergency.

Using or disclosing during emergency relief efforts

2.110 IPP 2.1(d) may also be relevant to information uses and disclosures after a disaster or accident has occurred, to assist in emergency response efforts such as locating victims and reuniting them with their family, ensuring victims receive medical attention and ensuring they have the opportunity to take advantage of various other forms of support (such as financial assistance and counselling).

2.111 Disclosure of this type is also likely to be permitted under IPP 2.1(d) as lessening or preventing serious harm to public welfare. A proper conception of "public welfare" in this context includes offering assistance to victims, to assist the community more generally to overcome the effects of disasters and other trauma that occurs in its midst. It is legitimate for authorities to try to reach victims to offer support. But authorities have to be aware that not everyone responds to particular authorities in the same way. Disaster victims can always decline offers of support made by or on behalf of government agencies, and their wishes for no further contact should be respected.

Other IPP 2 grounds may be relevant in emergency situations

2.112 Organisations should also recall that personal information may be used by reference to other parts of IPP 2, such as where the use is for the primary purpose of collection or for a reasonably expected related purpose (IPP 2.1(a)). For instance, travellers who provide agencies with the contact details for their next of kin do so in order to enable contact to be made in case of emergency. During an emergency it would be in line with the primary reason for collecting these details for those details to be disclosed to proper authorities and used to assist in informing families in appropriate ways, and for victim identification and other relevant disaster response work.

2.113 Where personal information is sought after an accident or disaster occurs, such as passenger or guest lists, IPP 2.1(a) would allow that information to be disclosed to relevant agencies involved in emergency response and recovery efforts. Individuals caught up in a disaster would reasonably expect their information to be shared in order to locate, identify and assist them and their loved ones. In this context of disaster response, privacy must be assessed in relation to the emergency at hand. Bodies have to be identified promptly; missing or incapacitated persons need assistance quickly; and in many situations, the persons closest to the persons affected can provide authorities with important help in these tasks. In practice, this means prompt access to personal information about those affected for the proper authorities so that they can make necessary responses to an emergency.

IPP 2.1(e): Investigating suspected unlawful activity

2.114 Where an organisation has reason to suspect that unlawful activity has been, is being, or may be, engaged in, IPP 2.1(e) allows personal information to be used or disclosed:

a as a necessary part of the organisation's investigation of the matter; or

b in reporting the organisation's concerns to relevant persons or authorities.

2.115 This ground for use and disclosure should not be used lightly as it has serious privacy implications. It should not be used for speculative monitoring, surveillance or intelligence gathering. There should be some credible basis for the suspicion.

Unlawful activity

2.116 The activity being investigated must be unlawful, not simply unethical or objectionable. Clearly, suspected breaches of the criminal law would fall within the meaning of "unlawful activity".

2.117 Misconduct by public sector officials may be considered unlawful if it contravenes a statutory secrecy or confidentiality obligation. Examples of such obligations include those provisions that make it an offence to misuse information acquired when carrying out official duties, for example section 95 of the *Constitution Act 1975* (Vic).[140] Additional examples of statutory confidentiality or secrecy obligations were referred to in the earlier discussion in the Overview section (para 16). Misconduct may also be considered unlawful if (consistent with other provisions in the *Information Privacy Act* that refer to the investigation of unlawful activity in similar terms[141]) it involves conduct that may result in the imposition of a penalty or other sanction, such as the types of misconduct[142] set out in the *Public Administration Act 2004* (Vic) – see Case Study 2-10.

CASE STUDY 2-10: Disclosure during investigation of serious misconduct allegations[143]

The complainant, an employee of the Department, was the subject of serious misconduct allegations. The Department disclosed personal information (including his bank account and holiday and sick leave details) about the employee to an external investigator for the purposes of enquiring into the alleged misconduct. The Department also appointed a review panel to independently assess the investigator's report.

The Department argued that IPP 2.1(e) applied to its investigation of allegations of misconduct by the complainant because that conduct raised issues of breaches of the Code of Conduct provisions, given legislative force under the *Public Sector Employment and Management Act 1998* (Vic) [which was later replaced by the *Public Administration Act 2004* (Vic)], and section 95 of the *Constitution Act 1975* (Vic).

The Privacy Commissioner considered that IPP 2.1(e) permits the use and disclosure of personal information at any stage of an investigation into serious misconduct for the purposes of determining whether the suspected activity is taking place. While noting that it is likely for disclosures during an investigation to involve a mix of personal information that may or may not be relevant to the investigation, in this case, the information was necessary to the investigation. Accordingly the Privacy Commissioner declined the complaint on the basis that there had not been an interference with privacy.

However, to avoid future confusion, the Department decided to amend its serious misconduct policy to expressly state that an employee's personnel file could be disclosed to an internal or external investigator for the purpose of understanding an allegation of serious misconduct.

Investigation by the organisation

2.118 When an organisation proposes to use or disclose personal information in order to investigate the matter itself:

a any suspicion of wrongdoing should be based on reasonable grounds, not just unsubstantiated gossip or rumour;

b the use or disclosure must be considered necessary after due consideration of alternatives;

c the use or disclosure should be as confined as possible throughout the organisation's investigation, both in terms of the number of individuals whose information is involved and the number of people who are given access to the information.

2.119 Personal information may be used or disclosed at any point during an investigation into unlawful activity or serious misconduct – see Case Study 2-10.

Disclosure to relevant persons and authorities

2.120 When an organisation decides to report suspected unlawful activity, such use or disclosure should be limited to the persons or authorities with a need to know the information because they have relevant duties to perform in the circumstances. Examples include law enforcement organisations, an organisation responsible for the protection of public revenue, such as the State Revenue Office, or regulatory authorities such as the Food Safety Council.

IPP 2.1(f): Required or authorised by law

2.121 IPP 2.1(f) allows personal information to be used or disclosed otherwise than for the primary purpose if such use or disclosure is required or authorised by or under law. This principle is consistent with section 6 of the *Information Privacy Act* in that other more specific laws dealing with use and disclosure will prevail.

Required by law

2.122 "Required by law" means there is a legal obligation to use or disclose personal information in a particular way.[144] Words such as "must" or "shall" will indicate a requirement, and may be accompanied by the presence of a sanction for non-compliance. Warrants, court orders and statutory provisions are examples. One type of statutory provision that is often relevant to IPP 2.1(f) is the power to demand the production of documents or information – see Case Study 2-11.

CASE STUDY 2-11: Responding to a demand for the production of documents[145]

The complainant and several other people had written letters to a Statutory Body about a company that was licensed by the Statutory Body. Some of the letters contained information about the complainant as well. The Statutory Body noted these letters in its file on the licensed company. At a later date, the company went into liquidation and the court-appointed liquidator gave notice to the statutory entity that it required it to produce all documents relating to that company.

Due to the delicate nature of many of the letters, the Statutory Body contacted the liquidator to check whether it was required to produce *all* the documents it held on the company, including the letters. The liquidator assured the Statutory Body that it was required to produce *all* documents and correspondence. Prior to producing (disclosing) the letters, the Statutory Body required the liquidator to sign a confidentiality agreement limiting the use and disclosure of the information (and requiring its return at a later date).

The complainant discovered that the liquidator had obtained the letters and filed a complaint, arguing that the production of documents required by the liquidator was confined to "company books" and not letters written about the company to the Statutory Body.

The Privacy Commissioner considered that whether the disclosure permitted under IPP 2.1(f) turned on the correct legal interpretation of the scope of the liquidator's powers under section 530B of the *Corporations Act* and, as such, was a matter best determined by VCAT. The matter, however, was not referred to VCAT because the parties were able to resolve their differences. The Statutory Body has since amended its policy to seek legal advice before producing personal information pursuant to any statutory requests.

2.123 Also see *Dodd v Department of Education and Training (General)* [2005] VCAT 2207, where VCAT found that the Department's disclosure of two documents to the Victorian Institute of Teaching (VIT) fell squarely within IPP 2.1(f). The two documents consisted of Mr Dodd's exchange of letters with a teacher about the veracity of her evidence before a disciplinary hearing held by the Department in relation to the conduct of another teacher. VCAT found the disclosure was in accordance with section 27(2) of the *Victorian Institute of Teaching Act 2001* (Vic) which requires the Department to provide the VIT with any information the VIT might reasonably require to conduct its enquiry. The Department was acting under a mandatory duty to provide the information.

Authorised by law

2.124 "Authorised by law" means that while the law permits the use or disclosure, it does not make either compulsory. Words such as "may" are indicative of this, and discretionary powers may be involved. An authorising power must be reasonably specific; a general power or function for "anything incidental" would be insufficient.

2.125 Authorisation under law need not be confined to a specific statutory duty under an Act, but may extend to other common law duties or authorities for disclosure, such as common law rules of evidence – see Case Study 2-12.

> **CASE STUDY 2-12: Disclosing information to court officers permitted**[146]
>
> In a pre-hearing conference, a Local Council disclosed personal information about the person bringing the action against the Council. The person claimed that the disclosure in the pre-hearing conference was an infringement of his privacy. The Local Council asserted that the disclosure was authorised by law under IPP 2.1(f).
>
> The Privacy Commissioner determined that the law permits, and in some cases requires, persons to give information to officers of the court, or evidence to a court about matters relevant to a case. It is the person presiding over the pre-hearing conference or the hearing who decides what is relevant. Accordingly, the Privacy Commissioner considered the disclosure to be a permitted disclosure under IPP 2.1(f).

2.126 Also see *Re: An application by the NSW Bar Association* [2004] FMCA 52. In that case, the Federal Magistrates' Court granted leave to the NSW Bar Association to inspect court records to assist them in their investigation into whether an individual was practising law without a practising certificate. The Court held that, leaving aside whether its judicial functions are exempt from the federal *Privacy Act 1988*, its decision to allow the inspection of court records was authorised by or under law as the leave decision was in accordance with the authority set out in Regulation 2.08 of the *Federal Magistrates Court Rules 2001* to grant leave to a person who demonstrated a proper interest in searching or inspecting court documents.

Administrative release of information under s 16(2), FOI Act

2.127 Section 16(2) of the FOI Act authorises organisations to make information (including documents that might otherwise be exempt under the FOI Act) available to the public informally, without requiring individuals to lodge a formal written request for access under the FOI Act, where the organisation can properly do so or is required by law to do so. This procedure for publishing or disclosing documents outside of the FOI Act is sometimes referred to as "administrative release".[147]

2.128 Where the document contains personal information, organisations should be mindful of their obligation under section 33(3) of the FOI Act to, where practicable, notify the person who is the subject of the information and provide him or her with an opportunity to object to any proposed release. This obligation to give notice cannot be ignored when information is administratively released under section 16(2) of the FOI Act. Nor can organisations ignore section 33(3) by purporting to rely on IPP 2 and section 6(2) of the *Information Privacy Act* – see the decision of VCAT in *Smith v Victoria Police (General)* [2005] VCAT 654, where Senior Member Preuss said, at paras 67-70:

> Section 6(2) of the *Information Privacy Act* preserves "any right, privilege, obligation or liability conferred or imposed under that [FOI] Act or any exemption arising" from the provisions of the *Information Privacy Act*. There is another section in the *Information Privacy Act* which specifically deals with the FOI Act (s 12) but it is not relevant to the substantive considerations in this case....
>
> In my view, Mr Smith's right to the lawful application of s 33(3) was paramount to any consideration that might apply under the *Information Privacy Act* by reason of s 6(2) of the *Information Privacy Act*. Similarly, by reason of the same section, the obligation upon the Police to give the applicant relevant notice before disclosure of private information under s 33(3) cannot be ignored by reference to provisions in the *Information Privacy Act* which might otherwise permit disclosure.
>
> In my view, the Police were unable to take advantage of s 6(2) of the *Information Privacy Act* to justify their actions under the FOI Act...

2.129 Section 16(2) of the FOI Act only authorises disclosure where organisations can "properly do so" or are required by law to do so. It would not be "proper" to give access under section 16(2) of the FOI Act where this would involve an unreasonable impact on the personal privacy of an individual or breach of some other legal obligation. In addition to considering obligations under section 33(3) of the FOI Act, organisations should also consider whether it would be proper to release information having regard to:

a any relevant duties of confidentiality or statutory secrecy requirements; and

b existing legal obligations under the *Information Privacy Act* not to disclose personal information about any person for a purpose other than the primary purpose of collection unless the disclosure is in accordance with IPP 2.1(a)-(h).

2.130 Organisations should note that rights of complaint under the *Information Privacy Act* may become enlivened when an individual's privacy is breached as a result of an administrative release of information under the FOI Act. In *Smith v Victoria Police (General)* [2005] VCAT 654, VCAT accepted jurisdiction under the *Information Privacy Act* where Mr Smith's personal information had purportedly been disclosed under section 16(2) of the FOI Act.

CASE STUDY 2-13: Failure to properly consider FOI Act led to breach of IPP 2[148]

The complainants were engaged in a dispute with a neighbour and, as part of the dispute, had written regular letters to the Local Council requesting Council take action. The letters contained detailed information about the complainants, legal advice and future legal proceedings, information relating to other third parties, conversations with government employees, and information about the complainants' financial position. The complainants had, when writing to Council, included requests that the information be kept strictly confidential.

The neighbour had made an FOI application to Council, who released the documents concerning the above information about the complainants to the neighbour. The complainants only became aware of the release after contact from a third party, and contacted Council, who confirmed release of the documents.

Section 33(1) of the FOI Act states that documents are exempt from disclosure if this would amount to an unreasonable disclosure of a person's personal affairs. Section 33(3) of the Act provides that where a request is made for documents containing information relating to the personal affairs of a third party and it is decided access should be granted, the third person should be notified of the decision and of their right to appeal. This had not occurred.

The Privacy Commissioner decided that, by Council disregarding the provisions of the FOI Act, Council had not treated the disclosure as an FOI matter, rather, the provision of the documents was similar to any other release of information. As a result, the Privacy Commissioner considered that her jurisdiction was enlivened.

Privacy Victoria viewed (referred from the Victorian Ombudsman) approximately 223 pages of documents released by Council to the neighbour under FOI, and considered that about 185 pages released consisted of correspondence between the complainants and Council which raised issues under the IPA. The Commissioner considered that 'in light of the volume, nature and seriousness of the personal information that was disclosed... the release did not appear to be authorised under IPP 2.1.'

Obligations to make documents available for inspection

2.131 IPP 2.1(f) will permit disclosures to be made by organisations acting in accordance with its statutory obligation to make documents available for inspection, as occurred in *Complainant H v Local Council* [2004] VPrivCmr 2. In that case, the Privacy Commissioner found that online publication of the Council's minutes (which included a petition with the complainant's name and address) was permissible under IPP 2.1(f) since the Council was obliged under Regulation 21 of the *Local Government Regulations 2001* (now revoked) to make minutes of ordinary meetings available for public inspection except where meetings were closed to the public. The Privacy Commissioner noted that, in this case, the obligation to make minutes available for inspection was not dependent on anyone making a request for access, nor were there any restrictions on the hours or place at which the minutes could be inspected.

2.132 Similarly, making public registers available for inspection in accordance with statutory obligations will fall squarely within IPP 2.1(f). Organisations should look carefully at the extent of their obligation to determine whether a disclosure requires a request to first be made, or whether the disclosure is restricted in time or place. An authority to make documents available for inspection during office hours at the organisation's place of business will not, for instance, justify wider dissemination (such as "24/7" publication over the internet to the world at large) or dissemination of excessive information (such as full records when the legislation only requires or authorises extracts to be made available). For more guidance on complying with privacy obligations when making public registers available for inspection, see the OVPC's guidelines, *Public Registers and Privacy – Guidance for the Victorian Public Sector*, August 2004.

Disclosing only to the extent required or authorised

2.133 In some cases, the legislative authority behind the information request or demand may be conditional or limited in some way. For example, the legislation may require an investigation to be formally established before a demand for information can be issued to obtain information to assist in that investigation. The amount of information authorised to be sought may be privileged from disclosure, or disclosure may be limited to what is necessary to satisfy the authority underpinning the demand or request – see Case Study 2-14.

CASE STUDY 2-14: Publication of personal details in tribunal decision not authorised or required by law[149]

The Commonwealth Administrative Appeals Tribunal ("the AAT") considered the federal equivalent to IPP 2.1(e) to determine how much information should be included in a published AAT decision. In that case, the applicant's daughter was searching for her family name on the internet when she came across an AAT decision on AustLII. The decision related to her father's application to the AAT to review a Department of Employment, Education and Training decision that he not be paid Austudy at the student homelessness rate. The decision revealed quite explicit details, including addresses of relevant persons and details of the applicant's relationship with his parents.

The AAT considered principles of open justice and its statutory obligations under the *Administrative Appeals Tribunal Act 1975* (Cth) to hear matters in public and to publish its reasons for decisions. The AAT found that its decisions need only publish as much of a person's information as is necessary to disclose adequately the intellectual process that resulted in the particular decision.

In the applicant's case, the AAT had gone beyond what was necessary to fulfil its obligations and may exercise its power under the AAT Act to restrict access to personal information. Accordingly the AAT made an order to restrict publication of the addresses of the applicant and his parents as not being authorised or required under law.

IPP 2.1(g): Reasonably necessary assistance for law enforcement and protection of public revenue

2.134 IPP 2.1(g) allows an organisation to use or disclose personal information where the organisation reasonably believes that the use or disclosure is reasonably necessary for any of five specified purposes undertaken by or on behalf of a law enforcement agency:[150]

a the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;

b the enforcement of laws relating to the confiscation of the proceeds of crime;

c the protection of the public revenue;

d the prevention, detection, investigation or remedying or seriously improper conduct; or

e the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

2.135 If an organisation uses or discloses personal information to assist law enforcement agencies for any of the above purposes, IPP 2.2 requires the organisation to make a written record of that use or disclosure. This obligation to maintain records is discussed at paras 2:164-2:165.

What is a "law enforcement agency"?

2.136 IPP 2.1(g) authorises disclosure to law enforcement agencies. "Law enforcement agency" is defined in section 3 of the *Information Privacy Act*. The definition specifically includes state and federal police; crime commissions and examiners; the Business Licensing Authority, and the Special Investigations Monitor. The definition also includes agencies involved in the prevention and detection of crime; the release of persons from custody; the execution of warrants; the provision of correctional services; the management and seizure of property under confiscation laws; and the protection of public revenue.

2.137 IPP 2.1(g) also authorises disclosure to persons who carry out any of the five functions (listed in the previous section) on behalf of the law enforcement agency. This would include, for example, lawyers preparing matters for trial on behalf of a law enforcement agency. See, for example, the suggestion that the Victorian Government Solicitor's Office might be regarded as a "law enforcement agency" when acting as an agent for the Medical Practitioners Board during the Board's hearing into the conduct of a medical practitioner: *CT v Medical Practitioners Board of Victoria (General)* [2005] VCAT 1810.

Specified law enforcement purposes

2.138 Although the range of authorised recipients is broad, the authority to disclose under IPP 2.1(g) is limited. The use or disclosure must be tied to one of the five specified purposes, set out below.

IPP 2.1(g)(i): prevention, detection, investigation, prosecution or punishment of crime and other breaches of the law

2.139 IPP 2.1(g)(i) allows information to be used or disclosed for the purpose of prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction.

2.140 A criminal offence is an act or practice that is prohibited by criminal law at Commonwealth, State or Territory level. Many offences are created by the laws that are administered by the law enforcement agencies, for example fisheries offences enforced by officers appointed by the Department of Primary Industries. If in doubt ask the requester for details of the offence.

2.141 "Penalty" generally refers to a punishment, including a fine or monetary payment. "Sanction" generally refers to some other legal requirement, order or action utilised to punish non-compliance with a law. Common sanctions may include revocation of a licence, withdrawal of a benefit, or disciplinary actions (such as suspension or dismissal).

2.142 In *Complainant AB v Victoria Police* [2006] VPrivCmr 3, fingerprints obtained from applicants for firearms licences, such as the Complainant, were stored on the national fingerprints database and routinely compared to those found at crime scenes across Australia. The Privacy Commissioner decided that the use by police of personal information of firearms licence holders could be held and used for the investigation of criminal offences.

IPP 2.1(g)(ii): enforcement of crimes confiscation laws

2.143 Laws relating to the confiscation of the proceeds of crime include the *Confiscation Act 1997* (Vic) and comparable laws in other States, Territories and in the Commonwealth. These laws allow for the seizure and confiscation of property and other proceeds that are derived from the commission of criminal offences.

2.144 In Victoria, the agency responsible for enforcing confiscation orders is the Asset Confiscation Office, which is a business unit within the Enforcement Management Division of the Department of Justice.

IPP 2.1(g)(iii): protection of the public revenue

2.145 The meaning of "public revenue" was considered in the New Zealand case of *Woman complains process server revealed debt details at old address* (Case Note 2663) [1998] NZPrivCmr 6. In that case, the NZ Privacy Commissioner referred to the ordinary dictionary meaning of "revenue" and decided that the term did not include recovery of an occasional overpayment made by a government department:

> The agency also submitted that the disclosure was necessary for the protection of public revenue (principle 11(e)(iii)). As the debt was an overpayment by a government department, it believed the process server was recovering public revenue.
>
> The Oxford English Dictionary defines revenue as "annual income, especially that of the state or government institution". "Income" is in turn defined as "periodical, especially annual, receipts from one's work, lands and investments", so an essential characteristic of "revenue" is regular payments to a person or agency. In view of this, I did not consider that the occasional recovery of an overpayment could be viewed as revenue. I formed the opinion that the recovery of overpaid expenditure was not the revenue Parliament intended to protect by this exception.

2.146 "Public revenue" refers to regular payments to Commonwealth, State, Territory and Local Governments, such as taxes (including excise and duties), levies, rates, application fees, and charges. The term may not encompass fines enforcement, as fines are not regular payments made to a government agency. However, as discussed below, IPP 2.1(g)(v) may provide a basis for use and disclosure in the fines enforcement context.

IPP 2.1(g)(iv): prevention, detection, investigation or remedying of seriously improper conduct

2.147 "Seriously improper conduct" refers to serious breaches of standards of conduct associated with a person's duties, powers, authority and responsibilities. It includes corruption, abuse of power, dereliction of duty, and breach of obligations that would warrant the taking of enforcement action by an enforcement body.

2.148 The types of activities or behaviours that constitute seriously improper conduct, or misconduct, are in some cases set out in statutes that apply to specific organisations or the public service as a whole. For instance, section 86A of the *Police Regulation Act 1958* (Vic) sets out the types of activities that would constitute "serious misconduct" in relation to members of the police force, while section 22 of the *Public Administration Act 2004* (Vic) lists the types of activities that would be regarded as "misconduct" by public sector employees.

2.149 A number of statutory agencies exist to investigate allegations of serious misconduct, particularly where they concern individuals engaged in regulated professions such as teachers, lawyers and health professionals.

IPP 2.1(g)(v): preparation and conduct of court or tribunal proceedings, or implementation of the orders of a court or tribunal

2.150 Use and disclosure under this heading would include proceedings in the courts and tribunals of Victoria, other States and Territories, and the Commonwealth.

2.151 The Sheriff's Office, for instance, is empowered by a number of statutes to implement orders of courts and tribunals, including the enforcement and recovery of fines and orders for the payment of money.[151]

2.152 Uses and disclosures of personal information to a law enforcement agency that is empowered to implement the orders of a court or tribunal requires a clear link to the order that is being enforced. Any disclosure should be limited in scope to what is necessary and relevant in each case. This ground should not be used as a basis for the bulk release of information about individuals who are not subject to the orders which are being enforced.

Reasonably believe that disclosure is reasonably necessary

2.153 Organisations are not prevented by the *Information Privacy Act* from continuing, as they did before the *Information Privacy Act* came into force, to cooperate with police and other law enforcement agencies in their investigation of criminal activities. IPP 2.1(g) expressly authorises organisations to assist police and a range of other law enforcement agencies by providing information relevant to a number of broadly-worded law enforcement functions. IPP 2.1(g) requires, however, that organisations consider the reasonableness of their actions before handing over personal information. The tests of "reasonable belief" and "reasonable necessity" must be satisfied.

2.154 Organisations must "reasonably believe" that it is "reasonably necessary" to disclose the information for one of the specified purposes. In determining when it is reasonably necessary to disclose, the Explanatory Memorandum to the *Information Privacy Act* suggests:

> Minimal information about the purpose of collection by the law enforcement agency would usually be enough to establish that the disclosure was "reasonably necessary". Organisations may, alternatively, seek guidance from the Privacy Commissioner about what assurance they should require before releasing information to such an agency.

2.155 Organisations are not authorised by IPP 2.1(g) to simply hand over information on request. IPP 2.1(g) requires the organisation to make a judgment about whether the use or disclosure is reasonably necessary in the circumstances. See *Dodd v Department of Education and Training (General)* [2005] VCAT 2207, where VCAT noted that a Department may need to give more consideration to relevance when exercising a discretion to release information under IPP 2.1(g) than it might when responding to a compulsory demand for information under IPP 2.1(f):

> It is a central plank of Dr Dodd's submissions that he considers the Department had a responsibility to consider the relevance of these two documents to the enquiry into [a fellow teacher's] conduct when making the documents available to VIT [the Victorian Institute of Teaching, regulator of the teaching profession]. *While that submission might have force if one were considering IPP 2.1(g), that is not the case with IPP 2.1(f).*
>
> Section 27(2) of the VIT Act requires the department to provide VIT with any information VIT might reasonably require to conduct its enquiry. The mandatory duty imposed on the Department is to provide information, nothing more. It does not impose a duty on the Department to consider matters such as relevance – that rests with VIT. And indeed it would be a strange state of affairs were it not so. VIT is given the power to inquire and it would be an extraordinary fetter on its task if it were only to be given the material the Department considered relevant to the task. VIT is not bound by the Department's findings; it must consider the evidence afresh and come to its own conclusion. Furthermore the remedies available to it are not identical with those provided to the Department. In my view there is absolutely no foundation for suggesting that the department should consider the relevance of documents it makes available to VIT pursuant to the obligation cast on it by section 27. [emphasis added]

2.156 The organisation should take steps to satisfy itself that the use or disclosure is reasonably necessary for the specified law enforcement function. The organisation should, at a minimum, satisfy itself of the bona fides of the requester and the request:

a Is the information to be released to an authorised member of a "law enforcement agency" (as defined in s 3 *Information Privacy Act*)? Has the member's identity and authority to make the request been verified?

b Is the information relevant to one of the five purposes specified in IPP 2.1(g)? Has this use been confirmed by the law enforcement agency? What information has been provided to verify that the information is to be used for the stated purpose?

EXTRACT: Assessing a Request from a Law Enforcement Agency – Advice from the Australian Communications and Media Authority

The following guidance is sourced from the Australian Communications and Media Authority (ACMA) *Disclosure of Customer Details under Part 13 of the Telecommunications Act 1977 – Frequently Asked Questions* (December 2010). The guidance is designed for Carriage Service Providers fulfilling law enforcement requests under that Act, which contains a similar requirement to the *Information Privacy Act*.

The requesting agency will typically... provide the carrier with a ...written request that:

- is on the agency's letterhead or logo;
- is signed by an officer or staff member of the agency;
- indicates the level of priority the request should be given
- identifies the specific service(s) (or information) being enquired about
- cites the offence that is being investigated
- provides an assurance that the information will only be used for the purpose(s) for which it is being sought, and will be secured against unauthorised disclosure; and
- is dated and provides return contact details.

Assessing whether disclosure is "reasonably necessary" – Advice from the Australian Privacy Commissioner[152]

...Generally speaking, an organisation can regard a disclosure as "reasonably necessary" if:

- it identifies the requesting officer and which unit of which agency he or she comes from;
- it establishes the reason for request – what is being investigated, at least in broad terms and why the information is necessary to that investigation;
- it establishes the identity and contact details of a senior officer at the agency who can verify that the request is being made in connection with a legitimate investigation; and
- the information requested is sensitive or if a large amount of personal information is involved or if the requesting officer has not made sufficiently clear the reason for the request – it has contacted the senior officer to discuss.

Where an organisation frequently discloses information to an enforcement agency, these matters may be dealt with by an agreement between the parties that if specific criteria are satisfied in requesting the information it will be regarded as "reasonably necessary".

Organisations are not obliged to disclose information under these sections of the [*Telecommunications Act*] if they are not satisfied that the use or disclosure is reasonably necessary. It is the Privacy Commissioner's view that organisations should take seriously their obligation to make decisions about whether a use or disclosure is reasonably necessary. Organisations are urged to adopt a cautious and accountable approach to the obligation to assess "reasonable necessity". At the same time, there is clear benefit to the community in enforcement agencies having access to information needed to carry out their functions and the Privacy Commissioner would not support unnecessary impediments to this.

2.157 In some cases, organisations may determine that it would not be appropriate to release the information under IPP 2.1(g). This may be because they have not been persuaded that the information is necessary for one of the authorised purposes. Or the organisation may determine that, due to the sensitivity or volume of information requested, it would be more appropriate to withhold the information until and unless a warrant or other legal authority is produced.

2.158 Any use or disclosure of personal information under IPP 2.1(g) must be noted by the organisation in writing (see IPP 2.2, discussed at paras 2:164-2:165). If providing information to a law enforcement agency, organisations should remember IPP 4 (Data Security) and take steps commensurate with the sensitivity of the matter to ensure the information gets securely to the right law enforcement official and, where appropriate, is securely returned or destroyed after use.

IPP 2.1(h): Commonwealth security agencies

2.159 IPP 2.1(h) allows an organisation to disclose information to officers of the Australian Security Intelligence Organisation (ASIO) and the Australian Secret Intelligence Service (ASIS) where the agency has requested the information in connection with its functions and:

a the disclosure is made to an ASIO or ASIS officer or employee who is authorised in writing by the Director-General of ASIO or ASIS to receive the information; and

b the Director-General of ASIO or ASIS has also certified in writing that the disclosure would be connected with the performance by ASIO or ASIS of its functions.

2.160 Organisations need to be satisfied that a request for information is legitimate (see para 2:163) and appropriately documented. IPP 2.1(h) requires written authority identifying the recipient from ASIO/ASIS and certifying that the information is needed for ASIO/ASIS's functions. Organisations should bear in mind that compliance with Parliament's safeguard – the requirement for written authority – is important to complying with the *Information Privacy Act* and preserving the reputation of the organisation should it be audited at any time in future.

Exercising discretion to disclose under 2.1(f)-(g)

2.161 IPPs 2.1(f) and (g) give organisations a *discretion* to disclose where authorised (but not required) by law, or to assist law enforcement agencies in carrying out a number of law enforcement functions. Organisations should always cooperate responsibly with law enforcement agencies, but they need to query them responsibly too. Organisations are not obliged to accede to requests for information or for assistance by law enforcement agencies, unless those requests are backed by a power to compel information (such as under warrant or another enforceable order, made by or under law in the proper form).

2.162 Prior to disclosing personal information under IPPs 2.1(f)-(g), organisations should consider whether the disclosure is in fact required by law. Before releasing personal information, organisations should also consider whether prior notice must or can be given to those individuals whose information is being disclosed, and whether there is any public interest reason to resist or challenge the demand. See, for example, *Royal Women's Hospital v Medical Practitioners Board of Victoria* [2006] VSCA 85, where the hospital (unsuccessfully) challenged the Medical Practitioners Board's search warrant for medical records, arguing that the records were protected from having to be produced on public interest immunity grounds. If in doubt, organisations should seek legal advice prior to disclosure.

Verifying the authority underpinning requests for information under IPPs 2.1(f)-(h)

2.163 When dealing with a request for information or documents under IPPs 2.1(f)-(h), organisations should satisfy themselves that the request is legitimate and the requester is authorised to act on behalf of the organisation that has the authority or demand power. This may entail verifying the identity and authority of the person making the request, for instance by requiring a verbal or written confirmation from a more senior officer in the organisation. The requester should also be able to provide a specific reference to their legislative authority, for instance by stating the section in the relevant Act that they are relying on to authorise or demand the information being sought.

IPP 2.2: Written notes of uses/disclosures under IPP 2.1(g) to law enforcement agencies

2.164 A written note must be made of any disclosure to a law enforcement agency under IPP 2.1(g). The note should specify at least the following information:[153]

a the personal information used or disclosed, with a copy of any material supplied;

b the law enforcement agency or agencies and their representatives' names;

c the basis of the reasonable belief that the use or disclosure was reasonably necessary, taking care not to prejudice any investigation or proceeding; and

d the name and title of the decision-maker.

2.165 Where a law enforcement agency makes a written request for information in a manner that conforms with the suggestions earlier in this section (see paras 2:156-2:158), then the requirements of IPP 2.2 are likely to be met.

IPP 2 Notes

[106] *King v SA Psychological Board* [1998] SASC 6621; *R v AW* [2005] QCA 152.

[107] *Complainant AF v Local Council* [2007] VPrivCmr 1.

[108] *Little v Melbourne CC* (General) [2006] VCAT 2190 (30 October 2006) at 24-25.

[109] Office of the Victorian Privacy Commissioner, *Privacy and School Reports*, Information Sheet 02.02, 8 May 2002.

[110] *Johns v the Australian Securities Commission* [1993] HCA 56 per Brennan J at paras 14-15. Also see Dawson J at para 3, Gaudron J at para 1, and McHugh J at para 9. This case concerned the disclosure of transcripts of evidence by the Australian Securities Commission (ASC) to the Royal Commission into the collapse of the Tricontinental group of companies. The transcripts of Johns' evidence (the managing director of these companies) had been acquired through the compulsory examination powers of the ASC and were subject to confidentiality obligations and strict limitations around use and disclosure. The ASC permitted the Royal Commission to use the material in public hearings, which were then reported by the media. Johns successfully argued that he had been denied natural justice by the ASC in not being provided an opportunity to be heard before they allowed the confidential material to be publicly disseminated so as to prejudice his rights or interests. Public disclosure could prejudice Johns' personal reputation and encroach on his right to maintain silence about the matters being investigated by the ASC. The High Court of Australia held that the ASC's decision to disclose the transcripts to the Royal Commission for use in public hearings was therefore invalid.

[111] Office of the Victorian Privacy Commissioner Information Sheet 02.10, *Emergencies and Privacy*, January 2010.

[112] Office of the Victorian Privacy Commissioner Information Sheet 04.08, *Fences and Privacy*, June 2008.

[113] Explanatory Memorandum, *Information Privacy Bill 2000* (Vic) 28.

[114] *Ng v Department of Education* [2005] VCAT 1054 at paras 89-94.

[115] *Duggan v Moira Shire Council*, Unreported, VCAT, Preuss SM, 11 October 2004, No. G394/2004 at para 35.

[116] Also see *Complainant A v Local Council* [2003] VPrivCmr 1; and Complainant H v Local Council [2004] VPrivCmr 2.

[117] *Complainant D v Minister* [2003] VPrivCmr 4.

[118] *Ng v Department of Education* [2005] VCAT 1054 at para 95.

[119] *Complainant H v Local Council* [2004] VPrivCmr 2.

[120] *Complainant AG v Local Council* [2007] VPrivCmr 2.

[121] *Complainant AC v Public Sector Body* [2006] VPrivCmr 4.

[122] *Complainant AU v Public Sector Agency* [2011] VPrivCmr 3.

[123] Note that, while consent can be used to authorise unrelated secondary uses and disclosures under IPP 2, consent cannot serve as a basis for the collection of information under IPP 1 where that collection is unnecessary or unreasonably intrusive. See the discussion of optional information in the section on IPP 1, at para 1:84-1:85.

[124] Canadian Institutes of Health Research, *CIHR Best Practices for Protecting Privacy in Health Research*, September 2005, available from http://www.cihr-irsc.gc.ca.

[125] See, for instance, the discussion of preserving individuals' right to withdraw from participation in human research at paras 2.2.19-20 in Australia, National Health and Medical Research Council, *National Statement on Ethical Conduct in Human Research*, 2007, available at http://www.nhmrc.gov.au.

[126] Council of Europe, Committee of Ministers, *Explanatory Memorandum to Recommendation No. R (97) 18 of the Committee of Ministers to member states concerning the protection of personal data collected and processed for statistical purposes*, adopted 30 September 1997, para 85(b), available at http://www.coe.int.

[127] Australian Privacy Commissioner, *Public Interest Determination No. 5*, issued 29 April 1991 and tabled 17 June 1991, available at http://www.privacy.gov.au.

[128] Australian Privacy Commissioner, *Public Interest Determination No. 8*, issued 22 March 2002 and tabled 14 May 2002, available at http://www.privacy.gov.au.

[129] Some of these questions are drawn from para 4.4 ("weighing the public interest") in the *Statutory Guidelines on Research* issued by the Victorian Health Services Commissioner in February 2002. Regard has also been given to the discussion of risks and benefits of research (see, eg, Chapter 2.1) in the National Health and Medical Research Council, *National Statement on Ethical Conduct in Human Research*, 2007, available at http://www.nhmrc.gov.au.

[130] Office of the Victorian Privacy Commissioner, *Data Matching in the Public Interest – A guide for the Victorian public sector*, Edition 1 – August 2009, page 5.

[131] Office of the Victorian Privacy Commissioner, *Data Matching in the Public Interest – A Guide for the Victorian PublicSsector*, Edition 1 – August 2009, p 14-15.

[132] Office of the Victorian Privacy Commissioner, *Data Matching in the Public Interest – A Guide for the Victorian public sector*, Edition 1 – August 2009, p 14-15.

[133] *Information Privacy Act 2000* (Vic) s 58(m) requires the Privacy Commissioner to monitor data-matching and data linkage to ensure any adverse effects on privacy are minimised. However, the Privacy Commissioner does not have a power to make "public interest determinations" similar to the power of the Australian Privacy Commissioner (*Privacy Act 1988*, Part VI). The Australian Privacy Commissioner can determine that the public interest in an agency's act or practice outweighs to a substantial degree the public interest in the agency adhering to the relevant Privacy Principle.

[134] Federal Privacy Commissioner (Moira Scollay), "Guidance notes to the principles" in *National Principles for the Fair Handling of Personal Information*, January 1999, pages 18-20.

[135] *M v Department of Human Services* (General) [2009] VCAT 456 (23 March 2009).

[136] The additional requirement for necessity was regarded as "clearly a tougher requirement" by the New South Wales Administrative Decisions Tribunal Appeal Panel in *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77 at para 69.

[137] *NS v Commissioner, Department of Corrective Services* [2004] NSWADT 263.

[138] Office of the Victorian Privacy Commissioner, *Jenny's case: Report of an investigation into the Office of Police Integrity pursuant to Part 6 of the Information Privacy Act 2000*, Report 01.06, February 2006, page 15 (endnotes omitted).

[139] Available from http://www.privacy.vic.gov.au.

[140] Section 95 of the *Constitution Act 1975* (Vic) prohibits officers in the public service from (a) publicly commenting upon the administration of any department of the State of Victoria; (b) using except in or for the discharge of his official duties any information gained by or conveyed to him through his connexion with the public service; or (c) directly or indirectly using or attempting to use any influence with respect to the remuneration or position of himself or of any person in the public service.

[141] See the definition of "law enforcement agency" in section 3, *Information Privacy Act 2000* (Vic), and references in IPP 2.1(g) and (i) to the investigation of criminal offences or breaches of a law imposing a penalty or sanction.

[142] Section 22 of the *Public Administration Act 2004* (Vic) defines "misconduct", for which penalties (including a salary reduction, demotion, suspension or dismissal) may be imposed, to include: (a) a contravention of a provision of the Public Administration Act, the regulations or a binding code of conduct; (b) improper conduct in an official capacity; (c) a contravention, without reasonable excuse, of a lawful direction given to the employee as an employee by a person authorised (whether under this Act or otherwise) to give the direction; (d) an employee making improper use of his or her position for personal gain; (e) an employee making improper use of information acquired by him or her virtue of his or her position to gain personally or for anyone else financial or other benefits or to cause detriment to the public service or the public sector.

[143] *Complainant I v Department* [2004] VPrivCmr 3.

[144] In *Secretary, Department of Premier and Cabinet* v *Hulls* [1999] 3 VR 331 per Phillips JA at 342 suggested that "requires" means demands or necessitates.

[145] *Complainant J v Statutory Entity* [2004] VPrivCmr 4.

[146] *Complainant A v Local Council* [2003] VPrivCmr 1.

[147] See, for example, Victorian Ombudsman, *Review of the Freedom of Information Act*, discussion paper, May 2005, available at http://www.ombudsman.vic.gov.au, pages 44-46.

[148] *Complainants AI v Local Council* [2008] VPrivCmr 1.

[149] *Tam Anh Le v Secretary, Department of Education, Science and Training* [2006] AATA 208.

[150] Section 3 of the *Information Privacy Act 2000* (Vic) defines "law enforcement agency" and s 13 exempts law enforcement agencies, where necessary, from compliance with parts of six IPPs for four stated reasons.

[151] See, for example, section 111, *Magistrates' Court Act 1989* (Vic); and section 62, *Sentencing Act 1991* (Vic).

[152] This advice was provided by Australia's second Federal Privacy Commissioner, Moira Scollay, to the Australian Communications Authority (now the Australian Communications and Media Authority) *Telecommunications and Law Enforcement Manual*, July 1998 (Manual is currently under review).

[153] Although IPP 2.2 does not specify what should be included in a written note, the organisation should include enough information so that the organisation is in a position to retrieve the personal information, as and when appropriate, and fulfil its obligations under IPP 3 and IPP 4.

IPP 3: Data quality

3.1 IPP 3 is aimed at keeping quality of personal information high. It states:

> An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

3.2 Personal information gathered by government forms the basis of decisions, many of which affect the lives of the individuals concerned or the community generally. Decision-making is likely to be better if it is based on accurate, up to date information. Many people think of privacy protection as being exclusively about preventing improper use or disclosure of personal information. But even where personal information is properly used or disclosed, it can do harm if it is wrong or out of date.

3.3 The importance of data quality to decision-making was acknowledged by the New South Wales Administrative Decisions Tribunal Appeal Panel:

> ...the use of data for the purpose for which it was collected will often involve the taking by the agency of some significant decision affecting the interests of the individual. Therefore the use should ensure that data quality principles are observed.[154]

3.4 Note that where the word "quality" is used in these Guidelines, it refers collectively to the states of being accurate, complete and up to date.

"Accurate" and "complete"

Accurate

3.5 Accurate means "free from error or defect" or "in exact conformity to truth, to a standard or rule".[155]

3.6 "Inaccuracy" under IPP 3 will cover personal information that is factually erroneous. It will also cover opinions based on, or conclusions drawn from, erroneous facts.[156] Wrongly addressed personal correspondence and misspelt names are examples of factually inaccurate personal information[157] (see Case Study 3-1).

CASE STUDY 3-1: Incorrect address recorded resulted in disclosure[158]

In 2006 the complainant was contacted by the Department and asked to provide address details for a specific purpose. The Department also contacted the complainant's relative and asked for that relative's address for the same, specified purpose.

In 2007, a representative of the Department attended the complainant's relative's residence and attempted to serve a subpoena on the complainant. The complainant's relative advised that the complainant did not reside, and had never resided, at the address. The complainant subsequently contacted the Department to complain about the matter. The Department informed the complainant that the relative's address was the address it had on record as the complainant's address. The complainant again provided the correct address to the Department.

Later in 2007, the complainant wrote to the Department and provided a postal address as the address for return correspondence. In early 2008, the Department wrote a letter of response to the complainant and sent it to the complainant's relative's (now former) residential address. The letter contained detailed and delicate information relating to the complainant.

The complainant made a complaint to the Privacy Commissioner under IPP 3.

The Department acknowledged that correspondence for the complainant had been sent to the complainant's relative's former address in spite of being informed by the complainant that this was not the correct address. The Department also acknowledged that the complainant's address could have been verified prior to sending a representative to serve the complainant with a subpoena.

The Privacy Commissioner considered that the Department's failure to correct and update the complainant's address information raised issues of data quality under IPP 3. At conciliation, the Department agreed to make a note on the complainant's file to verify the accuracy of the complainant's contact details prior to sending any future correspondence. In addition, the Department agreed to undertake a data cleansing exercise to ensure the accuracy of all the personal information contained on the complainant's file.

3.7 Information that is attributed to the wrong person will also be regarded as inaccurate (see Case Study 3-2).

CASE STUDY 3-2: Surveillance records created about the wrong person[159]

A Government Department received a claim for compensation from the complainant's same sex partner. In order to assess the validity of the claim, the Government Department engaged a Contracted Service Provider to undertake surveillance of the claimant. The Government Department gave the Contractor a physical description of the claimant, whose physical features were significantly different from that of her partner (the complainant).

The Contractor undertook surveillance for use in assessing the compensation claim, but mistook the complainant for her partner. The report included detailed information obtained in the course of surveillance about the complainant's movements, activities she engaged in with her children, and other activities over a 48-hour period.

The Privacy Commissioner considered that, as the contractor had collected information about the complainant in connection with the claim, and had wrongly attributed this information, the information it had collected was not accurate.

Complete

3.8 Complete means "having all its parts or elements; whole; entire".[160] The application of the word "complete" will depend on the specific information, context and purpose. As with accuracy, the obligation to hold, use and disclose complete information will arise where the information would give a misleading impression to others or lead them to make incorrect decisions, if not for the missing information. Case Study 3-3 illustrates this:

CASE STUDY 3-3: Incomplete address information[161]

The complainant entered into a loan agreement with a finance company for the purchase of a motor vehicle. The complainant repaid the loan by regular direct debit. Before the loan was repaid in full the direct debit arrangement ceased. The complainant was unaware that the account had fallen into arrears until he found a default listed on their consumer credit file. The complainant also claimed that he had not received any notification from the finance company of the amount outstanding or of the finance company's intention to list the default on his consumer credit file (as required under 18E(8)(c) of the *Privacy Act 1988* (Cth) and paragraph 2.7 of the *Credit Reporting Code of Conduct*).

The Privacy Commissioner found that when the complainant's account fell into arrears the finance company had attempted to contact him by writing to him at his last known address. However, during the investigation it became apparent that the address used by the finance company was incomplete. The finance company had omitted enough information from the address so that it was unlikely that the complainant could have received the letters advising him the account was in arrears and that the default would be listed on his credit report.

The finance company agreed to contact the credit reporting agency and ask that the listing be deleted. The credit reporting agency subsequently removed the payment default listing.

3.9 Although information held by an organisation may be "true and correct", that information may be incomplete by omitting subsequent events. The Australian Privacy Commissioner has stated:

> The obligations in NPP 3 [Data Quality principle] go beyond requiring organisations to take reasonable steps to make sure personal information is correct. They must also take reasonable steps to make sure personal information is complete and up to date. In my view, a listing [on a Tenancies Database] might be "true and correct" but be incomplete, for example because it notes that a debt of X amount was owed but does not note that it has since been paid, or be out-of-date because it relates to very old events.[162]

Inaccurate opinions

3.10 The definition of "personal information" in section 3 makes it clear that inaccurate or untrue opinions will fall within the ambit of the *Information Privacy Act*.

3.11 Incomplete or inaccurate opinions are those that demonstrate a "total inadequacy of underlying factual information" as well those which are based on "bias or ill will, incompetence or lack of balance or necessary experience in the person forming the opinion, or the existence of such a trivial factual substratum as to render the opinion formed dangerous to rely upon and likely to result in error, or where facts have been misapprehended."[163]

3.12 In order for an opinion to be considered 'inaccurate' or 'incomplete' under IPP 3, the steps that an organisation has taken to ensure accuracy will often be determinative. For example, where an organisation has come to an 'informed opinion' by taking into account competing facts and/or views of relevant parties before reaching its final opinion, this will usually be enough for the opinion to be considered 'accurate' or 'complete' under IPP 3. An opinion will not be inaccurate under IPP 3 simply because the person the opinion relates to disagrees with it. (For further discussion, see paras 3:21-3:28 regarding reasonable steps).

Considerations in ensuring accuracy

3.13 The first step in recording data should be to ensure the information itself is accurately recorded. If the information is an opinion, it should be stated as such and if possible, the name of the person holding that opinion should also be recorded.

3.14 Where appropriate, an opinion may need to be amended. If the factual basis of the opinion is found to be flawed, but it is impracticable or inappropriate for the opinion to be amended, it would be a reasonable step in the circumstances for an organisation to ensure that the flawed basis is recognised as such, particularly if the organisation uses the opinion. If the flawed opinion is disclosed, the organisation should ensure that the fact of the flawed basis of the opinion is pointed out to recipients.

3.15 Part V of the FOI Act provides for the addition of a notation to a disputed opinion so that, while the integrity of a file is maintained, the contrary view, perhaps now based on better or more complete factual information, is also available to future decision makers.[164] This is a way to deal with vexed situations in which two appropriately qualified persons give conflicting opinions on the same matter.

3.16 For more guidance on the relationship between IPP 3 and IPP 6, see the discussion at paras 6:74-6:75.

Practical tips

Some practical tips for ensuring data accuracy:

Names: Take care with people's names. Don't make assumptions. Think how you feel when someone gets your name wrong. If a person tells you their name over the phone or from the other side of an enquiries counter, spell the name back to them to check that you've entered it correctly. Be alert for names with varied spellings but the same sound, like Jon/John, Catherine/Kathryn and Stuart/Stewart.

Spelling: Repeat initials and unclear letters when taking down personal information over the phone – P for Peter, D for Delta, M for mother, N for nervous, etc. But be careful that phrases like "R for Robert, Smith" don't end up as "Arthur Robert Smith".

Precision: Be precise. Vagueness and ambiguity will cause problems later. When you key in relevant details about a phone conversation or interview in which you were a participant, you will need to be clear not just for your own future reference, but for others who were not participants but who use the data later. A file note that can be read two ways (one of them adverse) can cause problems for others. Distinguish fact from opinion.

Check: The best person from whom to get personal information about an individual is that individual. Be wary about using second- or third-hand information about people without checking it. Other agencies or individuals may have different work tasks and may not need to be as precise about the personal information as you do for your job role.

Warn: If you can't check it, qualify it accordingly so that the next user of the information is put on notice that it still needs checking (especially if it may adversely affect the person it's about). If the quality of the data is questionable, qualify it accordingly.

Addresses: Accurate addresses avoid accidents and acrimony. A misspelt street name or a wrong house or flat number can result in a letter never reaching its intended recipient. Worse, the letter might be opened and read by someone it is not meant for, and they may know the person it was meant for, which can worsen the privacy breach.

"Up to date"

3.17 Up to date means "extending to the present time; including the latest facts".[165] The requirement to keep information up to date is intended to deal with situations in which subsequent information would make the existing record inaccurate or obsolete if it were not added.[166]

3.18 But the fact that personal information relates to an event from the past does not necessarily mean that the information is out of date. For instance, a birth record stating the weight of a newborn will not be out of date simply because time has passed. The information was recorded in accordance with the facts known at the time, for purposes relevant to the circumstances of the birth. If weight becomes important at a later time in the individual's life, more up to date information will of course need to be obtained. The extent to which new information or subsequent events indicates a need to update old information will depend on the purpose for which the information is used or disclosed. As Judge Rendit of the Victorian County Court said:

> Old information may still be accurate and unchanging, such as the place where one is born. The older one gets the further that fact recedes in time, but it never becomes "out of date". Nor, for example, the fact that a person has obtained a particular academic qualification in a certain year or was convicted and sent to prison for a criminal offence. Time does not change these facts.[167]

3.19 Ensuring records are up to date is largely about ensuring they are not likely to convey a misleading impression to others who view the information.

3.20 As the information should be fit for its intended use, it may be appropriate to replace or expunge out of date information, such as when updating mailing addresses – see, for example, Case Studies 3-4 and 3-5. In other cases, record-keeping obligations may require the old information to be retained. In such cases, the old information may be archived or a notation made about its lack of currency.

CASE STUDY 3-4: Use of inaccurate personal information[168]

The complainant had taken out a loan with a bank. He later moved to a new address and notified the bank of the change. Upon defaulting on repayment of the loan, the bank engaged a debt collector and passed on the complainant's personal data, including his old and new addresses. The debt collector sent letters of demand to both addresses, thereby making it known to the new residents at the complainant's old address that the complainant was in debt.

The Hong Kong Privacy Commissioner found that the bank had breached the Data Quality principle in treating the complainant's old address as his correspondence address for debt collection purposes. The bank had no reason to pass on the old address, as it had been communicating with the complainant at his new address and had no reason to believe that he could still be contacted at the old address. The old information should not have been used without checking its currency.

The bank agreed to expunge the complainant's old address from all its records except the original loan application form. The bank also instructed the debt collector to erase the data from its records.

CASE STUDY 3-5: Listing on tenancy database inaccurate and out of date[169]

The complainant rented a property, which was later repossessed by order of the Residential Tenancies Tribunal. The Tribunal also ordered a payment be made to the landlord through the real estate agency managing the tenancy. The responsibility for the property subsequently passed to a second real estate agency, and the Residential Tenancies Tribunal issued a second order for the complainant to make payment, through the original real estate agency.

Almost five years later, the second real estate agency made a listing of the complainant's name on a tenancy database, in relation to the earlier Tribunal orders. The complainant noted that they never had any dealings with the second real estate agency, and contacted that agency to point out the length of time that had elapsed. The complainant raised the issue with the tenancy database.

NPP 3 provides that an organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

The second real estate agency told the Privacy Commissioner that the Tribunal's orders were made in favour of the landlord, not the agency, and that the landlord was entitled to change agents at any time. They added that the delay in listing had been due to the mistaken belief that the complainant had already been listed on the database.

The Commissioner agreed that there was a relationship between the landlord and the agency, but did not agree that there was any relationship between the agency and the tenant. The listing by the second real estate agency onto the database created the false impression of a relationship between the complainant and the agency, and so the personal information could not be considered accurate. In addition to this, the Commissioner found that the length of time which had passed rendered the information out of date as the information was no longer current. As a result of this finding, the tenancy database removed the complainant from their records.

"Reasonable steps"

3.21 IPP 3 does not require organisations to take every possible step to ensure quality, but rather, to take "reasonable steps" to ensure it. Thus the steps that are reasonable in one context will differ from another. The underlying principle is that the personal information should be fit for its purpose.

3.22 The reasonable steps required to ensure data quality in particular circumstances will depend on several factors, including:

a the nature of the information;

b how recently the information was collected;

c how quickly the information can go out of date;

d who provided the information;

e the purpose for which the organisation uses the information;

f to whom the organisation discloses the information;

g how, and for what purpose, the information will be used by the recipient; and

h the consequences for the individuals concerned if the data is not sufficiently accurate, complete and up to date.

3.23 The nature or type of personal information, and the consequences that may flow from poor data quality, are particularly important. Some information, if incorrect when used or disclosed, will merely irritate until it is corrected. For instance, the misspelling of a name or use of an incorrect title. Small inaccuracies will normally not result in any harm, but in some circumstances, they may. Recording the wrong age may impact on someone's concession entitlements. Other categories of information could inconvenience if incomplete or out of date when used, such as a wrong address. Again the potential for harm may not be great where there was simply a delay in receiving wrongly addressed correspondence. On the other hand, a wrong address could result in the intended recipient missing a crucial deadline due to the delay or lack of the letter being forwarded. Or a wrong address could result in a search warrant being exercised at the wrong premises, as occurred in New Zealand in *Baigent's case* – see Case Study 3-6.

CASE STUDY 3-6: Search warrant obtained with respect to wrong address[170]

Police obtained a search warrant for an address occupied by Mrs Baigent, mistakenly believing it was the house of a suspected drug dealer. Upon arrival, police were met by Mrs Baigent's son who contacted his sister, a Wellington barrister. It was alleged that an officer stated in the telephone conversation to Mrs Baigent's daughter, "We often get it wrong, but while we are here we will have a look around anyway." The police then proceeded to conduct a search of the house.

Mrs Baigent sued for damages on a number of grounds, including a claim of a breach of the right to be free from unreasonable search and seizure under section 21 of the New Zealand Bill of Rights. [Note: Section 21 is similar in terms to the right to privacy under section 13 of the Victorian *Charter of Human Rights and Responsibilities 2006*].

The claim was initially struck out on the basis of Crown immunity, where it was argued the Crown is not liable for anything done by its agents in executing a judicial process (here, a search warrant). However, on appeal, the Bill of Rights cause of action (and other actions) were reinstated. The Court of Appeal argued that the Crown's statutory immunity did not provide a good defence and the Crown was liable both vicariously and directly for the conduct of police. The Court read in a requirement of "good faith" in executing the warrant, which had not been met in this case.

NOTE: Although the Court of Appeal decision implied a right to seek damages for a breach of the NZ *Bill of Rights Act*, the Victorian *Charter of Human Rights and Responsibilities Act 2006* expressly provides that a breach of a Charter right will not give rise to damages. Nevertheless, the Charter preserves existing rights to seek compensation apart from the Charter. This would include rights to compensation and other redress under the *Information Privacy Act*. In addition, despite exemptions to some of the IPPs under s 13 of the *Information Privacy Act*, law enforcement agencies must still comply with IPP 3.

3.24 Certain categories of information may seriously disadvantage or humiliate an individual if the information is of poor quality. For example, information about the fact of, and the results of, an investigation into any allegation of improper behaviour needs to be accurate, complete and (especially if there was an appeal) up to date. Where it is part of an organisation's function to publish identifying information about disciplinary matters, publications should be marked with an "accurate at" date or "last revised" date.

3.25 Where information can have adverse consequences for an individual, it will require greater care, meaning greater "reasonable steps" to be taken, in order for the requirements of IPP 3 to be met. For example, organisations should take appropriate steps to confirm the accuracy of the information they use, or the accuracy of facts from which opinions are drawn (eg, where that information may be gathered from several other sources) before making a decision/taking action that will deprive individuals of benefits or result in serious adverse consequences. See the New Zealand privacy case described in Case Study 3-7.

CASE STUDY 3-7: Adverse action based on inaccurate information without providing prior opportunity to comment[171]

A government body administering the New Zealand accident compensation scheme cancelled the complainant's attendant care and home help compensation based on information contained in an assessor's report. The Government Body conceded that the report contained inaccurate information, but argued that it was entitled to rely on the report as the assessor was qualified to provide it.

The New Zealand Privacy Commissioner found that cancelling the complainant's compensation without giving him an opportunity to respond was a serious decision. It would have been reasonable to have given the complainant an opportunity to comment on the report as the Government Body was considering taking adverse action against him. As the government body failed to do so, the Privacy Commissioner found it was in breach of the Data Quality principle.

3.26 Similarly, the Australian Privacy Commissioner has found that, in making an assessment of "reasonableness", it is appropriate to take into account the purposes for which the information is collected and the consequences for the individuals concerned. In the Tenancies Database case (summarised later in Case Study 3-11), the Australian Privacy Commissioner was satisfied that inclusion of a person's details on a tenancy database has an impact on an individual's ability to obtain housing, and this was relevant to assessing whether the steps TICA had taken to ensure data quality were reasonable.[172]

3.27 Organisations should take reasonable steps to ensure that data remains intact during all phases of its handling – from collection, recording and transcription through to its storage and any dissemination. Data quality may be especially vulnerable at times of data entry and photocopying. Mistakes can be made keying in the information, and pages can be lost. Data in digital form may be susceptible to change or loss in ways that paper documents are not. This is in part because technology allows bulk electronic data to be handled in relatively automated ways.

3.28 The integrity of personal information can be maintained by taking various steps to secure the information from unauthorised modification, disclosure, or loss. These steps include periodic checks to assess the accuracy of data entry, publishing documents in a read-only format, use of encryption to securely transmit data, and adoption of technologies that create a log of when information is altered or deleted and by whom. One simple effective way to monitor data quality is to make it a habit to ask subjects of information, in any correspondence with them, to point out whether any of the information in the correspondence needs correcting or updating. Reasonable steps to protect data from unauthorised modification or premature disposal are discussed further in these Guidelines under IPP 4.

CASE STUDY 3-8: Wrong information used for mailing address after shared information arrangement[173]

The complainant had dealings with a Government Agency for a number of years, which had involved the complainant receiving mail through a Post Office Box (PO Box). The complainant then received two letters delivered to their home address rather than the PO Box. The complainant raised this matter with the agency, but was informed that no explanation could be given as the agency had no file record of the complainant's address being changed from the PO Box to the residential address.

The Commonwealth Information Privacy Principle 8 (which applies to Australian Government organisations) provides that a record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that the information is accurate, up to date and complete.

The Government Agency informed the Commissioner that it had an arrangement with two other government agencies to share data regarding mutual clients. As a result of a clerical error while handling some of this shared information, the complainant's residential address was added to their electronic database record in place of the PO Box address.

The complainant was satisfied with the assistance the Commissioner had provided and decided to continue to deal with the matter with the Government Agency directly.

The time for checking accuracy

Old records and archives

3.29 Personal information collected and used for a particular purpose and then archived does not need to be constantly checked for accuracy. Organisations do not have to monitor data quality when information is dormant.

3.30 Data quality should be assessed at some key points, including at the time of collection, when the information is used or re-used, and when it is disclosed to another organisation. Where use is regular or constant, the frequency of monitoring the quality of data will depend in part on the potential for that type of information to lose quality over time.

When disclosing to other organisations

3.31 An organisation must comply with IPP 3 when it collects and uses personal information. However, responsibility for complying with IPP 3 does not end there. If an organisation keeps a record of the information, then IPP 3 duties endure. The organisation also has a duty to consider the quality of the data when and if the information is subsequently used or disclosed.

3.32 The recipient organisation should make corresponding enquiries about the quality of the information received. The recipient will usually be in a weaker position to judge the data's quality than the disclosing organisation. If the recipient organisation is also bound by the *Information Privacy Act* or a similar law, then that organisation will also have data quality responsibilities that will adhere to the information from the time of receipt.

3.33 If it subsequently becomes apparent to either the disclosing or recipient organisation that the information suffers from significant data quality issues, it would be good privacy practice to advise the other organisation accordingly.

Public registers and online information

3.34 Where personal information is made available over the internet, ensuring data quality may require steps to correct not just the information on the organisation's website but to also ensure that other search engines that tap into the site, and archives that store information on it, do not retain the inaccurate data. In other words, inaccurate information, though deleted from an organisations website, may be "cached" on search engines such as Google. This may result in information that is inaccurate or not up to date, remaining publicly available. See Case Study 3-9.

CASE STUDY 3-9: Inaccurate public register information retained in search engine and archive's database, despite being removed from the "official source"[174]

The complainant held a licence in relation to a sensitive trade activity under a statutory scheme. Online Google searches led to results that associated her name with another related and more sensitive trade activity, also regulated by the Statutory Entity. She felt humiliated about being wrongly identified with the more sensitive trade and was concerned about the risk of harm that may result from being identified and then located.

Shortly after receiving the complaint, the Statutory Entity removed its register from the internet. However, the complainant advised the Statutory Entity that, even though the register had been removed, the old copy of the webpage was still accessible as a "cached" backup through Google.

The Statutory Entity then began liaising with the Australian controller of Google.com.au to have its link to the register disabled. The overseas controller of Google.com was also contacted and arrangements made for the abstract to be removed. Not confident that the matter would be resolved expeditiously, the complainant complained to the Privacy Commissioner.

The Statutory Entity made a number of undertakings about the online publication of public register information, and the Privacy Commissioner was satisfied that the matter was being adequately dealt with. However, several months later, it became apparent that an internet archive [www.archive.org] still retained copies of the original webpages. The Privacy Commissioner notified the Statutory Entity, who took immediate steps to have the information removed from the archive.

3.35 In some cases, the best way to ensure data quality may be to format online information in such a way that it can only be accessed from the organisation's website – the "official source".[175] For example, this may involve excluding search engine "spiders" or "robots" from indexing the site.

3.36 Regulators of particular trades and professions should ensure that in administering public register information, the information accurately reflects registration status for individuals. Use of the phrases, "de-registered" or "cancelled" next to a professional's name can have a very different connotation to the phrase "not current" or "not currently practising". In one situation, the words may be viewed as benign – in another, adverse.[176]

3.37 Additional steps for ensuring data quality of public registers is available in OVPC's *Public Register Guidelines*.[177]

Data cleansing

3.38 "Data cleansing" involves the large-scale comparison or matching of two or more sets of personal data (either held by the same organisation or by different organisations), for the purposes of updating one or both of the sets. It is a relatively automatic, computerised process.

3.39 Data cleansing can be used to improve the quality of data and promote compliance with IPP 3. However, this method carries certain privacy risks which need to be taken into account in deciding whether it would be appropriate to carry out a cleansing exercise.

3.40 The potential for organisations retaining excessive information not relevant to an agency's functions is one such risk, with its attendant risk of creating profiles of individuals drawn from the aggregation of multiple data sets. Consistent with obligations under IPPs 1.1, 1.2 and 4.2, organisations should ensure they do not collect and retain excessive and irrelevant data as a result of a data cleansing exercise.

3.41 Organisations should also consider whether a data matching exercise is the best method for addressing data quality concerns. It may be more appropriate, for instance, to periodically invite individuals to update their details or to establish a mechanism for that to occur at the individual's election – such as an online service that accepts change of contact details. Providing individuals with the ability to update their data is consistent with obligations under IPP 1.4, which recognises that the best quality data is most likely to be that which is directly collected from the individual concerned. Organisations should be mindful, however, of the risks of identity theft where online change-of-details facilities are designed with a focus of convenience over security. Systems should not be designed to readily allow anyone to change any other person's details. Organisations should ensure they can verify the identity or authority of the person seeking to update personal information details. It should be remembered that the verification process needs to be as client-friendly as possible without making things easy for an identity thief.

3.42 Resultant mismatches produced from a data cleanse is another risk. Small discrepancies in a person's initial or address can lead to cases of mistaken matches, and mistaken identity. It will not always be "reasonable" to engage in data-cleansing for the purposes of updating personal information. The privacy risks associated with a data match may outweigh any expected benefit from improving the quality of the data held.

3.43 Organisations that share data for the purpose of data cleansing need to consider what consequences will flow from an apparent mismatch. Whose data is more likely to be accurate? Are additional checks required before deleting or updating the record? Are there legitimate reasons for differing fields to be held about the same person? For instance, an address provided for the purpose of assessing capital gains tax may differ from the address given to an electoral commission for the purpose of voting. Legal definitions underpinning the information provided may vary. Will the "cleansed" data lead to an action or decision that will affect the individual's rights, benefits or other interests?

3.44 These issues arose in the United States, when erroneous data supplied by a private contractor was used to cleanse the Florida voting registration rolls prior to the 2000 presidential election, resulting in the disenfranchisement of thousands of eligible voters.[178]

3.45 Government organisations may have inconsistent data about an individual for other reasons. Details may have changed between the different interactions with government. Names and addresses change for legitimate reasons. Marriage, divorce and, for an important minority, participation in a witness protection scheme are examples.

3.46 Reasonable steps to ensure the accuracy of personal information being used for a data cleanse, or that produced by it, might entail:

a manually double-checking the automated "matches" for false matches due to minor discrepancies such as the wrong middle initial in a record; and/or

b seeking confirmation of accuracy from the individual to whom the cleansed data relates before making further use of that data.

3.47 Consistent with transparency obligations under IPPs 1.3, 1.5 and 5, organisations participating in a data cleanse should ensure they inform individuals of their practice of data cleansing – particularly where new information has been obtained during the course of the cleanse and is to be used by the organisation. Individuals should not be left wondering, for instance, how you got their new contact details.

3.48 In some cases, it will be appropriate to give all individuals whose information is involved prior notice of the matching activity to be undertaken to allow them an opportunity to seek, in advance, correction of records held. This not only facilitates data quality, but it ensures an organisation meets its obligations under IPP 1.3 (notice of collection) and IPP 1.4 (direct collection where reasonable and practicable).

Contracted service providers

3.49 Where information handling is outsourced to private organisations, the contractual boundaries and responsibilities for data quality of each organisation need to be clearly defined in relevant service contracts. An organisation should consider:

a which organisation will control the data;

b which organisation will be responsible for updating it; and

c what obligations will arise where information is found to be out of date, inaccurate or incomplete.

3.50 Organisations and contracted service providers who are bound by the *Information Privacy Act* cannot pass on their obligation to ensure data quality to other agencies or persons who are not covered by the *Information Privacy Act*. As the Federal Privacy Commissioner has noted, "The Privacy Act places responsibility on organisations with respect to data quality that cannot be passed onto others by contractual arrangements (although others may assist in meeting the obligations)."[179]

3.51 For more detailed guidance on the obligations of contracted service providers under IPP 3, see *Outsourcing and Privacy – A guide to compliance under the Information Privacy Act – Edition 1* May 2010, pages 16 and 21.

Relationship between IPP 3, other IPPs and the FOI Act

3.52 Compliance with other IPPs assists organisations to comply with IPP 3. IPP 1.4 requires that where reasonable and practicable an organisation must collect personal information about an individual only from that individual. In most contexts, information collected directly from the individual concerned is more likely to be accurate, complete and up to date. See Case Study 3-10 for an example.

CASE STUDY 3-10: Information not collected from individual directly led to data quality issue[180]

The complainant and their partner held a joint bank account. After a family dispute, the partner advised the Financial Institution of the dispute and amended the signature authority on the joint account. Later, a relative of the partner contacted the Financial Institution to amend another account and provided further information about the family dispute. After the contact, a staff member at the Financial Institution further modified the joint account to block all withdrawals not signed by both parties. The Financial Institution contacted the complainant about the modification days after it was made.

The complainant alleged the Financial Institution had improperly collected their personal information from a third party under NPP 1.4 (similar to IPP 1.4) and failed to ensure the personal information was accurate, complete and up to date under NPP 3 (similar to IPP 3).

The Commissioner also took the view that it was reasonable and practicable to collect the complainant's personal information from the complainant. Consequently, the Financial Institution had interfered with the complainant's privacy by collecting the complainant's personal information from a third party in this case.

The Commissioner considered a range of factors in determining whether the Financial Institution had taken reasonable steps to ensure the accuracy of the information it collected, including how reliable it was likely to be, who it was collected from, and what it would be used for. Given the information was not provided by the account holders, was subject to change and had an effect on the complainant's finances, the Commissioner took the view that the Financial Institution had not taken reasonable steps to check the accuracy of the personal information it collected from the third party. Therefore, the Financial Institution had failed to comply with NPP 3.

The Financial Institution offered the complainant financial compensation. The complainant accepted the offer.

3.53 Where information cannot be collected from the individual, the notification requirements of IPP 1.3 and 1.5 ensure that the individual knows the personal information about him or her has been collected, how it is going to be used, whom it is going to be disclosed to, and the fact that the individual can seek access to that information and correct it if necessary.

3.54 If organisations properly protect personal information from unauthorised access and modification under IPP 4, then they protect aspects of its quality too.

3.55 Access to personal information, whether under the procedures of the FOI Act or under IPP 6, can help an organisation comply with IPP 3. Data quality is likely to be higher where individuals can get access to the information that relates to them and seek correction where appropriate.

3.56 Where the information is shown to be inaccurate, incomplete or out of date, or there is a dispute about the quality of the information, Part V of the FOI Act gives individuals a right to request a correction or amendment or add a notation to the record. Similarly, IPPs 6.5 and 6.6 require a contracted service provider to take reasonable steps to address the data quality issues by amending, correcting, or associating a statement with the record.

3.57 While obligations under IPP 3 are related to those under the FOI Act and IPP 6, there is a fundamental difference. IPP 3 is concerned with the adequacy of steps taken by an organisation to ensure data quality. In other words, IPP 3 focuses on whether an organisation has done all it reasonably should to ensure the accuracy of personal information. IPP 3 also does not place a resulting obligation on an organisation to correct personal information that is inaccurate. The FOI Act and IPP 6, however, oblige an organisation to correct inaccurate information.

3.58 The Australian Privacy Commissioner's complaint determination illustrates how the Data Quality principle interacts with multiple other IPPs. See Case Study 3-11.

CASE STUDY 3-11: Role of notice and access rights in ensuring data quality[181]

TICA operates a Tenancy History Database that holds personal information about thousands of Australians relating to alleged rental defaults, including failure to pay rent and damage to property. Information is also held about tenancy applicants on an Enquiries Database. The information is obtained from property managers and made available to TICA's members for a fee. The Privacy Commissioner commented that he was aware of a wide range of anecdotal evidence that indicated that a listing with TICA could have a negative impact on an individual's ability to gain housing.

TICA was found to have breached NPP 1.5 (notice of indirect collection), NPP 3 (data quality), and NPPs 6.5 and 6.6 (access and correction). The Australian Privacy Commissioner noted that proper notification of the collection of personal information in this context could play an important role in ensuring accuracy as it allowed individuals to challenge a listing they believed to be inaccurate. TICA had failed to advise tenants contemporaneously that they had been listed and had not provided adequate mechanisms to correct records or associate a statement where the accuracy of records was in dispute.

3.59 Access rights may need to be exercised by a complainant before they pursue a complaint for a breach of IPP 3, or seek a correction under the *Freedom of Information Act* or IPP 6. This preliminary step may be necessary in order to determine what information is contained in a record and whether that information is sufficiently accurate, complete and up to date. See Case Study 3-12.

CASE STUDY 3-12: Data quality unable to be assessed without evidence of what information was held[182]

A member of the public wrote to an organisation reporting that she believed a serious assault had taken place. The organisation contacted the police and obtained personal and possibly inaccurate information about the member of the public who had written the letter.

The person complained that not only had the organisation collected personal information when it should not have, but that it had collected inaccurate personal information from the police. The organisation asserted that it had only collected enough personal information from the police to further its enquiries into the alleged assault. The Privacy Commissioner was not provided with any evidence that unnecessary or sensitive information (under IPP 10) had been collected.

The Privacy Commissioner declined to entertain a complaint that the Respondent organisation held records that may have contained sensitive or inaccurate information. The Privacy Commissioner determined that it was more appropriate for the Complainant to seek access to her records under the FOI Act and, if the records turned out to be inaccurate, to request a correction under that Act

3.60 Compliance with IPP 3 will also be assisted by organisations complying with obligations under other Acts, such as the *Public Records Act 1973* (Vic), section 13 of which provides that the officer in charge of a public office must, amongst other things:

a cause to be made and kept, full and accurate records of the business of the office; and

b be responsible for carrying out within the office a programme of records management in accordance with the standards established under section 12 by the Keeper of Public Records.

3.61 Organisations may also have additional legal obligations to ensure the integrity of information they hold, for example under the *Electronic Transactions (Victoria) Act 2000* (Vic) and the *Evidence Act 2008* (Vic).

IPP 3 Notes

[154] *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77 at para 32.

[155] Macquarie Dictionary, *Australian Online Dictionary*, http://www.macquariedictionary.com.au.

[156] The definition of "personal information" in section 3 makes clear that inaccurate or untrue information and opinions will clearly fall within the ambit of the *Information Privacy Act*.

[157] See, for example, *L v Commonwealth Agency* [2003] PrivCmrA 10, where the Federal Privacy Commissioner found that the agency had breached the Data Quality principle by sending correspondence to the wrong address. The agency had been unable to indicate whether checks had been carried out to confirm the accuracy of the address before use.

[158] *Complainant AJ v Department* [2008] VPrivCmr 2.

[159] *Complainant X v Contracted Service Provider to a Department* [2005] VPrivCmr 6.

[160] Macquarie Dictionary, *Australian Online Dictionary*, http://www.macquariedictionary.com.au.

[161] *D v Finance Company* [2009] PrivCmr A 4.

[162] *Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd and complainants C, D, E, F and G v TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrA 2 at para 45.

[163] *Leverett and Australian Telecommunications Commission* (1985) 8 ALN N135.

[164] For more on access and correction, FOI and IPP 6, see the discussion of IPP 6 in these Guidelines.

[165] Macquarie Dictionary, *Australian Online Dictionary*, http://www.macquariedictionary.com.au.

[166] See *G v Health Commission of Victoria*, Unreported judgment, County Court of Victoria, 13 September 1984, page 6, where Judge Rendit said, in relation to the obligation under the Victorian FOI Act to correct records that are inaccurate, incomplete, out or date, or misleading: "'out of date' has, in my view, a meaning of further subsequent information coming into existence which renders the earlier recorded information obsolete or 'out of date'."

[167] *G v Health Commission of Victoria*, Unreported judgment, County Court of Victoria, 13 September 1984, pages 6-7

[168] *Use of inaccurate personal data, Complaint case no ar9798-2* [1998] HKPrivCmr 17.

[169] *P v Tenancy Database* [2007] PrivCmrA 18.

[170] *Simpson v Attorney-General (Baigent's case)* [1994] 3 NZLR 667, New Zealand Court of Appeal. Also see the discussion of this case by the Law Commission of New Zealand, *Crown Liability and Judicial Immunity: A response to Baigent's case and Harvey v Derrick*, Report no. 37, May 1997, paras 9-11.

[171] *Beneficiary complains ACC acted on inaccurate information in cancelling compensation (Case Note 17749)* [1999] NZPrivCmr 13.

[172] *Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd and complainants C, D, E, F and G v TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrACD 2 at paras 35 and 43.

[173] *Q v Australian Government Agency* [2007] PrivCmrA 19.

[174] *Complainant E v Statutory Entity* [2003] VPrivCmr 5.

[175] See Office of the Victorian Privacy Commissioner, *Public Registers and Privacy – Guidance for the Victorian Public Sector*, August 2004, pages 23-26.

[176] See for example, Office of the Victorian Privacy Commissioner, *Submission to the Department of Human Services Review of Regulation of the Health Professions*, February 2004 and *Public Registers and Privacy – Guidance for the Victorian Public Sector*, August 2004.

[177] See Office of the Victorian Privacy Commissioner, *Public Registers and Privacy – Guidance for the Victorian Public Sector*, August 2004, pages 26-28.

[178] Robert E Pierre, "Botched name purge denied some the right to vote" (31 May 2001) *Washington Post*. Also see other references made available by the Electronic Privacy Information Clearinghouse (EPIC) at http://www.epic.org/privacy/choicepoint/.

[179] *Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd and complainants C, D, E, F and G v TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrACD 2, para 44.

[180] *M v Financial Institution* [2009] PrivCmrA 16.

[181] *Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd and complainants C, D, E, F and G v TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrACD 2.

[182] *Complainant C v Department* [2003] VPrivCmr 3.

IPP 4: Data security

4.1 IPP 4 contains two distinct obligations, the first dealing with data security and the second dealing with the disposal of data:

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.

4.2 The rationale for these two principles is clear. The potential for harm arising out of misuse of personal information is minimised where appropriate security safeguards are adopted and the information is retained in identifiable form only for the minimum period necessary.

Security and retention as part of the "life cycle" of personal data

4.3 These Data Security and Disposal Principles form part of the life cycle of personal information in any records management system.[183] Sometimes the best security measure an organisation can take is not to collect information about identifiable individuals when it does not need to (see IPPs 1.1, 7.4, 8 and 10).

4.4 Personal information can take many forms and will need to be secured at various stages throughout its "life" – from the time of creation (when the data is first recorded), through any transformation (such as from paper to electronic form), during its transmission (whether physically carried or sent digitally through a computer network), and while it is held (for example, text messages stored in a mobile phone). Your obligations to secure personal information under IPP 4.1 will continue for as long as you hold the data – that is, until the time of appropriate disposal under IPP 4.2 (and any other relevant laws, such as the *Public Records Act 1973* (Vic)[184]).

4.5 Organisations may find that the form in which data is kept, the medium in which it is held or the method by which it is transmitted may give rise to distinct security risks that need to be managed. Moreover, different methods of disposal may need to be considered.

Records management and other relevant personnel within the organisation can provide valuable assistance

4.6 Managing data security and retention issues is likely to involve input from individuals with various kinds of expertise. Public records officers/archivists will be essential in assessing when records should or can be destroyed. Records management personnel have invaluable experience and knowledge about the day-to-day management and flow of information within an organisation. Information and communications technology (ICT) specialists will be able to offer advice about available and adaptable technologies that enable security and disposal to occur. Building and facilities managers play a role in securing the premises and equipment that is used to store and transmit personal information. Legal advisers can assist in recommending ways to ensure compliance with privacy and related statutory obligations. For example, security and disposal/retention obligations are also relevant to public records legislation,[185] computer crimes provisions,[186] document destruction statutes,[187] and various public administration laws.[188]

4.7 The Data Security and Disposal Principles are discussed in turn.

IPP 4.1: Security of data

4.8 IPP 4.1 is concerned with an organisation's obligation to take reasonable steps to protect personal information it holds from misuse, loss, unauthorised access, unauthorised modification and unauthorised disclosure.

4.9 Since the 1980s, there has been a significant amount of work done in the area of data and information security.[189] Organisations can draw on a wealth of resources and expertise for guidance on managing data security risks.[190] Many publications are particularly thorough and, if followed, will provide robust security across various areas of potential risk. The advice of security experts can also be sought.

4.10 Regardless of where advice is obtained, an organisation may still need to identify and assess the risks associated with its particular holdings and its methods of handling personal information. An assessment of data security risks could be incorporated into an organisation's broader approach to risk management. A Privacy Impact Assessment (PIA) may assist organisations in identifying and mitigating possible security and privacy risks.[191] A PIA often forms part of the overall corporate risk assessment process and is best undertaken with the involvement of experienced people from various parts of the organisation. This includes legal, information technology, audit, human resources and line management. A PIA will assist organisations to determine what steps it is reasonable to take. Suitable security policies can be framed and detailed security measures crafted.

Distinguishing data security from information privacy

4.11 The concept of data (or information) security is both broader and narrower than information privacy. Information security is generally regarded as wider than information privacy, as data security is often concerned with the protection of both personal and non-personal information. While the *Information Privacy Act* applies only to information about identifiable individuals, information security can apply beyond this context to encompass other types of information, such as information relating to business transactions or trade secrets, or information concerning national security threats to essential services and critical infrastructure.

4.12 Information security is narrower than privacy, on the other hand, as its primary goal is to safeguard information and information systems, rather than extend to other information handling principles common to information privacy laws (such as limiting collection, enabling anonymous transactions, or ensuring access to one's own information).

4.13 The main sub-goals of information security include factors such as confidentiality, data integrity, availability, authentication and non-repudiation:

> To the average person, "security" corresponds with "confidentiality"; that is, ensuring that information is available only to those people properly authorised to receive it. This is generally achieved through some form of encryption. However, "security" increasingly includes a number of other important factors:
>
> - Integrity, which ensures that information has not been changed or tampered with;
> - Availability, which ensures that communications and computing systems are not disrupted in their normal operations;
> - Authentication, which ensures that a person accessing or providing information is actually who they claim to be; and,
> - Non-repudiation, which ensures that a person is not able to deny the receipt of information if they have, in fact, received it.[192]

4.14 However, organisations should endeavour to design their security measures in a way that supports, rather than restricts, the other information handling principles. So, for instance, a heavy focus on confidentiality that limits access to authorised persons only should not in principle impair an individual's ability to access and correct their own information (IPP 6 and the FOI Act). Authentication processes should not in principle lead to an excessive collection and retention of personal information (IPPs 1.1 and 4.2). A focus on ensuring that individuals do not deny the fact that they received information (non-repudiation) should leave room for the possibility of individuals transacting anonymously, where lawful and practicable (IPP 8). See, for instance, the balance that was struck in *Complainant W v Public Library* [2005] VPrivCmr 5, which involved a complaint about the way a library's anti-virus software operated to unnecessarily collect users' personal information by making copies of files that were scanned for viruses. By changing the way the software was configured so that copies of the scanned files were made on the user's floppy disk rather than the library computer's hard drive, the library was able to meet its need to secure its computer facilities against viruses while minimising the unnecessary collection of information.

4.15 Where it is thought that privacy principles impede justified security interests, consider whether the balance can be struck within the terms of the *Information Privacy Act*. The *Information Privacy Act* and the IPPs were drafted to accommodate various interests (such as national security and law enforcement interests) and many of its obligations are couched in terms of what is "reasonably" required in a given case. If the privacy law must necessarily give way, any restriction should be limited to what is necessary and proportionate in the circumstances, and be clearly authorised under law.

Relationship between data quality (IPP 3) and data security (IPP 4)

4.16 A breach of IPP 3 (Data Quality) may cause a subsequent breach of IPP 4. Failure to keep accurate, complete and up to date personal information may lead to an inadvertent disclosure and data security breach. See, for example, Case Study 4-1, where an organisation's failure to ensure correct address details led to a data security breach.

CASE STUDY 4-1: Failure to ensure correct records leads to unauthorised disclosure[193]

The complainant was contacted by the Department and asked to provide her and her relative's address for a specified purpose. Subsequently, a representative of the Department attended the complainant's relative's residence to attempt to serve a subpoena on the complainant. The relative advised that the complainant did not reside at the address and never had. The complainant contacted the Department to find out why a subpoena had been served at her relative's address. The Department stated that the relative's address was the address on record for the complainant. The complainant again provided the correct address to the Department.

Later that year, the complainant wrote to the Department and provided a postal address for return correspondence. The Department responded, but sent the letter to the complainant's relative's former address. The letter contained the complainant's personal information.

The complainant alleged that the Department had failed to comply with IPP 3 (by failing to correctly record the complainant's postal address and update the details) but also IPP 4 (in attending the incorrect address to serve a subpoena and sending correspondence to the incorrect address).

The Privacy Commissioner considered that the failure to update the address details raised issues under IPP 3, and that use of an incorrect address to send correspondence raised issues under IPP 4. The matter was settled at conciliation with a formal apology, a note on the file to verify accuracy before sending correspondence, and by the Department undertaking a data-cleansing exercise to ensure the accuracy of all personal information on the complainant's file.

Relationship between unauthorised disclosures and security breaches

4.17 A breach of IPP 2 (Use and Disclosure) may also involve a breach of IPP 4, and vice versa. See, for example, Case Study 4-2, where an organisation agreed to improve its security practices following an unauthorised disclosure of the contact details of a woman fleeing an abusive relationship.

CASE STUDY 4-2: Failing to take reasonable steps to protect information from unauthorised disclosure[194]

The complainant, fearful for her safety after leaving an abusive relationship, changed her name by deed poll and moved to an address unknown to anyone, including her parents. She went to a statutory entity to update her name and address details and requested the entity not to disclose her new contact details to anyone. She was assured that privacy laws protected her details from unauthorised access.

The complainant's former partner later made two requests to the statutory entity for access to the complainant's contact details. The first was refused according to the entity's business practices, but the second was successful and the complainant's details were disclosed, contrary to the entity's policies. That same day, the complainant contacted the entity and discovered her details had been disclosed to her former partner. The complainant returned to her home to find a window had been forced open. She fled her home and went into hiding.

At conciliation, the statutory entity agreed to review its business rules and procedures concerning the protection of information of persons who fear for their safety, and to implement changes to their database to warn counter staff of a request to suppress disclosure. The entity also paid the complainant $25,000 compensation.

4.18 Inappropriate disclosures will not, however, necessarily be accompanied by a breach of the IPP 4. Information may be inappropriately disclosed despite adequate security measures having been put in place. That is, an organisation may have complied with IPP 4 in taking "reasonable steps" to secure personal information, but these security precautions may have been circumvented or ignored, resulting in an unauthorised disclosure in breach of IPP 2. This is what occurred in the NSW case of *NS v Commissioner, Department of Corrective Services* [2004] NSWADT 263, where a parole officer ignored the Department's computer warning not to disclose the confidential information in its database to unauthorised persons or access it for personal reasons. The NSW Tribunal found the Department had taken reasonable steps to secure the information. However, it would not be safe for organisations to assume the same findings would be made in Victoria. A computer flag, without more, is unlikely to be regarded as adequate to secure sensitive criminal history records. Additional measures would be expected, such as training and audit trails. Unlike NSW privacy law, the *Information Privacy Act* imposes clear obligations on organisations to take reasonable precautions and exercise due diligence to avoid a contravention of the *Information Privacy Act* from occurring.[195]

4.19 Careless and accidental disclosures may invoke both IPPs where the organisation could have better secured the information, for instance through better record management procedures or staff training.

4.20 It may be the case, as Waters and Greenleaf have suggested, "that a disclosure will only involve a breach of the security principle if it could have been prevented had better security procedures been in place."[196]

4.21 In cases involving external access to information (eg, by hackers), the Security Principle is more likely to be relevant than the Disclosure Principle. The Disclosure Principle focuses on the activities of the organisation in disclosing the information, while the Security Principle focuses on preventing unauthorised disclosure (by the organisation) and unauthorised access (by persons within or outside of the organisation).

Balancing convenience and efficiency with privacy and security

4.22 New government initiatives undertaken with convenience in mind may carry privacy risks that should be taken into account at the early stages of development. For example, migrating paper records onto an online, widely accessible, medium illustrates the point. Keying in the data (whether through a manual or automated process) may result in inadvertent errors or omissions, suggesting the need for oversight or quality control to minimise unauthorised modifications.

4.23 Making information available over the internet offers greater convenience by allowing individuals to choose the time and place where they can view information or transact with government. Government agencies benefit as well, with cost savings associated with reduced demand on administrative staff who previously mediated these transactions. Yet the migration to a digital or online format may create new privacy risks. When information is in electronic form, it can be replicated and distributed faster and wider than paper documents. An example is discussed in Case Study 4-3.

CASE STUDY 4-3: Telecommunications company required to increase security against unauthorised access[197]

The Australian Privacy Commissioner considered a practice of a telecommunications company under National Privacy Principle 4 (similar to IPP 4). The telecommunications company allowed individuals to access their own mobile phone account information by calling a 1800 number, following the voice prompts, and keying in the relevant mobile number. The account information available to the caller was the credit balance and transaction details of the last payment.

The Privacy Commissioner commenced an own motion investigation into the matter, and considered that individuals "freely provide their mobile phone number to other people and organisations for a vast range of personal and professional reasons. Therefore, a mobile phone number is easily accessible by many parties."

The Commissioner formed the view that the telecommunications company was not adequately protecting account holders' personal information from unauthorised access. "This is because anyone who knew an individual's mobile phone number and mobile carrier could call the 1800 number and access the individual's account balance without their authority."

As a result, the telecommunications company proposed various changes (including authentication and satisfying other criteria, and the possibility of additional security measures). The Commissioner was satisfied with the changes and ceased the own motion investigation into the matter.

4.24 Organisations should be extremely careful when considering whether to "open up" their systems for online use, whether access is granted to the world (via the internet) or to designated organisations (via an extranet or a restricted access area on the internet). Unless a privacy-aware approach is taken to the online system architecture, personal information contained in online databases can be dangerously exposed. (See the discussion of online information, at paras 4:56-4:58.)

"Reasonable steps" to secure information

4.25 Consistent with the taking of "reasonable steps" under other IPPs (notably IPP 3), taking reasonable steps under IPP 4.1 to protect personal information will depend on the particular circumstances.[198]

Security measures should be proportionate and appropriate to the likely risk of a security breach and the gravity of harm that may result

4.26 As suggested in the section dealing with IPP 9 (see paras 9:11-9:12), there are a number of categories of information holdings that may require advanced protection to avoid or mitigate against potential harms that might arise from any misuse or unauthorised access or disclosure. These include information holdings that:

a involve vast amounts of personal information;

b involve information about vulnerable persons;

c involve sensitive information (defined to include personal information such as racial and ethnic origin, political opinions, sexual preferences, and criminal record);[199]

d carry a risk of identity theft or financial harm; or

e carry a risk of harm to a person's life, safety, liberty, reputation or livelihood.

4.27 In deciding what "reasonable steps" to take, organisations should consider factors such as:

a the nature or sensitivity of the personal information concerned;

b the likelihood of a security breach occurring; and

c the gravity of any harm to an individual if a security breach occurs.

4.28 For example, one type of information that should attract a high level of security is biometric data (eg fingerprints, iris scans, genetic samples and DNA profiles, voice recognition, photographs, and digitised signatures). This is because biometric data is a powerful tool for verifying identity. Inadequate security measures can result in a biometric being misused or compromised, such as where a digitised signature is stolen and used to commit financial fraud, or a genetic sample is taken and submitted for non-consensual paternity testing. Public confidence in the databases and identity management schemes can be shaken. Individuals can suffer severe hardship and harm to their reputation, livelihood, family and social relationships. A biometric, once compromised, is difficult or impossible to recover. Unlike a PIN number, a fingerprint or DNA profile cannot be "re-issued".[200]

4.29 While it is recognised that organisations do not have unlimited resources to use in designing and adapting security safeguards to protect personal information, organisations would be expected to implement safeguards that are appropriate and proportionate in the circumstances. This will inevitably involve a balancing of a number of factors, including risks to personal privacy and costs of implementation. Useful guidance offered by the New Zealand Privacy Commissioner, which is derived from the OECD Data Security Guidelines, sets out various matters relevant to an assessment of what steps might be regarded as "reasonable":

> Under [the Data Security Principle], information must be protected by security safeguards that are reasonable in the circumstances. The standard of reasonableness in the circumstances is consistent with the proportionality principle in the OECD Guidelines for the Security of Information Systems 1992:
>
> *Security levels, measures and costs should be appropriate and proportionate to the value of and degree of reliance on the information systems and the severity, probability and extent of potential harm, as the requirements of security vary depending on the particular information systems.*
>
> When considering "reasonableness" in the security context, factors which may be relevant include:
>
> - the workability of the safeguards
> - the cost of the safeguards
> - the risks involved
> - the sensitivity of the information and
> - the other safeguards in place.[201]

4.30 The OECD Guidelines were endorsed by the Privacy Commissioner in his report into *Mr C's Case* as being "valuable high-level principles from which to derive, in a coherent whole-of-government way, more detailed sets of standards tailored to the many diverse settings that characterise public administration."[202]

4.31 In considering the costs of safeguards, organisations should be mindful not only of the costs associated with designing or introducing the safeguards, but also the costs of failing to do so. A security breach may not only lead to the financial and personal costs associated with providing redress to those whose privacy is adversely affected, but may also trigger expenditure to contain the breach and reassure the community that the incident is not likely to occur again.

Some key areas to consider

4.32 Information security standards usefully focus on a number of areas where data security risks could be managed, such as physical security (that is, securing a building or equipment where information is housed), logical security (that is, controlling access to data), and communication security (that is, protecting data during transmission). Additional areas for attention can be found in the standards and other publications referred to above.

4.33 The following are some examples of steps organisations may consider to be reasonable when securing personal information.

Limiting access to those with a "need to know"

4.34 One obvious safeguard to protect personal information from unauthorised access is to determine who in the organisation *needs* to have access to the information in order to do their job. Organisations should ensure that personal information contained in manual and computer files is not readily accessible to everyone in the organisation, irrespective of their need to know. See, for instance, the New South Wales privacy complaint in Case Study 4-4.

> **CASE STUDY 4-4: Open access policy to student records results in security breach**[203]
>
> A soccer coach used his position as a teacher at the player's school to access her school records, which contained the student's medical information. The student's medical records were then used by the teacher and soccer club president to persuade the player and her parents to provide the soccer club with an indemnity in case she was injured during a game.
>
> A review by the NSW Department of Education found that the school had no recorded policy or procedures in place to control access to students' general records. The Department conceded it was in breach of the Security Principle.
>
> The Tribunal commented that, in some cases, it may be appropriate for information to be widely available within a school to meet the purposes for which it was collected. However, in other cases, it may be more appropriate for a small number of relevant staff to have access to the information.
>
> The Tribunal suggested that the school should have had guidelines for the use of personal information in its student records. It also suggested that staff should have been given appropriate training about their obligations under the privacy legislation and an appreciation of the potential for conflict with their teaching and other roles within the community.

4.35 When looking at your access policies, you should clearly distinguish between those in the organisation who have the ability to access information ("able to know") from those who need to access it ("need to know"). Only those who *need* to know should be *able* to access the information. As the NSW Tribunal suggested in Case Study 4-4, there may be some exceptional cases where wide or universal access may be appropriate. More usually, access will be restricted to a narrower group of persons within the organisation, particularly where the information is sensitive or delicate.

4.36 Determining access control involves not only deciding who should be able to access information. You may also need to consider matters such as:

a Is it necessary to limit the amount or type of information accessible to certain persons, depending on their role?

b What rights should authorised individuals have to deal with the information? For example, should they have "read only" access, or be authorised to change, add or delete information?

c How can they use the information? Case Study 4-4 illustrates the potential conflict that may arise when a person accesses official information for private reasons. Guidance on addressing this issue, and the potential for unauthorised disclosures by public officials, is provided in paras 2:101-2:107.

d Is the information accessible to contractors? For instance, does the organisation outsource functions or activities that involve information handling, or otherwise allow the contractor access to the organisation's premises or ICT systems? Organisations should give careful consideration to the nature of any contract, what contractors have been engaged to do, and therefore what level of access, if any, they have to the organisation's information systems and records.[204]

e Where access is granted to external users (that is, persons or bodies outside of the organisation that has custodianship over the information), what safeguards are in place to protect the information? For instance, how many of the external staff have access, and to what extent? What protections or controls are in place to ensure external users maintain the security of the information?

f To whom can authorised persons disclose the information? Is there a need to specify which persons or bodies are authorised recipients, or comprise a class of authorised recipients? Conversely, are there persons or bodies to whom the information should not be disclosed, due, for instance, to concerns about the safety of the person who the information is about? (See paras 4:17-4:21 for the discussion about the relationship between data security and unauthorised disclosure.)

g Who grants authorisation for access, and on what basis? Who authorises disclosure to other persons or bodies, and on what basis? Are there clear criteria, protocols or policies for determining who gets access, or who is authorised to receive information? Is authorisation granted by a suitably senior person within the organisation?

h Which staff are "power users", able to access virtually anything? Have the number of "power users" been kept to the necessary minimum?

4.37 Organisations should ensure their staff understand their access rights and responsibilities under the *Information Privacy Act*. This may entail, as suggested by the NSW Tribunal in Case Study 4-4, having clear guidance about authorised access and appropriate use. An organisation can adopt a variety of strategies to communicate its access policies to staff and ensure they understand their obligations under the *Information Privacy Act* and the organisation's internal policies. Relevant information can be included on log-in screens, in handbooks, policies and procedural manuals. These may need to be reviewed periodically.

4.38 Also, as noted earlier (para 2:43-2:44), the extent to which personal information is circulated within an organisation will be affected by matters such as the size of the organisation and the functions of the individuals within the organisation (affecting their "need to know"). See *Complainant Q v Contracted Service Provider to a Department* [2005] VPrivCmr 3, in which the Privacy Commissioner accepted that it was reasonably expected that a Human Resources Manager could pass on the outcome of a criminal record check for a job applicant to two senior staff members with responsibility for supervision and management of the person's work. A person's reasonable expectation would be that the information would not flow outside the organisation, or to people within the organisation who did not have a "need to know". An example of wide circulation of information leading to a data security breach is discussed (Case Study 4-5).

CASE STUDY 4-5: Personal information circulated throughout an organisation and uploaded to "YouTube"[205]

The complainant was an employee in a Victorian Public Sector organisation, and was required to handle telephone enquiries from members of the public which were recorded by the employer. The complainant received an extremely abusive call from a member of the public who made threats against members of Organisation B. As a result, a senior member of the employer organisation sent an email to a senior member of Organisation B notifying it of the threats. The email included personal information about the member of the public, as well as the electronic audio file containing the record of the telephone call. The electronic audio file was also labelled with a misspelled version of the complainant's name.

The complainant's employer subsequently became aware that the email and electronic audio file were circulating in the public domain and that the recorded call had been placed on "YouTube" and another website. The complainant's employer (whose staff had notified Organisation B of the threats) made a complaint to Organisation B about the unauthorised disclosure of the email and electronic audio file.

The complainant complained about the employer, however, audit information indicated that it was likely that disclosure of the personal information had occurred through actions of Organisation B. The complainant lodged a separate complaint about Organisation B.

Organisation B advised that an email audit had revealed that the electronic audio recording had been accessed in excess of 2000 times by Organisation B employees for entertainment purposes, and given that entertainment purposes were completely unrelated to the primary purpose of collection, Organisation B acknowledged that this "may have contributed" to disclosure on YouTube.

The Commissioner's view was that circulation of the electronic audio file had exposed the complainant's personal information to the risk of unauthorised disclosure and it was 'highly probable' that one or more of the 2000 employees who had received the email had sent it outside of Organisation B into the public domain. Conciliation with Organisation B failed and the complainant referred his complaint to the Victorian Civil and Administrative Tribunal (VCAT) where an agreement was reached at compulsory conference.

Using audit logs to deter and detect security breaches

4.39 The ability to determine who has accessed personal information, when and for what purpose is a very useful security measure. Effective auditing can be used to both detect and deter misuse. Staff may be less inclined to misuse their access privileges if they are likely to be found out.

4.40 To be an effective deterrent and detection measure, audit logs (or audit trails) must be usable and used. That is:

a Organisations need to be able to interpret the audit log to determine what they need to know. For instance, does the audit log readily reveal who has accessed what information, and when? Is it necessary to know what was done with the information, such as whether it was simply read, or whether it was copied, forwarded, modified, or deleted?

b Audits must be carried out and responsibility given to a person who can assess whether a potential breach has occurred.

4.41 Audits can be effectively used in a number of ways. Automated auditing can be used, for instance, to alert the organisation to instances of unauthorised access to restricted categories of personal information which have been flagged in the system. Random audits can also be useful to monitor access by "power users".

4.42 The effectiveness of auditing capability in relation to use of police data was central in the Privacy Commissioner's investigation in *Mr C's Case* and formed an essential part in the compliance notices that were subsequently issued – see Case Study 4-6.

CASE STUDY 4-6: Compliance notice issued to improve ability to audit access to sensitive information[206]

Mr C was concerned that his records on the police database (LEAP) were being inappropriately accessed and were being circulated around the prison system. He was also concerned about inappropriate access to his records through the Department of Justice's database (E*Justice). After asking Corrections Victoria to investigate, a senior manager from the Department of Justice (DOJ) asked a senior member of Victoria Police to conduct an audit of who had access to LEAP information about Mr C.

On completion of the audit carried out on behalf of Victoria Police, a contracted service provider (IBM) was authorised by a senior member of Victoria Police to disclose a large amount of LEAP data relating to a significant number of individuals. The sensitive personal information was sent by unencrypted email to two DOJ employees, one of whom was Mr C. On the evening of the disclosure, Victoria Police asked DOJ to remove the email from Mr C's email inbox, which it did.

The Privacy Commissioner commenced an investigation under Part 6 of the *Information Privacy Act* into the security of personal information in the LEAP database. The investigation revealed possible security problems with DOJ's E*Justice database, which contained data from LEAP and is accessible by certain authorised persons external to Victoria Police. The Privacy Commissioner began a separate investigation into the security of personal information in the E*Justice database.

Investigation into Victoria Police and the email disclosure of LEAP data

The Privacy Commissioner found that the audit carried out by IBM was inefficient, generating a needlessly large amount of information. The audit data included details relating to at least 290 individuals.

Investigation into DOJ and the security of LEAP data on the E*Justice database

An internal investigation by the Ethical Standards Department of Victoria Police into Mr C's case revealed that, early in the life of E*Justice, some users made inappropriate access to LEAP data. The Privacy Commissioner found that there were serious weaknesses in DOJ's ability to audit E*Justice users' access to LEAP data.

Compliance notices issued to Victoria Police and DOJ

The Privacy Commissioner found that, in both investigations, there had been a serious contravention of IPP 4 and issued compliance notices to both Victoria Police and DOJ.

While acknowledging that Victoria Police was already taking steps to improve the standard of protection of LEAP data, the Privacy Commissioner determined that further steps were required. Those steps included improvements to the capacity to audit the use of LEAP data by external users, such as DOJ. The progress of steps taken by Victoria Police were to be independently audited during the following year.

While the Privacy Commissioner was satisfied that DOJ was already taking steps to improve its procedures and systems to audit use of E*Justice, he issued a compliance notice to DOJ requiring that the adequacy of these procedures and systems be independently audited during the following year.[207]

4.43 While audit functions are undeniably an important element of the armoury for protecting personal information, it must be remembered that audit occurs *after* the event (at the "back end"). Audit serves a complimentary role to access control, which aims to prevent unauthorised uses from occurring in the first place (the "front end"). A well conceived data security regime will have covered both aspects: the front door (access control) and the back door (audit).

Securing the places where information is physically stored

4.44 Another aspect of data security is physical security, which is concerned with controlling access to places where information is housed or stored. These can be places (eg, buildings, rooms, cabinets) or objects (eg, smart cards, mobile phones and other portable devices). This involves assessing what physical barriers or practices can be used to prevent unauthorised access, misuse, modification or loss from occurring.

4.45 Premises can be secured using a range of devices (eg, locks on doors, swipe cards, digital keypads or biometrics readers). There may be multiple layers of authorised entry and access. For instance, a wide group of people may be authorised to pass reception and enter the building, with a lesser number allowed entry to a particular floor where they work, and then fewer to the file room where general records from across the organisation are stored, or to the communications room where access to the computer network is controlled.

4.46 In the past, the traditional floor plan comprised lockable offices and workstations. This afforded a degree of privacy and security for personal information, as files could be left out and computer monitors could not be readily viewed by passers-by. However, the trend to open-plan offices, sometimes extending to sharing workstations and computers ("hot-desking"), may create certain challenges to physical security. Consideration will need to be given to ways to mitigate new risks. Organisations might consider, for example, adopting a "clean desk" policy; providing a separate conference room in which to meet visitors or in which to conduct sensitive interviews or telephone conversations; and providing lockable cabinets in shared workstations and having separate log-in passwords for accessing different workspaces on a shared computer.

CASE STUDY 4-7: **Improving physical security following a security breach**[208]

The Australian Privacy Commissioner was informed that a number of medical documents including patient prescriptions and pathology results were found scattered in a public park adjacent to a private medical centre. The documents included patient names, addresses and telephone numbers. It was suggested the documents had come from a large bin at the rear of the private medical centre.

The Privacy Commissioner considered that 'reasonable steps' to ensure data security "depends on the circumstances in which personal information is held" and the "sensitivity of personal information stored is also an important factor and higher levels of security could be expected for more sensitive information, such as health information."

The own motion investigation found that a bin at the rear of the medical centre had been tampered with and the contents thrown around the adjacent park. The Commissioner and the medical centre devised a number of steps to improve data security, including secure fencing to reduce the risk of break in, locks, secure destruction of personal information (including shredding) and training for administrative and medical staff for proper destruction of personal information, including an instruction that medical documentation should not be left with general medical waste for collection. The medical centre also advised it would write to all patients and advise them of the matter and the steps the medical centre was taking to address it.

Organisations which share premises and facilities with others

4.47 Where an organisation is considering sharing its premises or facilities with other bodies that have different functions or carry out different activities, consideration should be given to potential security risks. In some cases, organisations may find that they are co-located with other organisations in the same building or on the same floor. Or, different units in a department, or organisations within a government portfolio, may be required to share computer and other facilities. As discussed earlier, convenience and efficiency should be balanced with privacy and security. Sharing computer and other information facilities may inadvertently (or intentionally) lead to wider access to information that was previously accessible by particular authorised personnel. Consideration should be given, for example, to designing file rooms to maintain limited access to those persons with a need to know. Network and computer servers can be partitioned or restricted so that access is limited. Guidance should be issued to relevant staff to ensure that the co-location of related business units does not lead to unauthorised access or data sharing.

Securing electronically stored information

4.48 Information is also stored on equipment (eg, computers) and portable devices (eg, USB keys) that may need to be secured. Security may entail adopting policies and procedures about where the equipment is held or how it is used. Technology can also assist. To illustrate:

a *Laptop computers.* Upon leaving the business premises, laptops can be lost or stolen. Safeguards should be considered to ensure that, if the equipment falls into the wrong hands, then the information cannot be accessed. Encryption and password protection are obvious protections. Organisations might also consider providing staff with guidance about the types of information that should, or should not, leave the building.

b *USB keys.* USB keys, or memory sticks, are a wonderful convenience but can pose a serious security risk. Their storage capacity is substantial and growing exponentially. The devices are often used without any encryption. These factors carry obvious security risks. Organisations might consider using encryption and adopting policies and procedures to mitigate risks. As almost all computers are equipped with a USB port, staff should be advised about appropriate use of these devices. Consider whether personal USB keys can be used at work and under what conditions and who is entitled to store what type of information on the devices.

c *Mobile and smart phones.* Organisations should be aware that information recorded on mobile/smart phones and other hand held devices (eg, SMS text messages and voicemail) may be subject to the *Information Privacy Act*. Organisations should assess the extent to which such technologies are used and whether security or other privacy risks need to be addressed. Organisations may need to provide staff with guidance about the appropriate use of mobile phones for work-related messaging. Password protection can be used to limit unauthorised access. Other public accountability laws may also be relevant. See, for instance, the advice from the Public Records Office of Victoria, *Messaging technologies and recordkeeping*.[209]

Securing data during, and after, its transmission

4.49 Security obligations apply not only to information when it is stored or housed, but also while it travels. Transmissions by email or facsimile are examples. So too is collecting and making information available over the internet. Security risks can arise at various points during, and after, information is transmitted. Unencrypted email can be intercepted and read prior to its delivery in the recipient's inbox. Confidential facsimiles can be read by anyone with access to the machine. Online information may be accessed from anywhere in the world and may be difficult to remove after the initial publication. Given these methods of transmission are so commonly used, additional guidance is provided below.

ILLUSTRATION 1: Facsimiles (Faxes)

4.50 Facsimiles do not simply generate a paper document, but are computers that send, receive, and store data. Fax machines may also include copying and scanning functions, which only increase their potential to store identifiable information. Accordingly, similar protections that apply to computers should be considered in relation to facsimile or multi-purpose machines.

4.51 When it comes to transmitting documents, there is a potential for the information to be disclosed to more people than just the intended recipients. If the wrong number or email address is used, the personal information may be disclosed. If no record is kept of numbers dialled or the email addresses sent to, it may become impossible to determine who the information was erroneously disclosed to. See Case Study 4-8.

CASE STUDY 4-8: Automated disclosure following use of incorrect facsimile number[210]

Employees of a bank intending to send customer information to a department within the bank accidentally sent the information to another organisation with a similar facsimile number. The accidental recipient of the information was an organisation that was in the business of forwarding incoming faxes to its own customers. In at least two instances, the bank customers' information was automatically forwarded to numerous other people and organisations by the recipient organisation through its computer-generated fax update service.

Although none of the data subjects complained to the Federal Privacy Commissioner, the Commissioner initiated his own investigation as the mistaken transmission had happened before and suggested a systemic problem.

The bank agreed to stop using its facsimile-based service and introduced a secure online system for its employees to send personal information. The bank also permanently decommissioned the fax number and confirmed that it blocked all faxes except those from designated numbers.

4.52 For guidance on ensuring the security of facsimile transmissions, see the Ontario Information and Privacy Commissioner's advice,[211] which suggests a number of useful measures such as:

a isolate the fax machine in a secure area, to ensure only authorised personnel can read faxes containing personal or otherwise confidential information;

b use cover sheets which indicate the total number of pages faxed, and inform the recipient that the remainder of a transmission contains personal information or is otherwise confidential;

c confirm the number before dialling, including a periodic check of pre-programmed numbers, to ensure they are accurate and not out of date;

d phone ahead to advise that a facsimile of a sensitive nature is coming;

e check the confirmation report to confirm the accuracy of the destination number and that the correct number of pages have been transmitted.

IPP 4

ILLUSTRATION 2: Emails

4.53 It is easy to send emails and to attach vast amounts of personal information, as the investigation into *Mr C's case* (discussed in Case Study 4-6) illustrated. Information sent to an intended recipient can be intercepted or circulated to those with no authority or need to know. Care should be taken to get the email address right and not to send or forward copies of the email to additional recipients who do not require the information.

4.54 Organisations can enhance and maintain the security of emails through a variety of means. As suggested in OVPC's Information Sheet 06.02, *Email Disclaimers and Privacy*, June 2002, organisations should consider the following steps:

a establish what personal information can be sent via unencrypted (that is, unprotected) email, and whether alternative means of transmission (eg, delivery by hand) should be considered for information of a more sensitive, private nature;

b determine when and what level of encryption is to be utilised, having regard to any prior need to establish suitable arrangements with recipients (eg, use of digital certificates);

c adopt an email disclaimer to warn all recipients that the contents of the email may contain personal information and that privacy should be respected at all times. Set out what steps should be taken if the email is received by someone other than the intended recipient (such as notifying the sender and confirming whether the errant email should be deleted).

4.55 The report of OVPC's audit on email monitoring, *Deakin University – Electronic Mail Policies*, provides some additional guidance on good practice, such as:

a giving notice – give users sufficient information about the monitoring that is being undertaken without necessarily revealing the details of the security techniques and products employed so as to expose the organisation to a greater risk of attack;

b access control and roles – limit the number of systems administrators who have access to other users' email accounts; consider having them sign a specific confidentiality agreement if they are involved in a particularly sensitive role; and ensure the administrators are themselves subject to monitoring (eg, random audits);

c automated versus manual monitoring/filtering – consider using automated filtering/monitoring tools, as manual monitoring increases the chances for excessive intrusion by systems administrators; consider whether the automated monitoring tools need to be adapted or modified to ensure that legitimate functions and activities are not impaired (eg, that emails are not unnecessarily blocked because they include certain terms that may be "blacklisted" but are legitimately part of the lexicon of the researcher or other user);

d training – provide information and training to users so they are aware of their responsibilities and are accountable for their actions in a just and precise way.[212]

ILLUSTRATION 3: Online information

4.56 As already discussed at para 4:22, one of the drivers for the *Information Privacy Act* was a commitment to encourage the public to embrace e-government and e-commerce by reassuring them that their personal information would be protected. Great care needs to be exercised when an organisation seeks to collect or disseminate personal information over the internet. Computer or coding errors can result in unauthorised access or disclosure on a grand (world-wide) scale. See, for example, Case Study 4-9.

CASE STUDY 4-9: Unintended disclosure of competition entrants leads to multiple complaints[213]

The Department ran an online competition asking members of the public to vote on which of the Department's recent advertising campaigns was their favourite. Entrants were advised they would be automatically entered into a draw for a prize. When the Department published the results of the competition on its website, it inadvertently published the personal information of 1500 of the voters. When searching for their name in Google, their name, address, email address and telephone numbers were visible. As a result, 21 people lodged formal complaints, including complainants located outside of Victoria.

The Department had taken steps to remove the information from its website. However, the data was still available in an old copy of the webpage kept (or "cached") by Google.[214] The Department explained that human error led to the inclusion of one additional piece of code when publishing the results of the competition. This code allowed Google, and only Google, to locate the personal information and make it available on the World Wide Web because of the specific "spiders" (search capabilities) that Google utilises.

After a prolonged negotiation with Google offices in the United States, the information was eventually removed from the World Wide Web.

Several weeks later, the information reappeared through a Google search result. Google explained it had mistakenly updated its cache with old, rather than new, information. In response to the Department's request, Google refreshed its data with the updated information and thereby (again) deleted the personal information.

4.57 As is apparent from Case Study 4-9, personal information may be difficult to retrieve after the initial publication, despite the organisation removing the information from its server. In addition to having to negotiate with Google and/or other search providers, others have found it necessary to remove personal information from other sources, such as the Internet Archive – see the Case Study discussed under IPPs 1.3 and 3,[215] where a statutory agency published delicate information on the internet and, despite securing its removal from Google's cache, found the information continued to be available through the Internet Archive.

4.58 Organisations that are considering using the internet to collect or make available personal information should consider privacy and security at each stage – before, during and after collection/dissemination. As suggested in the OVPC's *Public Register Guidelines*,[216] organisations should consider the likely permanency of the information in cyberspace, and whether the website can be designed to reduce the likelihood that search engines can seek out the information or archives will remember. Special coding can be used to "repel" search engine robots and spiders, for instance, so that the website is excluded from a search. Organisations should plan to contain any breach that should occur. Reasonable steps might include: prompt removal of the information from its website; notification to affected individuals, where appropriate; and negotiation with search engines and other relevant operators to remove the information from any cache or archive.

ILLUSTRATION 4: Using another organisation to store personal information/ cloud computing.

4.59 Some technology service providers offer information technology infrastructure that hosts data or applications on behalf of an organisation. This is sometimes referred to as 'cloud' computing/storage.

4.60 There are three distinct ways in which a Victorian government organisation can conceivably use cloud computing. These differ as to where the cloud server is located or hosted:

a "private cloud" – within the organisation only – the government organisation hosts the cloud in Victoria or uses cloud technology within its organisation;

b "community cloud" – within the Victorian government – a centrally hosted cloud in Victoria that is used by various government departments and organisations;

c "public cloud" – either within Australia but outside of Victoria (with the data hosted in Australia), or offshore (hosted by a cloud computing service provider whose data servers are located overseas).

4.61 Although the use of cloud computing may offer cost advantages for organisations, it must be remembered that IPP 4.1 obligations continue to apply to data hosted in the cloud. There may be compliance issues if the cloud server is located in another jurisdiction. OVPC's *Cloud Computing* Information Sheet 03.11 contains more information for organisations anticipating using such technology.[217]

"Information it holds"

4.62 IPP 4.1 requires an organisation to take reasonable steps to protect the "information it holds". Section 4(1) of the *Information Privacy Act* states that an organisation "holds" personal information if it is in the possession or control of the organisation, whether alone or jointly with other persons or bodies, irrespective of where the information is situated, whether in or outside of Victoria.

Storing information via a service provider ("cloud computing")

4.63 Data security obligations do not cease if the information leaves Victoria. Reasonable steps must be taken to secure information that travels interstate or overseas, including in a cloud storage environment. Transborder dataflow obligations (IPP 9) may also be relevant depending on the relationship between the organisation and the recipient. Where custody or control over information is shared, which may often happen in an outsourcing context, each organisation has an obligation to secure the data. Organisations cannot contract out of their security (or other privacy) obligations[218] and need to carefully consider privacy and data security implications if they wish to use cloud computing technology.[219]

Safeguarding information from subsequent misuse

4.64 Where an organisation considers sharing or relinquishing custody or control over data, prior consideration should be given to what reasonable steps are required to safeguard the information from subsequent misuse. This might occur, for instance, where a copy of information is shared (such as bulk release of a dataset on a DVD or CD-Rom), or where information is to be released into the public domain (whether in hard copy or over the internet), or where a contract formally relinquishes custody and control. Confidentiality deeds or contracts may be useful. Restrictions on further dissemination, photocopying or bulk access might be contemplated. Independent audits and reporting requirements could be considered. The return or destruction of the information might be required after a specified time or in specified circumstances, such as where a security breach has occurred or an adverse audit report made.

When does an organisation "hold" information?

4.65 In some cases, an organisation may operate a building or venue where personal information is collected or shared by other individuals who are not employed or otherwise engaged by the organisation. Parents taking photographs of their children at a school sports day is an example. Here, the school does not possess or control the information. It does not "hold" the parents' photographs. If the school decides for other reasons to place limits on the taking of students' photographs by parents and other attendees at an event, it should not attribute the restrictions to the *Information Privacy Act* when the rationale lies elsewhere.

"Misuse"

4.66 "Misuse" of personal information is use that is improper or unlawful. Generally speaking, proper uses are those that conform to the *Information Privacy Act* and IPPs (principally, IPP 2), to other relevant laws, and to the policies and standards organisations adopt themselves. The law, policies and standards that are relevant will depend on the information, the organisation and the particular circumstances.

4.67 Unlawful uses include those that are expressly prohibited by the *Crimes Act 1958* (Vic) and other relevant laws. Examples include the use of personal information to obtain financial advantage by deception, to engage in fraud or blackmail. Personal information may also be misused when making false statements or falsifying documents

4.68 Use of personal information by a public sector official may be unlawful or improper if the use contravenes statutory or common law obligations of secrecy or confidentiality.[220] Misuse of information will also include uses of information by public sector officials otherwise than in carrying out official duties, or for personal or financial gain:

a Section 95(b) of the *Constitution Act 1975* (Vic) prohibits officers in the public service from using, except in or for the discharge of his or her official duties, any information gained by or conveyed to him or her through his or her connexion with the public service; and

b Section 22(e) of the *Public Administration Act 2004* (Vic) defines "misconduct" to include a government employee making improper use of information acquired by him or her virtue of his or her position to gain personally or for anyone else financial or other benefits, or to cause detriment to the public service or the public sector.

"Loss"

4.69 Information can be lost in the sense that its whereabouts are unknown[221] and in the sense that there has been a failure to preserve or maintain it. Loss includes intentional or inadvertent destruction. Loss can be temporary or permanent, partial or total.

"Unauthorised access, modification or disclosure"

4.70 Access will include viewing information on a computer screen or reading a document on a file. For example, unauthorised access may occur where a public official uses his or her access privileges to look up the records of a neighbour or celebrity for no reason other than to satisfy their curiosity.

4.71 Modification includes changing, removing or adding information.

4.72 The meaning of "disclosure" is discussed at para 2:7 and essentially means opening up something to view or revealing it. Unauthorised disclosures will include those disclosures that are not permitted under one of the grounds in IPP 2.1 and are not otherwise authorised or required under some other law.

4.73 Access, modification or disclosure of personal information may be regarded as "unauthorised" where the person:

a has *no* authority to access, modify or disclose the information – for example:

i. where there is a legal restriction on access, modification or disclosure (eg, a statute may prohibit certain disclosures, or may restrict access to prescribed persons only);

ii. where the person is not employed by the organisation and has no entitlement to deal with the information;

iii. where the person obtains authority through fraud or deception;

iv. where a purported demand for release of information has no basis in law or is otherwise invalid (eg, the demand power referred to by the requester does not exist); or

b *exceeds* their authority – for example, where the person goes beyond their limited authority:

i. to view certain information only (eg, by using their key to the file room to view confidential files unrelated to their duties);

ii. to make certain types of modifications only (eg, to update individuals' contact details but not otherwise alter the contents on their file);

iii. to disclose only to authorised persons or bodies; or

c *misuses* their authority – for example, by accessing information they are entitled to access, but for an ulterior purpose or motive (such disclosing information for personal financial gain).

CASE STUDY 4-10: Misuse and unauthorised access[222]

The Australian Privacy Commissioner considered an issue relating to unauthorised access under Information Privacy Principle 4(a) of the *Privacy Act 1988* (Cth) (similar to IPP 4). The complainant, a former employee of the government agency, complained that her personal record had been accessed by a current employee of the agency, who used the records to locate where the complainant was living. This caused the complainant to fear for her safety, change her name and place of residence.

The agency advised that following internal investigation, there had been unauthorised access by an employee to the complainant's personal record. The Commissioner found "inadequacy of the steps to prevent unauthorised access" and took the view the agency had not taken reasonable steps in the particular circumstances to protect the complainant's personal information.

The agency advised that it had since applied additional protection to the complainant's personal information, and terminated the employment of the individual responsible for the unauthorised access and use of the complainant's personal record. The Commissioner conciliated the matter, and the complainant accepted confidential settlement for costs associated with the complainant's change of name and place of residence.

What to do if a security breach occurs

4.74 Where a security breach has occurred, organisations should consider four key steps when responding to a breach/suspected breach, they are:

(1) Breach containment and preliminary assessment;

(2) Evaluation of the risks associated with the breach;

(3) Notification; and

(4) Prevention

4.75 Privacy Victoria has published guidance material *(Responding to Privacy Breaches – Guide Edition 1)*[223] which can assist organisations in attempting to respond and take appropriate action if a privacy breach occurs. Importantly, such steps may be of assistance should a complaint be made by a data subject.[224]

IPP 4.2: Disposal of data

4.76 IPP 4.2 requires organisations to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

Relationship between the disposal principle and other IPPs

4.77 While the Security Principle (IPP 4.1) encourages organisations to preserve and protect personal information from loss or premature disposal, the Disposal Principle (IPP 4.2) cautions against the indefinite retention of identifiable information when it is no longer required.

4.78 The Disposal Principle helps to minimise the potential security risks that arise when information is retained for too long. Data becomes out-dated and no longer appropriate for use. Disparate data sets accumulated over time become capable of being aggregated for reasons unconnected to the original purpose for collection and beyond what the reasonable expectations might have been at that time. Disposal of out-dated and unnecessary collections also removes the risk of inadvertent or unauthorised disclosure of that information.

4.79 Organisations can minimise the need to dispose of data by limiting the amount of identifiable information collected in the first place (IPP 1.1) and by providing opportunities for anonymous transactions (IPP 8).

4.80 Having clear policies about retention and disposal of information will assist organisations to comply with IPP 5 obligations, which require information handling policies to be made available on request. Organisations may choose to provide information about its retention and disposal at an early stage of collection, along with the other matters that are specified in its collection notices (IPP 1.3 and 1.5). Informing individuals about secure storage and intended disposal can assist in the collection of sensitive or delicate information by reassuring individuals that their information will no longer be available for unrelated or unexpected uses.

Relevance of the Public Records Act

4.81 Most organisations that are bound by the *Information Privacy Act* are likely to be required to comply with the *Public Records Act 1973* (Vic) (PR Act). These Acts should be read together, and organisations should refer to OVPC's Information Sheet 05.09 *Recordingkeeping compliance, recordkeeping systems and the Information Privacy Principles*[225] and advice issued by the Victorian Public Records Office (PROV), *Information Privacy and Public Records,* which was prepared by PROV in consultation with OVPC.[226] In summary, the Advice notes as follows:

a The *Information Privacy Act* gives way to the PR Act to the extent of any inconsistency. However, the two Acts are regarded as consistent in that a legitimate purpose for retaining personal information under IPP 4.2 is to maintain archives in accordance with the PR Act.[227]

b IPP 4.2 will **not** authorise the destruction or de-identification of records that must be preserved under the PR Act. If an organisation is bound by the PR Act, it should ensure it has the necessary authority from the Keeper of Public Records before destroying or altering (through de-identification) any public records. If a relevant Records Authority from PROV does not apply to a particular record or class of record in your custody, then the organisation should request an appraisal from PROV to determine the appropriate disposal action.

c In some cases, a Records Authority issued by PROV will set a minimum period for retention. In other cases, records can be destroyed without further authorisation from PROV under the "normal administrative practice" (NAP) principle, which applies to records of a facilitative ephemeral nature (eg, rough notes for preparing correspondence and other records). Where these records contain personal information, organisations should consider whether there is any purpose for retaining the records beyond the minimum retention period or despite the NAP principle. Note:

i. An organisation is not compelled by IPP 4.2 to destroy records after the minimum retention period has expired or where the NAP principle applies, provided it has a legitimate purpose for retaining the information. (The IPPs' use of the phrase, "needed for any purpose", is discussed further below.)

ii. Conversely, if an organisation does not have a legitimate purpose for retaining the information beyond the minimum retention period or despite the authority of the NAP principle, then IPP 4.2 applies and the organisation should consider what reasonable steps should be taken to destroy or de-identify the information.

d The IPPs do not apply to public records that are under the control of the Keeper of Public Records, due to the exemption for publicly available information in ss 11(1)(c) and 11(1)(d) of the *Information Privacy Act*. The PR Act permits records to be closed from public inspection where they are of a private or personal nature.[228]

"Reasonable steps to destroy or permanently de-identify"

4.82 Organisations should already have records management processes in place for disposal of records under the PR Act. Where an organisation is not bound by the PR Act, because it falls outside of the meaning of "public office" and is otherwise not covered by the PR Act, then a records management plan should be progressively developed to deal with current, archived and new collections of personal information. A records management plan would assist an organisation to meet its obligations under IPP 4.2.

4.83 Reasonableness of destruction or de-identification will be assessed in the context of each particular case. The sensitivity and extent of information should be considered with particular care, not only during risk assessment and setting access control, but also when assessing the timing and method of disposal. The potential for misuse or "function creep" (discussed at paras KC:77-KC:80) is curtailed where the period of retention is more strictly controlled.

4.84 Organisations may decide that the disposal obligations applying to particular types of information holdings may warrant greater clarity or specificity than might already apply under an existing disposal authority issued by PROV. Consideration should be given to amending or developing an applicable authority that covers information holdings that contain information that is sensitive or delicate, involve aggregated data from across a number of datasets, or relates to a vast number of individuals in the community. Advice from PROV should be sought. Ensure that there is appropriate liaison between those responsible for records management and those protecting privacy. Privacy protection is best served by formal liaison between several key players in any organisation, as discussed earlier (see para 4:6).

4.85 Reasonableness will also involve a consideration of the medium in which personal information is stored. Data media differences have a major bearing on the interpretation of destruction or de-identification.

Destroying hard copy documents

4.86 Hard copy documents are relatively straightforward. They can be shredded or otherwise physically destroyed or de-identified (PR Act permitting). Secure disposal is essential. The discovery of intact documents containing delicate and sensitive personal information in rubbish bins or blowing as litter in laneways is not unknown. See the NSW privacy case involving the discovery of hospital records by residents of a street in a Sydney suburb.[229] The health service acknowledged that it had engaged a contractor to transport the files to a secure storage facility to await destruction, but was unable to explain how the records came to be found in the street. The NSW Privacy Commissioner advised that he regarded the matter as a serious privacy breach.

Destroying electronic documents

4.87 When data is held electronically, more complex issues arise. Destruction may be guaranteed only if the hardware itself is destroyed. That is, if computer hard disks are physically destroyed. However, this will very often be impractical and wasteful. Further, deleting personal data does not necessarily constitute destruction because networked data is typically backed up and retrievable. Back-up media should be a sacrosanct component of any ICT environment. Therefore de-identification may often be the best option. But careful planning is required at the architectural design stage. When personal information is no longer required and de-identification is desired, it may be difficult to locate all data fragments unless the de-identification process was considered at design stage.

De-identification

4.88 An organisation may decide to dispose of information by de-identifying it, rather than through destruction. In that case, IPP 4.2 requires the de-identification to be "permanent". Permanent means irrevocable or irretrievable. On the face of it, this appears to set a very high standard. It may not be necessary to *irretrievably* de-identify data, provided that it is de-identified to the point that identity cannot be *reasonably ascertained*. This is because the *Information Privacy Act* ceases to apply when data no longer falls within the definition of "personal information". That is, when the information is about a person who is not identified or reasonably identifiable.[230]

4.89 Retaining data that is still potentially identifiable does, however, carry certain risks. What is not identifiable now may later become identifiable. For instance, new information may come to hand, or matching capabilities developed, that allow the data to be readily re-identified. If the de-identified information later becomes reasonably identifiable, obligations will be revived under the *Information Privacy Act*. Ultimately, you will need to decide on the likelihood of the information later becoming re-identified. You may also consider periodically reviewing whether additional steps are required to maintain the data in a sufficiently de-identified form. Alternatively, you may decide it is better to permanently and irrevocably de-identify the information.

4.90 Biometric data raises significant conceptual challenges. Outright destruction cannot be guaranteed for the same reasons discussed above. But permanent de-identification can also be difficult, and is possibly a contradiction in terms. Biometric data is by definition data that identifies. It is unique to an individual's body – for example, an iris scan, a finger scan, or a tissue sample revealing a DNA profile. The identification aspect of biometric data cannot be removed because that is what it is: identification.

4.91 As stated by the National Health and Medical Research Council in its *National Statement on Ethical Conduct in Human Research* (referred to in the Key Concepts section on personal information and de-identification), "with advances in genetic knowledge and data linkage, and the proliferation of tissue banks of identified material, human tissue samples may always be regarded as, in principle, potentially re-identifiable".[231] Reasonable steps to de-identify human tissue and other biometric data need to ensure that re-identification of the tissue or data is not reasonably possible. In the case of tissue samples, for instance, this may depend on the likelihood of a match being made between the de-identified sample and another identified sample or other identifying information.

"No longer needed for any purpose"

4.92 IPP 4.2 allows organisations to retain information for the original purpose for which it was collected, or "for any purpose". The purpose can be either the primary purpose for which the information was collected, or it can be some other legitimate purpose such as those specified in IPP 2.1. For example, personal information may be retained for related secondary purposes that are reasonably expected, for research, and where required or authorised by or under law. The *Public Records Act 1973* (Vic) is particularly relevant, as discussed above. Other statutory obligations may require or authorise records to be retained,[232] or may compel their destruction,[233] in particular circumstances. These statutes will prevail over the disposal obligation in IPP 4.1, to the extent of any inconsistency.

4.93 Information will often have great statistical and research value and can inform and guide public policy decisions. IPP 4.2 does not require this information to be destroyed. Nor does it authorise routine retention in identifiable form. Consistent with other provisions in the IPPs, consideration should be given to relying on consent where practicable and otherwise retaining and using information in de-identified form. (See the discussion of research elsewhere in these Guidelines at paras 2:59-2:92, 7:11, 8:5, 9:36, 10:31-10:32 and 10:44-10:57.)

4.94 The purpose for retaining personal information should be specific and identifiable, rather than undefined and hypothetical. IPP 4.2 does not authorise retention of information "just in case" it is needed for some future use by the organisation or by a third party. See the discussion of "function creep" in paras KC:77-KC:80, which emphasises the need for transparency and fair collection to maintain public confidence that personal information is to be used in accordance with assurances given at the time of collection.

IPP 4 Notes

[183] The life cycle of personal information is discussed at paras 8-10 in the Overview section.

[184] See Office of the Victorian Privacy Commissioner Information Sheet 05.09, *Public Records, Recordkeeping Systems and the Information Privacy Principles*, July 2009.

[185] *Public Records Act 1973* (Vic).

[186] See Division 3(6) of Part I of the *Crimes Act 1958* (Vic), which includes offences for unauthorised modification of or access to data.

[187] See, for example, the *Crimes (Document Destruction) Act 2006* (Vic), which prohibits the destruction of documents that are reasonably likely to be needed in a legal proceeding. Also see the *Evidence (Document Unavailability) Act 2006* (Vic), which sets out the consequences flowing from the unavailability of a document in a civil proceeding where, for example, a document has been destroyed or lost.

[188] In some cases, there are specific statutory obligations on securing and/or destroying records (such as the destruction of certain fingerprint records under the *Crimes Act 1958* (Vic)). Also see general prohibitions on unauthorised or improper use of information by public officials under, for example, section 22 of the *Public Administration Act 2004* (Vic) and section 95 of the *Constitution Act 1975* (Vic).

[189] The early development of data protection and privacy laws was guided by the work of the OECD, notably: the 1980 OECD *Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data*; the related set of guidelines dealing with data security, 1992 OECD *Guidelines for the Security of Information Systems*, which were replaced by the 2002 OECD *Guidelines for the Security of Information Systems and Networks*; and the guidelines dealing specifically with cryptography, 1997 OECD *Guidelines for Cryptography Policy*. These guidelines are available from the OECD website, in the "publications and documents" area of the section on "Information security and privacy", accessed 1 September 2011, http://www.oecd.org/.

[190] See, for example:

(a) Victorian Auditor-General, *Managing Internet Security: Good Practice Guide*, June 2004, http://download.audit.vic.gov.au/files/20040630-Internet-Security.pdf;

(b) Standards and manuals jointly issued by Standards Australia and New Zealand Standards http://www.standards.com.au, such as: (i) *Information technology – Security techniques – Information security management systems – Requirements*, Standard, AS/NZS ISO/IEC 27001:2006; (ii) *Information technology – Code of practice for information security management*, Standard, AS/NZS ISO/IEC 17799:2001; (iii) *Information security risk management guidelines*, Handbook, HB 231:2004;

(c) Commonwealth Attorney-General's Department, Protective Security Policy Section, *Australian Government Protective Security Policy Framework*, June 2010, available at http://www.ema.gov.au; and

(d) Australian Defence Signals Directorate, *Australian Government Information Security Manual (ISM)*, June 2011, unclassified and updated versions available for download at http://www.dsd.gov.au/infosec/ism/.

[191] See Office of the Victorian Privacy Commissioner, *Privacy Impact Assessments – A Guide*, August 2004. The Guide's Resource section lists numerous guides and examples of privacy impact assessments completed nationally and overseas.

[192] Australian Department of Defence, Defence Signals Directorate, *Information Security*, accessed 3 September 2011, http://www.dsd.gov.au/infosec/.

[193] *Complainant AJ v The Department* [2008] VPrivCmr 2.

[194] *Complainant B v Statutory Entity* [2003] VPrivCmr 2.

[195] *Information Privacy Act 2000* (Vic) s 68.

[196] Nigel Waters and Graham Greenleaf, "IPPs examined: The security principle" [2004] *Privacy Law and Policy Reporter* 36. A revised and updated version of this paper is also available: Nigel Waters, "Interpreting the security principle", paper presented at the Interpreting Privacy Principles symposium, *Interpreting Privacy Principles: Chaos or Consistency?*, 17 May 2006, Sydney, New South Wales.

[197] *Own Motion Investigation v Telecommunications Company* [2010] PrivCmrA 16

[198] See the discussion of "reasonable steps" in other areas of this Guide, particularly paras 3:21-3:28 under IPP 3.

[199] See *Information Privacy Act 2000* (Vic) (Sch 1 – The Information Privacy Principles).

[200] For an example of ways of dealing with data security and biometrics, see Office of the Australian Privacy Commissioner, Approval of the Biometrics Institute Privacy Code (s 18BB(2) of the *Privacy Act 1988* (Cth)), available at: http://www.privacy.gov.au. The Code, for example, includes supplementary principles for biometric information and states, "11.1 – Wherever practicable, a Code Subscriber shall ensure that biometric information is encrypted immediately after collection, that the original biometric information is destroyed after encryption and that biometric information is stored only in encrypted form."

[201] *Woman complains that she received another person's letter enclosed with her letter* [2003] NZPrivCmr 22.

[202] Office of the Victorian Privacy Commissioner, *Mr C's Case: Report of an investigation pursuant to Part 6 of the Information Privacy Act 2000 into Victoria Police and Department of Justice in relation to the security of personal information in the Law Enforcement Assistance Program (LEAP) and E*Justice databases*, Report 03.06, July 2006, page 29. In that compliance investigation, the Privacy Commissioner found that a serious contravention of IPP 4 occurred when Victoria Police's contracted service provider disclosed a large amount of sensitive information to two Department of Justice employees. The Privacy Commissioner issued a compliance notice under which Victoria Police were expected to, among other things, expend an estimated $102,000 for the construction of an information storage facility to improve the audit capability.

[203] *MT v Director General, NSW Department of Education & Training* [2004] NSWADT 194. This case was later reviewed by the NSW Administrative Decisions Tribunal Appeal Panel, but this issue concerning a breach of the Security Principle was not the subject of appeal. The appeal decision is discussed elsewhere in these Guidelines, in the section dealing with IPP 2.1(d).

[204] For more information relating to outsourcing and privacy, see Office of the Victorian Privacy Commissioner, *Outsourcing and Privacy – A guide to compliance under the Information Privacy Act*, May 2011.

[205] *Complainant AP v Organisation B* [2010] VPrivCmr 1.

[206] Office of the Victorian Privacy Commissioner, *Mr C's Case: Report of an investigation pursuant to Part 6 of the Information Privacy Act 2000 into Victoria Police and Department of Justice in relation to the security of personal information in the Law Enforcement Assistance Program (LEAP) and E*Justice databases*, Report 03.06, July 2006.

[207] In 2009, the Privacy Commissioner issued a report reviewing the response of both Victoria Police and the Department of Justice in relation to the Compliance Notices served. See Office of the Victorian Privacy Commissioner, *'Review of the response by Victoria Police to Compliance Notice 06/02 and the Department of Justice to Compliance Notice 06/03 served pursuant to Part 6 of the Information Privacy Act 2000'* (December 2009) available at http://www.privacy.vic.gov.au.

[208] *Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6

[209] Public Records Office of Victoria, *Messaging technologies and recordkeeping*, Advice to Victorian Agencies PROA 06/16, May 2006, Version 1.

[210] *OPC v Banking Institution* [2005] PrivCmrA 11.

[211] Ontario Information and Privacy Commissioner, *Guidelines on Facsimile Transmission Security*, revised January 2003, available at http://www.ipc.on.ca.

[212] Office of the Victorian Privacy Commissioner, "Lessons learned" in *Deakin University – Electronic Mail Policies*, Privacy audit 02.06, June 2006, pages 16-17.

[213] *Complainant AD & Others v The Department* [2006] VPrivCmr 5.

[214] Google stores many web pages in its "cache" as a backup for users to view in case the original page becomes temporarily unavailable: Google, *Google Help Center – Google Web Search Features*, 2011, accessed 1 September 2011.

[215] *Complainant E v Statutory Entity* [2003] VPrivCmr 5.

[216] See Office of the Victorian Privacy Commissioner, *Public Registers and Privacy – Guidance for the Victorian Public Sector*, August 2004, esp pages 26-28.

[217] Office of the Victorian Privacy Commissioner, *Cloud Computing* Information Sheet 03.11, May 2011, available at http://www.privacy.vic.gov.au.

[218] However, organisations may avoid liability in certain circumstances for a breach by a contracted service provider – see Office of the Victorian Privacy Commissioner, *Outsourcing and Privacy – A guide to compliance under the Information Privacy Act,* Edition 1, May 2011

[219] Office of the Victorian Privacy Commissioner, *Cloud Computing* Information Sheet 03.11, May 2011, available at http://www.privacy.vic.gov.au.

[220] See, for example, the statutory confidentiality and secrecy obligations referred to at para 16 of these Guidelines.

[221] See, for example, the Office of the Victorian Privacy Commissioner's report, *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. In that compliance investigation, the Privacy Commissioner found that an organisation had lost a file containing sensitive personal information when it was mistakenly posted to a woman in country Victoria. The organisation was not aware that the file had left their custody until nine weeks later, when it was contacted by a journalist for the ABC *Stateline* program.

[222] *F v Australian Government Agency* [2008] PrivCmrA 6.

[223] Office of the Victorian Privacy Commissioner, *Responding to Privacy Breaches – Guide Edition 1,* May 2008.

[224] See, for example, *Information Privacy Act* s 29 (Circumstances in which Privacy Commissioner may decline to entertain complaint), and specifically, s 29(1)(h)(i).

[225] Available at http://www.privacy.vic.gov.au.

[226] Public Records Office Victoria, *Information Privacy and Public Records*, Advice to Victorian Agencies, PROA 06/04, March 2003.

[227] This approach is consistent with the views expressed by the NSW Administrative Decision Tribunal Appeal Panel in *GR v Director-General, Department of Housing (GD)* [2004] NSWADTAP 26. The Appeal Panel commented, at para 54, that every attempt should be made to read the provisions of the privacy and public records statutes harmoniously. The NSW equivalent to IPP 4.2 required public sector agencies to keep information for no longer than necessary for the purposes for which the information may be lawfully used. The Appeal Panel noted that, when no longer needed, the information could then be disposed of in accordance with the NSW State Records Act. This may mean archiving the information under the State Records Act, and this would not be inconsistent with the Disposal Principle under the privacy legislation.

[228] Records closed for personal privacy reasons under s 9 of the *Public Records Act 1973* (Vic) are usually closed for a period approximating a person's lifetime. The decision to close records, or to vary or revoke a closure determination, is made by the Minister responsible for PROV in consultation with the Minister responsible for the administration of the public office concerned. These Ministers can also grant special permission to allow inspection of closed records. For further information, see Public Records Office of Victoria, *Records Information – Special Access: Public Records Act (1973) Sub-Section 9(2) Closure of Personal Records*, PROV Guide 14, July 2005.

[229] *Files not securely destroyed resulting in media report* [2002] NSWPrivCmr 4.

[230] See the discussion of personal information in the Key Concepts section, especially the paragraphs dealing with de-identified data and determining when identity can be reasonably ascertained.

[231] Australia, National Health and Medical Research , *National Statement on Ethical Conduct in Human Research*, 2007, page 29, available at http://www.nhmrc.gov.au.

[232] See, for example, the *Crimes (Document Destruction) Act 2006* (Vic), which prohibits the destruction of documents that are reasonably likely to be needed in a legal proceeding.

[233] See, for example, the obligations in the *Crimes Act 1958* (Vic) to destroy fingerprint records where a person is not subsequently charged or is found not guilty (s 464O), or where the fingerprint records relate to a juvenile offender (s 464P).

IPP 5: Openness

5.1 IPP 5 promotes a greater awareness and understanding about how organisations handle personal information. It is central to one of the *Information Privacy Act*'s objects – transparency.[234]

5.2 IPP 5.1 requires an organisation to have a written policy about its management of personal information, and to make this available on request. IPP 5.2 requires an organisation to tell people, if they ask, about the general sorts of personal information it holds and how it handles that information.

Relationship of IPP 5 with other information handling obligations

5.3 A privacy policy should be distinguished from a collection notice required by IPP 1.3 (Collection). A privacy policy is a statement about how an organisation manages the personal information it collects. It is a general, not exhaustive, statement about how personal information flows through an organisation. A collection notice, on the other hand, addresses a specific collection practice of an organisation (such as collecting personal information on a council planning application form, or for a job application).

5.4 A privacy policy can help people decide whether to make an application for access to information held by an organisation under IPP 6 (Access and Correction) or the FOI Act. People must know what type of information is generally held by an organisation so they can specifically ask for access to that information.

5.5 The obligations in IPP 5 (Openness) and Part II of the FOI Act (which serves a similar function to IPP 5 by, for example, requiring an agency to publish various statements, including a statement of the categories of documents maintained in the possession of an agency,[235] which are appropriate for assisting members to effectively exercise their rights under the FOI Act[236]) are also consistent with the public sector's obligations under the *Public Records Act* to keep full and accurate records.[237] An organisation may be able to meet these obligations by preparing a single document.

IPP 5.1: Written policy on management of personal information

5.6 IPP 5.1 states:

> An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.7 Victorian public sector organisations and their contractors bound by the *Information Privacy Act* should have a privacy policy in place. An organisation should periodically review its policy, especially where it has been given new functions or has undergone a restructure. It is good practice (and consistent with *Public Records Act* obligations to keep full and accurate records[238]) to include a date and version reference on a privacy policy. This assists in establishing what policy was in effect at any given time and may be relevant to assessing whether an organisation took reasonable steps at the time of an alleged breach, or what a person might have reasonably expected from the organisation at that time.

5.8 Newly established organisations should prepare a written privacy policy as part of the broader process of planning for compliance with the *Information Privacy Act*.

5.9 Typically, preparing to write a privacy policy involves examining the way personal information is gathered and flows through an organisation. The key to an effective privacy policy is to appropriately tailor the policy by figuring out what the organisation does with personal information, what it needs to do, what it properly can do and then ensuring that the organisation actually complies with its privacy policy. A privacy policy should not simply be a reproduction of the IPPs.

5.10 In privacy policy work, there is no "one size fits all". It is risky and short-sighted for an organisation to just copy another organisation's policy and presume it will work. Organisations should consult the work of others and take the best from good privacy policies, but should ensure that it considers how the privacy policy will operate it in its own organisation.

5.11 The process of writing or reviewing a privacy policy can help raise awareness within an organisation about how the organisation collects personal information, what it does with that information, and whether the existing practices need to be adapted.

5.12 Large organisations should consider whether they should have more than one privacy policy to cover, for example, the activities of individual business units which have distinct functions. It may be appropriate for an organisation to have a set of policies to cover different types of information or information handling practices. A separate website policy,[239] email monitoring policy or a social media policy are examples. An organisation may wish to consolidate its various compliance obligations under other Acts (such as the *Health Records Act 2001* (Vic), and/or Part II of the FOI Act) into a single document or set of documents.

Publishing the privacy policy

5.13 While there is no specific requirement under IPP 5.1 to publish the privacy policy – only to make it available on request to anyone who asks – an organisation may find it convenient and cost effective to publish its policy in hardcopy form and on its website. Other options include:

a sending a privacy policy with any written correspondence to individuals when they first transact with, or become a client of, an organisation;

b sending a privacy policy with annual notices such as re-registration forms; and/or

c having a copy of a privacy policy available at an organisation's enquiries desk or counter.

The layered approach

5.14 An organisation may decide to take a "layered" approach to complying with IPP 5. This could be achieved, for example, by a brief outline of information handling obligations provided on a form or poster, with additional layers of information readily available in brochures or on its website. For further guidance about multi-layered notices, see paras 1:69-1:71.[240]

Availiability of privacy policy

5.15 Privacy policies should be readily available to staff within an organisation so that a prompt response can be given to a request from a member of the public that the privacy policy be made available– see Case Study 5-1.

> **CASE STUDY 5-1: Failure to provide privacy policy despite repeated requests[241]**
>
> A woman was concerned about being filmed by a television cameraman while she was travelling on public transport. The filming was being carried out by a media organisation with the consent of a Contractor to a Government Department.
>
> Upon returning home, the woman contacted the Contractor and asked the customer service officer to confirm she had not been filmed, and to provide her with a copy of the Contractor's privacy policy. The officer said she would take some time to confirm the woman's request about not being filmed, but agreed to send out a privacy policy. The woman did not receive the policy. Several days later, the woman happened to see her image on a television current affairs program.
>
> The woman telephoned the Contractor twice more and each time, asked for the privacy policy to be sent out. Each time, she was told it would be sent out, but never received it. The woman then complained to the Privacy Commissioner.
>
> IPP 5 requires an organisation to make its privacy policy available to anyone who asks for it: the organisation had failed to make the privacy policy available to her upon her request. The complaint was successfully conciliated with the Contractor giving a written assurance that it would publish a reminder to all staff in an internal newsletter about the importance of privacy laws and ensuring that any requests for copies of its privacy policy would be promptly met.

5.16 IPP 5.1 does not, however, contain a requirement that a policy be provided within a specific time period after a request is received that the document be made available – see Case Study 5-2.

> **CASE STUDY 5-2: Delay by organisation in providing its privacy policy[242]**
>
> A person received a fine from a Contracted Service Provider (CSP) which administered fines under contract to a Department. The complainant wrote to the CSP and in the letter stated "you do not have my permission to forward this request to any other party on my behalf". The CSP forwarded the complainant's letter to the Department and sent a standard acknowledgment letter to the complainant indicating that the complainant's request had been referred to the Department.
>
> The complainant complained to the CSP and also requested a copy of the CSP's "privacy code of practice" (the privacy policy). The CSP took approximately two months to send a copy of its privacy policy to the complainant.
>
> The complainant made a formal complaint to the Privacy Commissioner.
>
> The Privacy Commissioner noted that the complainant was sent a copy of the CSP's privacy policy after a delay of approximately two months. The Privacy Commissioner considered, however, that IPP 5 does not contain a requirement that a policy be provided within a specific time period, as compared with other sections of the Act (for example, IPP 6). The CSP explained that the delay was due to various internal factors and the numerous letters received from the complainant.
>
> The Privacy Commissioner considered that, while such a delay was regrettable, the CSP did eventually provide its privacy policy and had taken steps to review its privacy guidelines. Additionally, it had subsequently placed a copy of its privacy policy on its website.
>
> Given that the CSP did in fact supply the privacy policy, and in the absence of any timeliness requirement in IPP 5, the Privacy Commissioner considered that the CSP had not interfered with the complainant's privacy.
>
> The complainant did not refer the complaint to the Victorian Civil and Administrative Tribunal. As a result, the Privacy Commissioner dismissed the complaint

5.17 It should be noted, however, that publication and dissemination of a privacy policy supports the principle of openness and instils public trust and confidence in an organisation.

IPP 5.2: Responding to requests about the sort of information held and how it is used

5.18 IPP 5.2 states:

> On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

5.19 Unlike IPP 5.1, IPP 5.2 does not expressly require an organisation to document the sorts of personal information it collects and handles – only to take reasonable steps, when asked, to let people know generally what kind of personal information it collects and how it uses it. IPP 5.2 does not require an organisation to inform individuals about what information is specifically held about them – requests for specific access to personal information are governed by IPP 6 and the FOI Act. For IPP 5.2 purposes, it is sufficient to give generic information about the sort of information that is held, its purposes, how it is collected, held, used and disclosed. IPP 5.2 should be seen as a requirement for a further, more detailed level of information beyond the minimum required in an IPP 5.1 document.

5.20 An organisation may find it more efficient, however, to meet the requirements of IPP 5.1 and anticipate common queries under IPP 5.2 in the same document, or by using the multi-layered approach discussed earlier. However, where a generic document does not cover a person's more specific request, an organisation is required to take reasonable steps to give a specific response. For example, an organisation's privacy policy may omit reference to their practice of taking and using photographs, or of monitoring email, or of recording telephone conversations. If an individual subsequently asks for information about how the organisation collects, holds, uses or discloses these sorts of records, the organisation should be able to provide a general response.

5.21 Where certain types of information are commonly collected and used by an organisation, the organisation may wish to review their generic policy to ensure it addresses those types of information. For example, in *Complainant H v Local Council* [2004] VPrivCmr 2, the Privacy Commissioner suggested to a local council that they consider using their IPP 5 privacy policy to alert ratepayers to the council's practice of publishing petitions (including petitioners' names and addresses) on its website. See also the New South Wales case of *SW v Forests NSW* [2006] NSWADT 74, where the Tribunal ordered the government organisation to review its privacy policy and make such changes as necessary to ensure the policy addressed the collection and handling of photographs.

5.22 In practice, staff will need to help people understand how the generic descriptions in an organisation's privacy policy apply to the individual's own personal information. The privacy policy and any other information sought by an individual may be that individual's starting point in deciding whether to make an access request under the FOI Act or IPP 6.

5.23 An organisation which wants to formally document the information it holds and handles can refer to the many precedents that are available in the series of annual Personal Information Digests[243] covering Commonwealth and ACT agencies, and to the "how to" guide[244] which helpfully sets out the kinds of general content and phrases that can be used in preparing documents that satisfy the openness principle, both of which are published by the Privacy Commissioner, Office of the Australian Information Commissioner.

5.24 Of all the IPPs, IPP 5 most clearly encapsulates an organisation's opportunity to build trust. Maintaining trust in turn ensures individuals provide accurate information. If policy accords with practice, and an organisation maintains a helpful customer-focused approach to privacy compliance, it can maximise the likelihood of complying with the requirements of IPP 5.

IPP 5 Notes

[234] Section 5 of the *Information Privacy Act 2000* (Vic) sets out the objects, one of which is to promote the responsible and transparent handling of personal information in the public sector.

[235] Section 7(1)(a)(ii) *Freedom of Information Act 1982* (Vic).

[236] Section 7(2) *Freedom of Information Act 1982* (Vic).

[237] Section 13 *Public Records Act 1973* (Vic).

[238] Section 13 *Public Records Act 1973* (Vic).

[239] See Office of the Victorian Privacy Commissioner, *Website Privacy – Guidelines for the Victorian Public Sector*, May 2004, available at http://www.privacy.vic.gov.au.

[240] See also Office of the Victorian Privacy Commissioner, Information Sheet 01.11, *Drafting and Reviewing a Privacy Policy*, March 2011.

[241] *Complainant G v Department* [2004] VPrivCmr 1.

[242] *Complainant AQ v Contracted Service Provider to the Department* [2010] VPrivCmr 2

[243] Available at http://www.privacy.gov.au. Note that, unlike the *Information Privacy Act*, the *Privacy Act 1988* (Cth) requires federal public sector agencies to publish a record outlining their personal information holdings. The federal IPP 5.3 (set out in Section 14 of the Commonwealth *Privacy Act*) lists the following matters which must be included in the agency's written statement: (a) the nature of the records of personal information kept by or on behalf of the record-keeper; (b) the purpose for which each type of record is kept; (c) the classes of individuals about whom records are kept; (d) the period for which each type of record is kept; (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and (f) the steps that should be taken by persons wishing to obtain access to that information.

[244] Available at http://www.privacy.gov.au.

IPP 6: Access and correction

6.1 IPP 6 provides individuals with a right to access and correct their personal information. These rights, common in nearly all privacy and data protection laws, are important for a number of reasons. The New Zealand Privacy Commissioner explains:

> Lying behind privacy legislation is a recognition of an individual's entitlement to some degree of personal autonomy. That autonomy would be illusory in many cases unless the individual can see what information is held for potential use by others. Another reason for the right of access is because of the concern that personal information to be used should be accurate and possibly the best way of ensuring such accuracy is to let the individuals see it and point out any errors. It provides some measure of accountability by agencies to the individuals whose personal information they hold and may use. Finally, an individual's right of access tends to make other aspects of the information privacy principles self-policing. Objectionable handling of personal information might tend to come to light through the individual securing access either in the hands of the agency concerned or in the hands of another agency to which the information has passed.[245]

6.2 The utility of IPP 6 access and correction rights in ensuring and maintaining data quality was discussed under IPP 3 (at paras 3:55-3:57). The relationship between IPP 6 and IPP 5 in promoting accountability and transparency about information holdings was also discussed earlier (at para 5:5).

6.3 Also see the discussion in the Overview section (paras 22-24) distinguishing Freedom of Information from information privacy in general terms.

Interaction of IPP 6 with the Freedom of Information Act

6.4 IPP 6 is the place where the *Information Privacy Act* and the *Freedom of Information Act 1982* (Vic) ("the FOI Act") intersect. While both IPP 6 and the FOI Act are similar, in that they both provide rights of access and correction, they apply in different circumstances. The interaction of the *Information Privacy Act* and the FOI Act is most directly described in the *Information Privacy Act* in sections 6(2) and 12:

a Section 6(2) provides that nothing in the *Information Privacy Act* affects the operation of the FOI Act or any right, privilege, obligation or liability conferred or imposed under the FOI Act or any exemption arising under the FOI Act; and

b Section 12 provides that nothing in IPP 6 or any applicable code of practice applies to documents that are regulated by the FOI Act, and access to and correction of these documents can only be granted in accordance with the FOI Act.

6.5 Other sections in the *Information Privacy Act* preserve the exemptions under FOI for documents that can be required during the handling of complaints or during compliance investigations.[246]

FOI is the usual procedure for access and correction

6.6 When passing the *Information Privacy Act*, Parliament intended the Act to fit with the existing FOI Act. The explanatory material accompanying the *Information Privacy Bill* when it was introduced into Parliament made this clear:

> In Victoria, the *Freedom of Information Act* already provides a right of access to documents held by Government. The Bill does not propose to disrupt the established systems of access under this scheme by supplanting them or creating a concurrent system.
>
> Accordingly, in the case of documents held by public sector agencies, the *Freedom of Information Act* will continue to be the only enforceable method of access.[247]

6.7 IPP 6 is designed to complement FOI rights, rather than duplicate them. If an organisation is subject to the FOI Act, then the procedures in the FOI Act will apply. If an organisation is not subject to FOI but is bound by the *Information Privacy Act*, then access and correction must be handled in accordance with IPP 6.

When does IPP 6 apply?

6.8 IPP 6 will apply to organisations that are bound to comply with the *Information Privacy Act* but are not covered by the FOI Act. The Second Reading Speech accompanying the *Information Privacy Act* when it was introduced into Parliament noted that IPP 6 would have a limited application:

> ...the access provisions in Principle 6 have a limited operation to contracted service providers, which are not always subject to freedom of information legislation, and certain other bodies.[248]

6.9 IPP 6's application to contracted services providers is discussed next, followed by application to other bodies that are not subject to FOI but are bound by the *Information Privacy Act*.

Contracted service providers

6.10 A government agency that engages a contracted service provider (CSP) and binds them to the *Information Privacy Act*[249] will need to consider how to manage access requests for personal information. Individuals may, for instance, be able to seek access directly from the contracted service provider (under IPP 6) or indirectly through the outsourcing government organisation where that organisation retains possession or control over the documents (under the FOI Act). These options are discussed in the Privacy Commissioner's Guidelines to Outsourcing and Privacy:

> Under IPP 6, a CSP will be required to provide access to personal information it holds about an individual to that individual/those individuals on request.
>
> Outsourcing organisations must consider the manner in which they will provide access to personal information. Any contract should state that:
>
> - the personal information collected will remain in the "constructive possession" of the outsourcing organisation (and the outsourcing organisation will provide access and correction under the FOI Act); or that
> - the CSP will possess and control the personal information (and therefore the CSP will provide access and correction under IPP 6).[250]

6.11 Where a service provider has *not* been contractually bound to comply with the *Information Privacy Act* (for example, the service provider is the agent of the outsourcing government organisation), the outsourcing government organisation will need to give thought to how it will ensure that it can get hold of personal information in the possession of the service provider for the purposes of the contract so that the outsourcing government organisation can meet its own access and correction obligations under the FOI Act.

6.12 See OVPC's Information Sheet 01.10, *Accessing and correcting your personal information*, January 2010, for further guidance on when IPP 6 and the FOI Act apply.

Other organisations not subject to FOI

6.13 IPP 6 will also be the mechanism for dealing with access and correction requests where the organisation is not bound by the FOI Act but is nevertheless subject to the *Information Privacy Act*. This will include those organisations that fall within section 9 of the *Information Privacy Act* but fall outside of the definition of an "agency" in section 5 of the FOI Act.[251] Ministers are subject to both Acts. However, parliamentary secretaries, who are expressly subject to the *Information Privacy Act*, do not appear to be expressly covered by the FOI Act. It may be that documents held by Parliamentary Secretaries could nevertheless be accessed under the FOI Act (instead of, or in parallel with, IPP 6) if they are under the control of a Minister.

Bodies excluded by ss 5(3) and 6, FOI Act

6.14 Some organisations are expressly excluded from having to comply with the FOI Act by virtue of sections 5(3) and 6 of the FOI Act. Section 5(3) excludes offices such as those of the Public Advocate, Solicitor-General and the Director of Public Prosecutions from having to comply with the FOI Act, while section 6 similarly excludes courts acting in their judicial function. While these bodies are bound by the *Information Privacy Act* and must comply with the other IPPs (subject to any applicable exemption[252]), section 12(b) of the *Information Privacy Act* expressly states that bodies excluded by virtue of these sections 5(3) or 6 in the FOI Act are not required to comply with IPP 6.

6.15 These excluded organisations can, of course, decide to voluntarily comply with IPP 6 and provide individuals with the ability to access and correct their own personal information. This would be in keeping with the spirit of the FOI Act and *Information Privacy Act* and may otherwise assist these organisations in complying with their obligations under other IPPs by, for example, ensuring data quality (IPP 3) by giving individuals the opportunity to see and correct their information.

Other bodies not bound by the FOI Act

6.16 IPP 6 may apply to those bodies bound by the *Information Privacy Act* but excluded or not covered by the FOI Act otherwise than by virtue of sections 5(3) and 6 of the FOI Act. However, it is unclear whether provisions which exclude organisations from having to comply with the FOI Act[253] might be regarded as inconsistent with IPP 6 for the purposes of section 6(2) of the *Information Privacy Act*.

6.17 Similarly, IPP 6 obligations may apply to those bodies that have been held by a tribunal or court decision to fall outside of the operation of the FOI Act. For example, in *Re Clarkson and Office of Corrections* (1989) 4 VAR 1, the Victorian Administrative Appeals Tribunal found that the Adult Parole Board ("APB") was not a prescribed body under the FOI Act. As the APB is a section 9(1)(e) body under the *Information Privacy Act*, being established under the *Corrections Act 1986* (Vic) for a public purpose, it would therefore be bound to apply IPP 6.

6.18 As already stated, relevant exemptions may apply under the *Information Privacy Act* and IPP 6 contains a number of grounds that may be relevant to organisations' decisions about whether, and to what extent, access should be granted.

Government organisations need to make the Information Privacy and FOI Acts work together

6.19 Members of the public who want to see their personal information held by government, and who may then want to have it corrected, will not necessarily appreciate the distinction between the FOI Act and the *Information Privacy Act* when they ask for access. They should not be disadvantaged by this. The important point for the public is that they have a statutory right of access and correction, not which Act provides those rights. Determining which access/correction regime applies (the FOI Act or the *Information Privacy Act*) is the responsibility of public administrators, not the public.

6.20 Organisations are expected to assist individuals who wish to access their personal information or direct them to the appropriate body. This onus on the agency is expressly referred to in section 17(3) of the FOI Act, which states:

> It is the duty of an agency or minister, as the case may be, to assist a person who wishes to make a request, or has made a request that does not comply with this section or has not been directed to the appropriate agency or minister, to make a request in a manner that complies with this section or to direct a request to the appropriate agency or minister.

6.21 This orientation towards assisting the requester is also promoted in other sections of the FOI Act, notably sections 3(2) and 16. See also the FOI Guidelines issued by the Victorian Attorney-General, which state variously:

> Upon receipt of request: assist applicant if request is not valid.
>
> Consult or communicate with applicant when:
> - request is unclear;
> - terms are too broad;
> - if deposit is required;
> - if there will be delays;
> - if there is a cheaper, easier or faster way to obtain information sought; and
> - there is a need to give an update on progress.[254]

6.22 Many organisations covered by the *Information Privacy Act* will also be covered by the FOI Act. They will have long-established procedures and trained staff to deal with FOI requests and correction of information in documents relating to the personal affairs of the requester.

6.23 If organisations take a practical and constructive approach, the differences between the language of the FOI Act and of the *Information Privacy Act* (discussed below) should not adversely affect the majority of individuals who seek to exercise one of the most basic elements of a privacy or data protection scheme - the right to access information about themselves and the right to seek correction of it.

IPP 6.1: Right of access

6.24 Like FOI, IPP 6 starts with a presumption of comprehensive access:

> 6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that [one of the exceptions in IPP 6.1(a)-(j) applies].

6.25 The Privacy Commissioner has interpreted the meaning of "except to the extent that [one of the exceptions in IPP 6.1(a)-(j) applies]" as indicating "that Parliament intended that access to personal information...should be provided as fully as possible, subject only to the exceptions in IPP 6.1."[255]

6.26 The Explanatory Memorandum to the *Information Privacy Bill* also states:

> Organisations are required to provide access to personal information unless one of the paragraphs in sub-principle 6.1 applies.

6.27 The exceptions are discussed further below.

Providing partial or limited access

6.28 Organisations should endeavour to provide access to the extent it can. Where an organisation is proposing to withhold personal information because one of the exceptions in IPP 6.1(a)-(j) applies, consideration should be given to providing access to some extent or in some other way.

6.29 This may involve using mutually agreed intermediaries under IPP 6.3 (see paras 6:66-6:68). Or, this may involve providing access to documents after removing (or blacking out) the material that was subject to the relevant exception in IPP 6.1(a)-(j). Providing partial access after removing information is consistent with section 25 of the FOI Act, which encourages organisations to release copies of exempt documents with such deletions as to make the copy not an exempt document. See, for example, Case Study 6-1, where the Privacy Commissioner discussed ways in which partial access could be granted.

CASE STUDY 6-1: Methods of providing better access[256]

The complainant applied to the Contracted Service Provider to a Department (the CSP) for access to information held about her, and on behalf of her young children for access to personal information about them. After initially taking 112 days to respond to the request, the CSP provided part of the file but argued under IPP 6.1(b) that release of any more of the complainant's and her children's personal information would have an unreasonable impact on the privacy of other individuals.

The Privacy Commissioner considered that the CSP had not outlined any steps it had taken to consider ways in which it could have provided more extensive access to the personal information it held about the complainant and her children. The Commissioner gave examples of methods that the CSP could have used to provide fuller access. These included "notifying/gaining consent of other individuals, removing or redacting identifying information of other individuals, or considering whether or not the release of information contained in each separate document was an "unreasonable" impact on the privacy of other individuals in each circumstance."

6.30 Organisations proposing to rely on an exception might also consider whether access can be granted subject to certain agreed conditions or undertakings. For instance, where the requested information contains information that may impact on another person's privacy, consideration might be given to granting access subject to an undertaking not to further disclose that information or not to use the information except for specified purposes.

6.31 These types of mechanisms for granting limited access are also consistent with the wording of IPP 6.1, which requires access to be given "except to the extent" that a relevant exception applies.

Form of access

6.32 IPP 6 does not stipulate how access is to be given – whether through a right of inspection, copies of records containing the personal information, or records in digital form. There is a growing body of case law in the FOI area on what constitutes proper access for FOI purposes. That case law may be relevant to the question of the form of access to be provided under IPP 6.

6.33 Generally, where possible, access to personal information should be given in the form requested. In most cases, this will be through provision of paper copies of records.

6.34 However, where an individual seeks access in a particular form and it is "neither possible nor appropriate to do so," an organisation is still able to meet the requirements of IPP 6 by providing access in another form. See, for example, *A v Medical Practitioner* [2009] PrivCmrA 1, where the Australian Privacy Commissioner considered that permitting an individual to view their medical record was acceptable in the circumstances.

When is information "held" by an organisation?

6.35 An organisation is required to provide access only when it "holds" personal information about an individual. Under section 4(1), an organisation holds personal information "if the information is contained in a document that is in the possession or under the control of the organisation, whether alone or jointly with other persons or bodies, irrespective of where the document is situated, whether in or outside Victoria."

6.36 If an organisation receives a request for access but the information does not exist or cannot be found, access will not be possible. However, the organisation is expected to be able to demonstrate reasonable searches have occured (see Case Study 6-2).

CASE STUDY 6-2: Organisation cannot find information requested[257]

A woman requested a copy of an email about her which had been sent by a Local Council's senior management to staff. The Local Council refused the request under the New Zealand Privacy Act (which contains a right of access to personal information) on the basis that the email could not be found. The woman complained to the New Zealand Privacy Commissioner.

The Commissioner asked the Council to provide it with details of the search it had undertaken for the email. The Council had conducted an extensive search of its electronic system for any correspondence with entries of the woman's name, or the subject matter of the email, for a period of several months around the time when the email was sent. In addition, the Council also searched its electronic system for any emails sent by the staff members in question for the same period of time. The Local Council also advised that it had searched its hard copy files of correspondence between the woman and the Council for the same time period.

The Commissioner considered that the Council had undertaken reasonable steps to search for the information, and the Council was entitled to refuse the request on the basis that the information requested could not be found.

IPP 6.1(a)-(j): Restricting access

6.37 The exceptions limiting the right of access under IPP 6.1 are listed in IPP 6.1(a)-(j). Access may be limited to the extent that:

(a) providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) providing access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders -

by or on behalf of a law enforcement agency; or

(j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.38 It should be noted that several of these exceptions are analogous to the exemptions in the FOI Act that allow access to information to be restricted, and regard should be given to relevant FOI Act case law.

6.39 Many of the terms in IPP 6.1(a), (f), (g) and (i) were discussed elsewhere in these Guidelines. See, for instance, the discussion of "serious and imminent threat" (IPP 6.1(a)) in the section on IPP 2.1(d) and the discussion of "lawful" (IPP 6.1(f)) under IPP 1.2. "Required or authorised by law" (IPP 6.1(g)) is also discussed under IPP 2.1(f). Many of the concepts in IPP 6.1(i) relating to law enforcement matters are discussed under IPP 2.1(g).

IPP 6.1(a): Access would pose a serious and imminent threat to the life or health of any individual

6.40 The exception in IPP 6.1(a) permits an organisation to withhold access to information where access would pose a serious and imminent threat to the life or health of any individual.

6.41 The term "serious and imminent threat" is extensively considered in relation to IPP 2.1(d) (see the discussion at 2:93).

6.42 It should be remembered, however, that organisations wishing to deny access need to "provide evidence as to how the access to the material would pose a threat to the life or health" of an individual and may need to consider whether the use of an intermediary (under IPP 6.3) would overcome any serious and imminent threat to the life or health of an individual (see Case Study 6-3).

CASE STUDY 6-3: Organisation purports to restrict access due to serious and imminent threat[258]

The complainant attempted to gain access to their personal information held by a Charitable Organisation. The Organisation stated that it needed to deny access as providing access would pose a threat to the life and health to the complainant and other individuals (amongst other grounds) under National Privacy Principle 6.1(a) of the *Privacy Act* (which is substantially similar to IPP 6).

The Australian Privacy Commissioner explained to the Organisation that if it wished to deny access on the exemptions it had cited, it would need to provide evidence as to how access to the material would pose a threat to the life and health of the complainant, and was asked to consider whether use of an intermediary to provide access to the information requested was an option.

The Organisation requested the complainant nominate a health practitioner to act as an intermediary, who assessed possible threats to life and health of the complainant from the personal information contained in the records before access was granted.

IPP 6.1(b): Impact on another's privacy

6.43 The exception in IPP 6.1(b) that providing access "would have an unreasonable impact on the privacy of other individuals" is similar to section 33 of the FOI Act, allowing exemption from disclosure in order to protect personal privacy where disclosure would be "an unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person)."

6.44 Under both the FOI Act and IPP 6, the exemption is not absolute. Organisations can decide to release information where the disclosure would not be "unreasonable",[259] or the impact on an individual's privacy is not "unreasonable". Disclosure might be regarded by organisations as reasonable under the *Information Privacy Act* where other public interests override the individual's interest in privacy.

6.45 Organisations should not release information about a third party without having first considered whether the privacy of that third party may be adversely impacted by the disclosure of his or her information. In some cases, it will be apparent from the material that disclosure may have an unreasonable impact on the third party's privacy. For instance, the information may disclose quite sensitive or delicate information about the individual's criminal record or personal relationships. There may be some circumstances where it is apparent that a disclosure of a third party's identifiable details may put him or her at risk of physical or other harm. Release of a third party's home address will often not be warranted and may place him or her at risk of harm, particularly where the person works in a sensitive occupation.

CASE STUDY 6-4: An example of an unreasonable impact on a third party's privacy[260]

The complainant was asked to leave a private school as a result of an investigation by the school. After leaving, the student sought access to the personal information held by the school including details of the investigation which led to the complainant being asked to leave the school under *Privacy Act 1988* (Cth) National Privacy Principle (NPP) 6 (which is substantially similar to IPP 6).

The school argued that providing the complainant with access to the investigation documents would amount to an interference with the privacy of other individuals, as the individuals in question had provided that information on the understanding their details would not be revealed to the complainant for fear of reprisal.

The Commissioner inspected the relevant documents and formed the view that the school could rely on the exception. The Commissioner noted that the content of the documents clearly identified other individuals. The view was reached that under the circumstances providing the documents to the complainant, even with the names of the third parties suppressed, would have an unreasonable impact on the privacy of those individuals.

6.46 A useful test for assessing an unreasonable impact on the privacy of individuals was put forward by the Australian Privacy Commissioner in the following case study.

CASE STUDY 6-5: A test for unreasonable impact on a third party's privacy[261]

The complainant made an insurance claim, which was investigated and paid. The complainant sought access to personal information collected during the course of the investigation. The Insurance Company supplied a number of documents but refused to provide access to some documents, claiming release would compromise the privacy of other individuals.

The Commissioner conducted preliminary inquiries and examined the documents which had not been released.

The Commissioner outlined the following test in assessing an unreasonable impact on privacy:

In assessing whether or not the provision of access to documents containing the personal information of third parties would have an unreasonable impact on the privacy of those individuals, the Commissioner may consider factors including:

- whether the individual would expect that their information would be disclosed to the third party, including whether any assurance of confidentiality was provided;
- the extent of the impact on the individual's privacy;
- whether any public interest reasons for providing access to the information outweigh any expectation of confidentiality; and
- whether masking the identifying details of the third parties would sufficiently protect the privacy of these individuals.

The Commissioner decided that providing access to some of the documents would have an unreasonable impact on the privacy of other individuals. These documents contained personal information about witnesses to the events leading to the insurance claim. The Commissioner considered that, in this case, the individuals who provided the witness statements would not have expected that their identity would be revealed, and that masking the names of the individuals would not prevent their identification, which could be discerned from the content of the statement. The Commissioner considered that the organisation could rely on the exception to refuse access to these documents.

However, the Commissioner also found that access could be provided to some documents that identified third parties if the identifying information was masked. The Commissioner advised the Insurance Company to mask these portions before providing them to the complainant.

6.47 Organisations may not always be aware of the potential impact disclosure may have on a third party. It is good practice for organisations to notify third parties, where practicable, of any proposed disclosure of their information and to provide them with an opportunity to say why their information ought not be disclosed. This would be consistent with third party rights under section 33(3) of the FOI Act. Providing affected third parties with notice and an opportunity to object to a proposed disclosure can provide organisations with a more complete picture of the impact that disclosure may have on the safety, reputation or other interests of affected persons. This will assist organisations to determine whether the disclosure might have an unreasonable impact on the privacy of the third party.

Overcoming unreasonable impacts on privacy

6.48 Organisations should also consider whether they can overcome any potential unreasonable impact on third parties' privacy by arranging for a partial release of the information to the requester with, for instance, the references to the third parties' identifiable details removed, as discussed in paras 6:28-6:31. See also the Privacy Commissioner's decision in *Complainant AS v Contracted Service Provider to a Department* [2011] VPrivCmr 1, where the Privacy Commissioner considered ways to reduce a potential impact on the privacy of third parties (see Case Study 6-1).

6.49 Where identifiable details are removed, it is important to ensure they are removed sufficiently to de-identify an individual to remove the impact on their privacy. Sometimes removal of name may not be enough - as the third party's identity may be able to "reasonably be ascertained" from the information.[262]

IPP 6.1(c): Frivolous or vexatious requests

6.50 Access can be restricted under IPP 6.1(c) where the request is frivolous or vexatious. The ordinary dictionary meaning of "vexatious" is "not having sufficient grounds of action and seeking only to annoy" and has been adopted by the Federal Court in a similar context involving requests for information (or interrogatories).[263]

6.51 In *G v Finance Company* [2010] PrivCmrA 8, the Australian Privacy Commissioner developed a view that frivolous and vexatious requests can include those that are:

- trivial and made for amusement's sake; or
- made as a means of pursuing some unrelated grievance against the organisation; or
- repeated requests for the same information.

CASE STUDY 6-6: Access request vexatious due to repeat request[264]

The complainant requested access to personal information held by a Finance Company. The Finance Company sought to deny the complainant access on the basis that the request was frivolous or vexatious.

After outlining the above factors, the Commissioner found that the complainant had made numerous requests, over a period of four years, for access to the account statements held by the Finance Company that related to the complainant. Evidence showed that the Finance Company had provided the complainant with access to their information on at least two occasions. The Commissioner found that the request for access was a repeat request for information that had been previously provided.

While the Commissioner stated that NPP 6 (the *Privacy Act 1988* equivalent to IPP 6) does not require individuals to have a specific "purpose" for requesting access to personal information, the Commissioner considered the purpose for requesting access in this case was relevant to the Finance Company's claim that the request was vexatious.

The complainant and the Finance Company had been involved in court proceedings several years previously. The Commissioner found that the repeated requests for access were substantially, if not solely, a means of obtaining documents to revisit the earlier litigation and pursue an unrelated grievance.

The Commissioner formed the view that the Finance Company could deny the complainant access to the information as the request was vexatious.

6.52 In deciding whether to refuse access on the basis of it being vexatious, organisations should ensure they look at the circumstances of the particular request. The requester must, as the New Zealand Privacy Commissioner suggested, be patently abusing their rights to access their information rather than exercising those rights in a bona fide manner – see Case Study 6-7, where the New Zealand Privacy Commissioner found that an employer had too readily refused an employee's request for access, which he made following a particular dispute he had with the company but which the company presumed to have been motivated by the trade union as part of an unrelated industrial action.

CASE STUDY 6-7: Access request made during an industrial dispute not vexatious[265]

An employee requested access to personal information held by his employer after a dispute involving the use of a company vehicle. The company refused his request under the New Zealand *Privacy Act 1993* on the ground that it was vexatious. The employee complained to the New Zealand Privacy Commissioner.

The company had decided the request was vexatious because, at the time, it was in the middle of significant industrial action, coordinated and supported by a trade union, and the union had encouraged members to make mass requests for access under the *Privacy Act*.

The Privacy Commissioner suggested that, for a request to be refused on the grounds that it is vexatious, "the requester must be believed to be patently abusing the rights of access to information, rather than exercising those rights in a bona fide manner." The request must be considered in light of the surrounding circumstances.

The Privacy Commissioner decided that the employer had not considered all the circumstances surrounding the employee's request, having apparently relied on the timing of the request to determine it was part of the industrial action. The access request was influenced by the employee's dispute over the company car, which was unrelated to the industrial action. The request appeared to be bona fide and made in good faith. The employer therefore did not have a proper basis to withhold the information from the employee.

Organisations should focus on the character of the request, not the individual making it

6.53 In determining whether to refuse access on the basis of it being vexatious, organisations must look at the character of the *request* – not of the *requester*. IPP 6 does not entitle organisations to declare an individual to be vexatious and thereby refuse to entertain any future request for access he or she might make. Organisations must consider the merits of each request, even where it is made by a person with a history of making vexatious requests. See, for example, Case Study 6-8, where the New Zealand Complaints Review Tribunal determined that police could not refuse to consider further access requests made by a serial complainant.

CASE STUDY 6-8: Serial complainant's request to police not vexatious[266]

The complainant had a long history of making complaints and access requests to police, often concerning matters in which he had no personal involvement. At some point, police deemed he was vexatious and refused his further requests.

The complainant made an access request under the New Zealand *Privacy Act 1993* for police to disclose the identities and addresses of the complainant's assailants. Upon seeking review, the New Zealand Complaints Review Tribunal found that the complainant was entitled to have the information police held. The Tribunal found that he had suffered humiliation, loss of dignity and injury to feelings and awarded him $200.

IPP 6.1(d): Information relating to existing legal proceedings between organisation and individual

6.54 IPP 6.1(d) resembles the FOI Act's section 32 (documents affecting legal proceedings). IPP 6 was not intended to interfere with existing procedures for discovery in legal proceedings. An organisation may withhold information which relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings.

IPPs 6.1(f) and (g): Providing access would be unlawful or denying access is required/authorised by law

6.55 **IPP 6.1(f) and (g) are similar to the FOI Act's section 38, which exempts documents from disclosure where they are subject to other statutory secrecy provisions. However, IPP 6.1(f) and (g) are broader in permitting access to be refused in circumstances other than pursuant to a statutory secrecy provision. For example, where disclosure of information would breach common law or equitable obligations of confidence, it may be unlawful to provide access (see Case Study 6-9).**

CASE STUDY 6-9: Access to information withheld due to the law of confidence[267]

The complainant made an application to acquire a car dealership from an Automotive Company. When assessing the application, the Automotive Company contacted the complainant's referees, who provided information about the complainant on the condition that the information be treated confidentially.

The Automotive Company rejected the car dealership acquisition. The complainant requested access to information that the Automotive Company held about them. The Automotive Company denied access to information, arguing that providing access would constitute a breach of its duty of confidence to the referees.

The Privacy Commissioner (considering the *Privacy Act* equivalent of IPP 6, NPP 6) considered whether providing access would be unlawful or that denying access is required or authorised by or under law.

The Commissioner considered that common law and equitable obligations constitute 'law' for the purposes of the *Privacy Act*. This means if an individual's personal information was subject to an equitable duty of confidence, then an organisation would be entitled to rely on NPP 6 grounds to deny the individual access to that information.

The Commissioner considered whether the information provided by the parties met the test for an equitable obligation of confidence (and the three-step test for an equitable breach of confidence) set out by Megarry J in *Coco v AN Clark (Engineers) Ltd* and subsequent cases.

The Commissioner found that first, the information collected from the referees had the necessary quality of confidence about it, as this information contained the referees' opinions about the complainant, and was not public knowledge. Second, the information was provided by the referees in circumstances importing an obligation of confidence. The Automotive Company had prefaced each communication with the referees that the communication would remain confidential. Third, it would be an unauthorised use of the information for the Automotive Company to provide the complainant with access, as the referees had provided the information on the condition it would remain confidential.

The Commissioner formed the view that the three elements of a successful cause of action for an equitable breach of confidence were made out. As such, the Automotive Company could deny access under NPP 6.1(g) as providing access would be unlawful, in that it would give rise to an action for breach of confidence.

IPP 6.1(h): Prejudice an investigation into possible unlawful activity

6.56 **IPP 6.1(h) allows an organisation to refuse access where that might prejudice an investigation of possible unlawful activity. This enables organisations to investigate unlawful activity, such as theft or fraud, without the access request compromising that investigation.**

6.57 **The Queensland Office of the Information Commissioner provides some guidance in relation to a similar exemption under the Queensland *Freedom of Information Act 1992*:**

> The FOI Act recognises that some information about law enforcement investigations needs protection. This can include information about ongoing investigations, and secret investigative methods or procedures...There can be any number of ways in which disclosure of information before finalisation of an investigation can prejudice the investigation. For example, the premature disclosure of information about a network of contacts or informants relevant to a current investigation might undermine the investigation. In some cases, even disclosure of the fact that there is an investigation could prejudice the investigation. In those cases, the use of a "neither confirm nor deny" response may be justified... Apart from such a case, however, the existence of an ongoing investigation is not, by itself, enough to make all documents relating to that investigation exempt... The agency must show how disclosure of the particular documents claimed to be exempt could reasonably be expected to prejudice that investigation.[268]

IPP 6.1(i): Prejudice law enforcement activities

6.58 IPP 6.1(i) does similar work to section 31 of the FOI Act to guard against prejudice to certain law enforcement activities. IPP 6.1(i) is broader, however, in permitting organisations to refuse access where it is likely to prejudice matters such as the protection of public revenue and the enforcement of crimes confiscation laws. Moreover, IPP 6.1 does not include the additional provisions in section 31(2) of the FOI Act that permit disclosure of law enforcement documents in the public interest where, for example, the document reveals the use of illegal methods and other matters.

6.59 IPP 6.1(i) may be used to deny access to information identifying an informer – see the New Zealand privacy complaint in Case Study 6-10.

CASE STUDY 6-10: Revealing identity of informers may prejudice criminal investigations[269]

A man requested access to information held by the New Zealand Department of Conservation after complaints were made against him in relation to his boating activities. The Department provided him with a copy of most of the information but withheld the names of the informants. The man initially complained to the New Zealand Ombudsman, but the matter was transferred to the New Zealand Privacy Commissioner because the information (the informers' identities) was regarded as "personal information" about the man who was informed against.

During the Privacy Commissioner's investigation, it became apparent that the Department withheld the informers' names on the basis that disclosure would be likely to prejudice the investigation and detection of offences.

The Privacy Commissioner accepted that the Department, which investigates various offences under conservation and marine protection laws, relies to some extent on individuals volunteering information about possible offences. The Privacy Commissioner was satisfied that the Department's ability to detect, investigate and prosecute offences would be prejudiced if the flow of information would cease or be diminished, and disclosure of informers' names might make these informers and other potential informers less willing to provide similar information in future. This is likely to prejudice the Department's ability to enforce the laws it administers. The Department's withholding of this information was therefore not in breach of the Access Principle.

IPP 6

IPP 6.1(j): Security of Australia

6.60 IPP 6.1(j) is similar to the national security exemption in the FOI Act's section 29A. IPP 6.1(j) is narrower in that ASIO, ASIS or a law enforcement agency must request that access be withheld on the basis that granting access is likely to damage the security of Australia. The organisation who is considering withholding access under IPP 6.1(j) must be satisfied that the security or law enforcement agency is performing a "lawful security function". ASIO and ASIS's functions are set out in their respective statutes, the *Australian Security Intelligence Organisation Act 1979* (Cth) the *Intelligence Services Act 2001* (Cth).

6.61 Where the request comes from a law enforcement agency, organisations should consider the nature of the investigation. "Lawful security function" will clearly encompass investigations into terrorism offences, but it would not extend to the investigation of ordinary criminal offences that do not involve some element of national security. In those cases, IPP 6.1(i) may be relevant.

IPP 6.2: Commercially sensitive decision-making

6.62 IPP 6.2 allows organisations to give individuals an explanation for a commercially sensitive decision, rather than direct access to the information underpinning that decision where that would reveal evaluative information generated in connection with the decision-making process. For example, the UK Information Commissioner found that a request under the *Freedom of Information Act 2000* (UK) for details about how much the British Broadcasting Corporation (BBC) had spent on media training for its staff over a specific time period, as well as names of agencies or businesses that had been used for the training, was "highly likely to provide an insight into the pricing strategy of the third party for provision of training...giving the third party's competitors an advantage in bidding for future contracts (and) would prejudice the commercial interests of the third party."[270]

6.63 IPP 6.2's references to "evaluative information" and to "commercially sensitive decision-making process" will invite consideration of FOI's exemptions that deal with evaluative or pre-decision processes and with commercially sensitive information, such as under the FOI Act's section 34 relating to exemption of documents revealing trade secrets and other commercially sensitive information.

6.64 IPP 6.2 cannot be used to withhold factual personal information on which a commercial decision is based – only "evaluative information". IPP 6.2 was intended to ensure that, where individuals are adversely affected by a commercial decision, they are able to receive an explanation of the reasons for the decision. See Case Study 6-11, where the New Zealand Privacy Commissioner upheld a decision by a bank to withhold information relating to commercially sensitive information.

> **CASE STUDY 6-11: Withholding commercially sensitive information permitted**[271]
>
> The complainant asked for access to his full records in the course of a dispute with his bank. Although the Bank provided most of the records, it withheld some emails under section 28(1)(b) of the (NZ) *Privacy Act* which allows an organisation to withhold information if it would "be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information."
>
> The New Zealand Privacy Commissioner considered that it was "unclear" whether the emails in question contained the personal information of the complainant. However, the Commissioner continued on to state "even if it were personal information about him, section 28(1)(b) permitted the bank to withhold information from him. The information was commercially sensitive. Its release could clearly prejudice the Bank's commercial position."

6.65 However, access should be fully provided if the commercially sensitive information can be removed. See Case Study 6-12 where the Australian Privacy Commissioner considered the possibility of "masking" commercially sensitive documents.

> **CASE STUDY 6-12: Providing access by masking commercially sensitive information**[272]
>
> The complainant made an insurance claim, which was investigated and paid. The complainant sought access to personal information collected in the course of the investigation under National Privacy Principle (NPP) 6 of the *Privacy Act* (which is similar to IPP 6). The company refused to provide access, claiming amongst other exemptions that it would reveal commercially sensitive information.
>
> In relation to NPP 6.2, the Australian Privacy Commissioner agreed that some of the documents would reveal commercially sensitive information. The documents described the type of information the insurance company considered important in assessing claims during an investigation. The Commissioner considered these documents would be covered by the exemption.
>
> However, the Commissioner found that for some other documents containing commercially sensitive information, access could be provided to the majority of the document with the commercially sensitive components masked. The Commissioner advised the insurance company to provide access to these documents by masking the parts deemed commercially sensitive. The company agreed to the recommendation and supplied the complainant with access to the documents, some of which had portions masked.

IPP 6.3: Providing limited access through intermediaries

6.66 Where one of the exceptions in IPP 6.1(a)-(j) applies, IPP 6.3 requires organisations to, if reasonable, consider the use of mutually agreed and properly authorised intermediaries to allow sufficient access to meet the needs of both parties.

6.67 As stated earlier, an organisation should endeavour to provide full access to the extent it can. Where the organisation determines that full access to the requested information should not be granted because a relevant exception applies, the organisation should endeavour to provide more limited access through intermediaries, such as the requester's relative, lawyer or other nominated representative agreed to by the organisation. This principle was intended to provide organisations with an alternative to a complete denial of access by using "neutral parties" to convey to the requester the general nature and content of the requested information. The Explanatory Memorandum to the *Privacy Act 1988* provides some guidance:

> Where access would otherwise be denied, NPP 6.3 requires an organisation to consider whether an alternative form of access (through an intermediary) would meet the needs of both parties. The sub-principle is not intended to provide a mechanism to reduce access if access would otherwise be required. There will be some cases - investigations of fraud or theft for example - where no form of access is appropriate. In other cases, (use of an intermediary) should be considered as an alternative to complete denial of access. For example, in the health context, an intermediary could usefully explain the contents of the health record to the individual as an alternative to denying access to the health information altogether. [273]

6.68 Organisations should consider, where reasonable, whether it would be appropriate to give full access to the agreed intermediary to enable that person to assess the content in order to explain the information to the requester or determine whether partial or conditional access should be negotiated (as discussed earlier, in paras 6:28-6:31). Some guidance is provided by the Australian Privacy Commissioner (below). See also *D v Charitable Organisation* [2011] PrivCmrA 4, where an intermediary (health practitioner) was used when an organisation had concerns as to possible threats to the life and health of a complainant.

IPP 6

EXTRACT: Australian Privacy Commissioner Information Sheet (Private Sector) 5 - 2001: Access and the Use of Intermediaries[274]

Role of an intermediary

An intermediary is a person or persons acceptable to both the organisation and the individual asking for access. The role of the intermediary is to enable an individual to get access to and have the content of the personal information explained where access would otherwise have been denied. What the intermediary explains to the individual will depend on the instructions the organisation gives the intermediary. The organisation's instructions will be determined by what the exception allows.

Before using an intermediary

An organisation may have explored other ways of providing limited access to the information a person has requested before deciding to use an intermediary. These may include:

- giving access to the information but blocking out the information covered by the exception;
- giving a summary of the information excluding the information covered by the exception; or
- any other ways which would meet the needs of the organisation and the person making the request for access.

EXTRACT: Australian Privacy Commissioner Information Sheet (Private Sector) 5 - 2001: Access and the Use of Intermediaries *continued*

Considerations in deciding to use an intermediary

An organisation may decide it is not possible to give either direct access or the limited access to personal information described above. Organisations must consider, if reasonable, whether the use of an intermediary to provide access to the information requested is an option. The organisation and the individual seeking access need to agree on the intermediary.

Factors that an organisation may consider when deciding whether to use an intermediary could include:

- the nature of the exception under which an organisation may deny access. In some circumstances such as (IPP 6.1(f),(g),(h) or (i)), using an intermediary will not be appropriate;
- whether the intermediary would meet the needs of both the organisation and the individual requesting access;
- whether giving access through an intermediary would lessen a threat to life or health that the organisation believes will arise if direct access is given to the individual (where that is the relevant exception);
- whether using an intermediary would enable a level of access acceptable to the individual without revealing personal information that is covered by any exception and which the organisation does not want disclosed;
- whether a suitable intermediary, likely to be acceptable to both the organisation and the individual, is available; and
- the cost of using an intermediary.

Steps if using an intermediary

It is up to the organisation to decide what steps it will take once a decision has been reached about using an intermediary. Factors may include the kind of relationship the organisation has with the individual, the exception that will deny the individual direct access and the sensitivity of the information requested. The Privacy Commissioner suggests the following steps:

- Notify the individual of the organisation's decision. An organisation could do this orally or in writing, stating the exception that prevents direct access and suggesting the use of a mutually acceptable intermediary.
- Explain in an easily understood way:
  - the role of the intermediary;
  - what kind of access the intermediary will give the individual to personal information about them; and
  - how the procedure would work.
- Explain any costs that the individual will incur if an intermediary is used.
- Explain what the individual needs to do next.

Steps if not using an intermediary

If the organisation decides not to use an intermediary, then (IPP 6.7) would require the organisation to provide reasons for denial of access. This would involve contacting the individual orally or in writing and explaining why the request for access has been denied. An organisation could also explain any processes it has for reviewing its decision.

IPP 6.4: Access fee

6.69 Section 69 of the *Information Privacy Act* allows organisations to charge a prescribed fee for providing access, and IPP 6.4 permits the organisation to refuse access until the prescribed fee is paid. IPP 6.4 and section 69 are expressly intended to be consistent with charges under the FOI Act:

> Sub-principle 6.4 restricts the scope for organisations to charge for access to the personal information they hold. It is intended that regulations made prescribing fees for access (clause 69) would be consistent with charges under the Freedom of Information Act.[275]

6.70 Regulations prescribing fees for access can be made by the Governor in Council under section 73(2) of the *Information Privacy Act*. As of the date of this document, there are no prescribed fees for access under the *Information Privacy Act*. As a result, organisations who are required by IPP 6 to provide access are not currently entitled to charge a fee for access or to refuse access because some fee or charge has not been paid.[276]

IPPs 6.5 and 6.6: Right of correction

6.71 If an individual establishes that the information held by an organisation about him or her is not accurate, complete or up to date, IPP 6.5 requires the organisation to take reasonable steps to correct the information.

6.72 If there is a dispute as to the accuracy of the information, and the organisation and the individual cannot agree about whether the information is wrong, the individual may ask the organisation to place a statement with the information claiming it is not accurate, complete or up to date. IPP 6.6 requires the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date.

6.73 Cases under Part V of the Victorian FOI Act – and equivalents in other jurisdictions – have developed practical approaches to handling such requests. Organisations responding under IPP 6 should educate themselves about these approaches. An example is provided in Case Study 6-13.

> **CASE STUDY 6-13: Correcting information**[277]
>
> The complainant was insured by an Insurance Company. The complainant discovered that her individual insurance file contained nine insurance claims relating to a policy she was not aware of. The policy had been taken out by the complainant's former partner and spanned a period of ten years.
>
> The complainant contacted the Insurer and asked it to remove her name from the policy and remove the listings from her insurance file. The Insurer refused.
>
> The Commissioner investigated the matter. The Insurer argued that it considered the complainant was insured on the relevant policy, and in such cases, the Insurer's normal practice was to list the claims on both insureds' individual insurance files. However, as a result of the investigation it contacted the principal insured who confirmed separation ten years ago, and that the insured had not removed the complainant from the insurance policy.
>
> The Insurer removed the complainant from the policy and removed the claims from the individual insurance file.

IPP 6

The relationship between IPP 6 and IPP 3

6.74 Providing individuals with a right of correction helps to ensure that organisations do not act on wrong information or misrepresent personal facts about individuals so as to adversely impact individuals about whom decisions are later made. The rationale for providing individuals with a right of correction to ensure the data quality of their information is maintained was discussed previously in these Guidelines under IPP 3.

6.75 The section dealing with IPP 3 should be referred to where appropriate, as it deals with many of the terms that are used in IPP 6.5 and 6.6 – notably, the terms "accurate, complete and up to date" and "reasonable steps". Also refer to Case Study 3-12 under IPP 3, which illustrates the interaction of IPP 3 and the right of correction in IPP 6, as well as the practical application of the terms used in both Principles.

Reasonable steps to correct information

6.76 The use of the term "reasonable steps" in IPP 6.5 and 6.6 was not intended to impose an onerous obligation on organisations in respect of information that was inaccessible and never to be used. On the other hand, the term "reasonable steps" was intended to be broadly interpreted to discourage the persistence of poor quality data and to encourage organisations to respond to data quality issues that individuals bring to their attention. See the extract from the *Australian Privacy Commissioner Information Sheet (Private Sector) 4 – 2001: Access and Correction*.

EXTRACT: Australian Privacy Commissioner Information Sheet Private Sector 4 – 2001: Access and Correction[278]

Reasonable steps to correct personal information

When considering what reasonable steps to take in meeting an individual's request to correct personal information, an organisation could consider:

- It has obligations under NPP 3 (similar to IPP 3) to take reasonable steps to make sure personal information it collects, uses and discloses is accurate, complete and up to date. This means that, when it comes to using or disclosing personal information, the onus is on the organisation to make sure information is correct.
- Allowing poor quality information to remain on a record may have adverse consequences for the individual and/or the organisation. For example, organisations may find that, in leaving poor quality information on the record, they breach NPP 3 (similar to IPP 3).
- Correction is not necessary if the information is no longer being used. However if this is the case, the organisation should consider destroying or de-identifying information it no longer needs (subject to any legal requirements to retain the information). Destroying or permanently de-identifying personal information that is no longer needed is a requirement under NPP 4.2 (similar to IPP 4.2).
- An organisation could discuss with the individual concerned the reasons it thinks it is inappropriate to delete or alter the original information. The organisation and individual may then be able to agree on alternative ways of noting the discrepancy regarding the accuracy of the information in a way that satisfies the needs of both parties.
- If an individual establishes with an organisation that information about them is incorrect, the organisation should consider correcting the information with any third parties that it has passed the information onto.

Reasonable steps in attaching a correction statement to a record

If an individual asks the organisation to attach a statement to the information stating that they don't believe the information is correct, the organisation must take reasonable steps to do so. Organisations may like to consider the following when considering reasonable steps to take:

- If the individual disputing the information provides a very extensive statement that an organisation cannot easily attach, the organisation could put a mark or a note on the information to indicate that the statement exists and where it can be found.
- An organisation would ordinarily need to associate the individual's statement about the disputed information in such a way that whenever that information is handled in the future it will be easy to see that the individual does not agree that this particular part of the personal information is accurate, complete or up to date.

Practical ways to correct information

6.77 The Victorian Privacy Commissioner adopts two aspects of the advice of the Federal Privacy Commissioner's *Plain English Guideline to Information Privacy Principles 4-7*[279] (which apply to federal government agencies and are adjusted here to substitute "organisation" for "Agency").[280]

6.78 On deciding how to correct information, whether by deletion, amendment or addition:

> If an [organisation] decides, either on its own initiative or on the request of the subject of the information, that a record needs to be changed in some way, it must decide whether to delete the record, amend it or add to it.
>
> Where possible, an [organisation] should generally retain both the old information - while clearly marking it as no longer current - and the new information; and should record the date and reason the old information was superseded. This allows the [organisation] to trace changes made to the information for audit purposes, and is useful when reviewing decisions made using the information, or dealing with complaints or enquiries related to it.
>
> There may however be some particularly sensitive cases in which the mere existence of the earlier incorrect information could be detrimental. In such cases, deletion may be the only appropriate option. It is essential if information is deleted that a notation is made of the reason for the deletion, and the officer responsible for the decision.[281]

6.79 On adding the individual's statement to the personal information the organisation holds about that individual on a database:

> There are a number of options for making annotations to information held in a database. The preferred one is for the statement provided by the person to be directly attached to the relevant information in the database. Other options are for the statement to be included in a field in the particular record, such as a free text comments field, or in a separate file of comments linked to the principal database. The least convenient option would be for the record in the database to be flagged to indicate that a statement provided by the person is associated with the record, and where that statement is to be found.
>
> The important thing is that it should be clear to anyone accessing the information that it has been disputed, on what grounds it has been disputed, and why the [organisation] has decided not to correct, delete or add to the information as the person asked.[282]

6.80 The critical requirement is that anyone accessing the information or record should be aware that it has been disputed, on what grounds it has been disputed, and why the organisation has decided not to correct, delete or add to the information as the person asked.

6.81 These techniques are models for compromise and potential touchstones for conciliation, in this sometimes difficult context of access and correction of personal information.

6.82 Unlike Part 5 of the FOI Act, IPP 6 does not require organisations to correct information that is misleading – provided it is otherwise accurate, complete and up to date. There may be cases, however, where information may give a misleading impression *because* it is inaccurate, incomplete or out of date, as discussed by Judge Rendit of the Victorian County Court, in *G v Health Commission of Victoria:*

> Obviously there is a difference between a misleading impression and an inaccuracy, although each will overlap the other to a large extent. One can readily envisage circumstances where the recorded facts are inaccurate, and also give a misleading impression. Equally, recorded facts which are accurate may yet give a misleading impression, either because of incompleteness or because of the language used in recording the facts, whilst accurate, yet would convey a misleading impression.[283]

6.83 Where it is difficult to determine whether information is misleading or whether it is inaccurate, incomplete or out of date, organisations are encouraged to err on the side of correcting (or placing a statement with) the information in accordance with IPPs 6.5 and 6.6.

IPP 6.7: Reasons for denial of access or refusal to correct

6.84 Where an organisation refuses a request for access or correction, IPP 6.7 requires the organisation to provide reasons for its decision.

6.85 The organisation may refuse a request for correction on what it regards as good grounds. It may, for instance, conclude that one more of the exceptions under IPP 6.1 applies and refuse access. Alternatively, the organisation may conclude that the individual has not established that the information is not accurate, complete and up to date, as IPP 6.5 requires. The organisation may believe that it has taken reasonable steps to correct and that the individual's request is unreasonable. The organisation may decide that to correct by expunging information would be contrary to proper records management practices and would harm the integrity of the file.

6.86 The validity of such decisions will turn on the particular circumstances. But as a matter of general policy, organisations should be sensitive to the intensity with which an individual may feel that the personal information – which can include an opinion, not just factual material – is wrong and remains uncorrected and beyond the individual's control in the hands of the organisation.

IPP 6.8: Time limit for responding to request for access or correction

6.87 IPP 6.8 sets a time limit for organisations to respond to a request for access or correction. Organisations must respond to a request as soon as practicable, but no later than 45 days after receiving the request.

6.88 Organisations should endeavor to provide access or agree to correct, or provide reasons for a denial of access or refusal to correct, within this time limit. IPP 6.8 does not, however, demand that organisations finalise their response within 45 days, provided they notify the requester within this timeline of the reasons for any delay in responding.

6.89 An organisation's reasons for delay in responding to a request for access or correction will likely be relevant to whether the Privacy Commissioner declines to entertain a complaint alleging a breach of IPP 6 because of what might be regarded as an unreasonable delay. An example where the Privacy Commissioner took a dim view of an organisation's delay is discussed in Case Study 6-14.

CASE STUDY 6-14: Reasons for delay in providing access insufficient[284]

The complainant contacted a Contracted Service Provider (CSP) to a Department for access to personal information held about her and her young children (on their behalf). The complainant initially attempted to make her request under the *Freedom of Information Act*. The CSP responded that it was not subject to that Act. The complainant then requested information under the *Health Records Act*. The CSP responded that it did not hold any "health information" as defined by that Act. The complainant then made a request under IPP 6.

The CSP responded after 24 days, explaining that they were seeking legal advice. Fifty-seven days after the complainant's request, the CSP again wrote to the complainant informing her that they were still awaiting finalisation of legal advice and would communicate with her. One hundred and twelve days after making the request, the complainant made a complaint to the Privacy Commissioner alleging the organisation had failed to provide access (IPP 6.1) and had not provided adequate reasons for the delay within 45 days of receiving her request (IPP 6.8).

The Privacy Commissioner referred the complaint to conciliation. Although it was not necessary to decide (as the organisation had provided a level of access in the interim) the Commissioner expressed concern about the length of time taken to respond to the request and questioned whether "obtaining legal advice" was a sufficient reason for delay under IPP 6.8.

Who is entitled to exercise the rights of access and correction under IPP 6?

Access to and correction of one's own information

6.90 The right of access and correction under IPP 6 can only be exercised by the person whose information is contained in the record. However, if that person is incapable of making a request for access or correction, an authorised representative may make the request on that person's behalf (sections 64(2), *Information Privacy Act)*. The role of authorised representatives in making decisions on behalf of others is discussed in the Key Concepts - Consent section at paras KC:44-KC:50.

Individuals only have right of access to their own "personal information"

6.91 It should be remembered that the IPP 6 only requires the organisation to provide access to "personal information". This is defined in section 3 of the *Information Privacy Act* as "information or an opinion (including information or an opinion forming part of a database), that is recorded in any form or whether true or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion." This means that organisations are only required to provide access to "personal information" as defined by the Act. This contrasts with the FOI Act where the right of access to information is wider than IPP 6 – to any "document" of an agency.[285]

6.92 Additionally, organisations must ensure that the person applying for access is actually who they say they are. There may be a possibility that an individual may attempt to use IPP 6 to access information about another individual by impersonating that person. Organisations should establish an individual's identity before providing access.[286] Failure to do so could breach IPP 4.1 (Data Security).

Accessing a child's personal information

6.93 Children and young people are entitled to seek and correct their own information where they are capable of understanding the general nature and effect of making a request to access or correct their personal information. Where they are incapable of understanding the nature and effect of such a request, an authorised representative (such as a parent) can make the request on their behalf under section 64(2).

6.94 An access request made under IPP 6 by a parent or other authorised representative must be done on behalf of the child and not motivated by the parent's own interests. See Case Study 6-15, where VCAT considered an access request made by a father to his daughter's file under Health Privacy Principle 6 of the *Health Records Act 2001* (Vic) where he asserted that he was entitled to it as her parent and guardian. VCAT found that the father had no independent right of access to his child's records, nor did he have standing to bring a complaint when he was denied that access.

CASE STUDY 6-15: Father not entitled in his own right to access his daughter's file[287]

In January 2005, a father sought access to his daughter's file, held by a registered psychologist. The application was unsuccessful, so he wrote to the Office of the Health Services Commissioner in October 2005, requesting the Commissioner's assistance to gain access to these records. In February 2006, the father asked the Health Services Commissioner to refer the matter to Tribunal.

The access request was made in the context of the father and his now former wife having undergone an apparently "tumultuous divorce following separation in 1999".

The father confirmed to VCAT that his complaint under the *Health Records Act 2001* (Vic) for a denial of access to his daughter's was made in his own right, not on his daughter's behalf.

VCAT found that the complaint provisions of the *Health Records Act* [equivalent to sections 25 and 27 of the *Information Privacy Act*] enabled a person to complain to the Health Services Commissioner about an interference with *that* person's privacy. The daughter was entitled to access her records and, if she were capable of making a complaint about refused access, she could do so. However, the *Health Records Act* does not entitle a parent to make a complaint in his or her own right, only *on behalf of* the child. The father therefore had no standing to bring a complaint about the psychologist's refusal to grant him access to his daughter's health information.

VCAT also referred to the mechanism for seeking access on behalf of a child set out in section 85 of the *Health Records Act* [equivalent to section 64 of the *Information Privacy Act*]. VCAT found that the father was entitled only to seek access to his own records or to his daughter's records if he applied on her behalf as an authorised representative. But that was not what he had done in seeking access to his daughter's records.

VCAT also cautioned that, had the father applied in a different capacity, it would not be safe to assume that a different conclusion would have been reached.

6.95 Similar findings have been made by privacy and information commissioners in other jurisdictions where parents have sought access to their child's information, often against a background of custodial or other family law proceedings.[288]

6.96 See, for example, the Canadian case involving an access request made to the Calgary Health Region.[289] In this case, the Alberta Information and Privacy Commissioner carried out an extensive review and consideration of the meaning of relevant terms (such as "understanding") and evolving case law (including *Gillick's* case, referred to earlier in the section on Consent), and other data protection and privacy laws (including in Victoria and other Australian jurisdictions). The Alberta Information and Privacy Commissioner determined that the mother did not have authority to access her 15½ year old daughter's psychological records and accordingly had no standing to ask for a review of the decision of the health provider refusing to give her access. The mother had failed to discharge the burden of proof to show that her daughter lacked understanding of the nature and consequences of exercising her own rights under the privacy legislation.

6.97 In assessing whether a minor has sufficient capacity to exercise her own right of access under the Alberta health privacy legislation, the Alberta Information and Privacy Commissioner suggested a number of relevant factors and indicated that the requisite level of understanding was not an onerous one:

> In order to determine whether the Applicant's daughter is capable of understanding the nature and consequences of exercising her rights or powers under [the *Health Information Act*, or "HIA"], I must have regard to factors such as the individual's age, maturity, independence, level of understanding and the nature and complexity of the HIA rights or powers. In my view, the level of understanding that is required for an individual to understand the nature and consequences of exercising rights or powers under HIA is not a particularly onerous standard.[290]

6.98 The fact that a parent is not independently entitled under IPP 6 to access their child's records otherwise than as agent for the child does not mean that there is no authority in the *Information Privacy Act* for parents to obtain information about their children.[291]

IPP 6 Notes

[245] New Zealand, Privacy Commissioner (Bruce Slane), *Necessary and Desirable: Privacy Act 1993 Review,* Report of the Privacy Commissioner on the First Periodic Review of the Operation of Privacy Act, 1998, Auckland: Office of the Privacy Commissioner, page 74.

[246] See sections 34, 39, 42 and 45 of the *Information Privacy Act 2000* (Vic).

[247] Clause note to IPP 6 in the Explanatory Memorandum accompanying the *Information Privacy Bill*. Also see the Second Reading Speech, Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000 (John Brumby, Minister for State and Regional Development), page 1907.

[248] Second Reading Speech to the *Information Privacy Bill 2000* (Vic), Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000, page 1907 (John Brumby, Minister for State and Regional Development).

[249] Contracted service providers will only be bound by the *Information Privacy Act 2000* (Vic) if the contract contains a provision of a kind referred to in section 17(2) of the *Information Privacy Act*.

[250] Privacy Victoria, *Outsourcing and Privacy – a guide to compliance,* May 2011, page 17.

[251] "Agency" is defined in section 5 of the *Freedom of Information Act 1982* (Vic) to mean a department, council or prescribed authority. "Prescribed authority" is further defined section 5 of the *Freedom of Information Act 1982* (Vic) and includes a body corporate established for a public purpose under an Act (excluding certain bodies, such as a Royal Commission), and certain persons and bodies declared by regulations to be a prescribed authority. Prescribed authorities are listed in the schedule to the *Freedom of Information Regulations 1998* (Vic). Bodies or persons may also be deemed to fall within, or outside, the FOI Act by virtue of other laws or pursuant to sections 5(2)-(4), *Freedom of Information Act 1982* (Vic).

[252] Notably, organisations that investigate or prosecute criminal offences and breaches of other laws that carry a sanction or penalty may not be required to comply with IPP 6 where they reasonably believe non-compliance is necessary: section 13, *Information Privacy Act 2000* (Vic).

[253] For example, section 56 of the *Rural Finance Act 1988* (Vic) exempts the Rural Finance Corporation from having to comply with the FOI Act.

[254] Victorian Attorney-General, *The Freedom of Information Act 1982 - Attorney-General Guidelines on the Responsibilities and Obligations of Principal Officers and Agencies,* December 2009, available at http://www.foi.vic.gov.au.

[255] *Complainant AS v Contracted Service Provider to a Department* [2011] VPrivCmr 1.

[256] *Complainant AS v Contracted Service Provider to a Department* [2011] VPrivCmr 1.

[257] *Woman complaints about Council refusing her request for an email (Case Note 210778)* [2010] NZPrivCmr 5 (1 May 2010).

[258] *D v Charitable Organisation* [2011] PrivCmrA 4.

[259] And, in the case of the *Freedom of Information Act 1982* (Vic), after having given the affected individual an opportunity to object in accordance with the "reverse FOI" mechanism in section 33(3) of the *Freedom of Information Act*. There is no equivalent obligation under IPP 6 to notify individuals of a proposed release of their information, although the obligations to provide notice of usual disclosures (IPPs 1.3 and 1.5) may be relevant.

[260] *A v Private School* [2008] PrivCmrA 1.

[261] *C v Insurance Company* [2006] PrivCmrA 3.

[262] See *Information Privacy Act 2000* (Vic) s 3 (definition of personal information). In *C v Insurance Company* [2006] PrivCmrA 3, the Australian Privacy Commissioner considered that "masking the names of individuals would not prevent their identification, which could be discerned from the content of the statement."

[263] *Aspar Autobarn Cooperative Society v Dovala Pty Ltd* (1987) 74 ALR 550 at 554.

[264] *G v Finance Company* [2010] PrivCmrA 8.

[265] *Employee's access request considered "vexatious" by employer (Case Note 18109)* [1999] NZPrivCmr 14.

[266] *Proceedings Commissioner v Commissioner of Police*, unreported, Complaints Review Tribunal, Decision No 18/2000, CRT 10/00, 10 July 2000, discussed in the New Zealand Human Rights Commission's *Annual Report 2000* at page 33, available at http://www.hrc.co.nz. The case was also discussed in a paper presented by Paul Roth in *New Zealand Twins: Access Review Processes For Personal And Third Party Requests*, given at an International Symposium on Freedom of Information and Privacy, Auckland, 28 March 2002, and re-published in the [2002] PLPR 21, the May 2002 issue of *Privacy Law and Policy Reporter*.

[267] *O v Automotive Company* [2009] PrivCmrA 18.

[268] Office of the Queensland Information Commissioner, *FOI Concepts – Law Enforcement Investigations*, October 2006, available at http://www.oic.qld.gov.au.

[269] *Man complains about Department of Conservation's refusal to disclose informants' identities (Case Note 80156)* [2005] NZPrivCmr 2.

[270] UK Information Commissioner's Office, Decision Notice – BBC, 24 August 2011, Case Ref: FS50375439, available at http://www.ico.gov.uk.

[271] *Bank refuses access to commercially sensitive information (Case Note 91538)* [2007] NZPrivCmr 1.

[272] *C v Insurance Company* [2006] PrivCmrA 3.

[273] Explanatory Memorandum accompanying the *Privacy Amendment (Private Sector) Bill 2000* (Cth).

[274] Office of the Australian Privacy Commissioner, *Information Sheet (Private Sector) 5 – 2001: Access and the Use of Intermediaries*, available at http://www.privacy.gov.au.

[275] See also the clause note to IPP 6 in the Explanatory Memorandum accompanying the *Information Privacy Bill 2000*. See also the Second Reading Speech, which states that the ability to charge fees in IPP 6 "is intended to allow consistency with the fees prescribed under the Freedom of Information Act": Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000, John Brumby, Minister for State and Regional Development, page 1907.

[276] These Guidelines are current to 1 November 2011. Organisations should check whether regulations have been made under the *Information Privacy Act* after this date, that authorise the charging of a fee for access under IPP 6.

[277] *P v Insurer* [2010] PrivCmrA 19.

[278] Office of the Australian Privacy Commissioner, *Information Sheet (Private Sector) 4 – 2001: Access and Correction,* available at http://www.privacy.gov.au.

[279] Australia, Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4-7*, February 1998, available at http://www.privacy.gov.au.

[280] Victorian organisations are reminded, in the context of correction decisions, that the *Public Records Act 1973* (Vic) prevails over the *Information Privacy Act* to the extent of any inconsistency (*Information Privacy Act* s 6).

IPP 6

[281] Australia, Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4-7,* February 1998, page 19, available at http://www.privacy.gov.au.

[282] Australia, Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 4-7,* February 1998, page 20, available at http://www.privacy.gov.au.

[283] *G v Health Commission of Victoria*, Unreported judgment, County Court of Victoria, 13 September 1984 at page 10.

[284] *Complainants AS v Contracted Service Provider to a Department* [2011] VPrivCmr 1.

[285] *Freedom of Information Act 1982* (Vic) s 13 (Right of Access).

[286] See Office of the Victorian Privacy Commissioner Information Sheet 07.08, *Confirming Identity and Privacy: A Guide for Organisations*, December 2008, available at http://www.privacy.vic.gov.au.

[287] *Callanan v McLoughlan (General)* [2006] VCAT 1099.

[288] See, for example, *Father seeks access to daughter's file recording sexual abuse allegations (Case Note 12946)* [1998] NZPrivCmr 9; and *Woman complains about CYFS withholding details of daughter's sexual abuse allegations (Case Note 25473)* [2003] NZPrivCmr 12.

[289] *Re: Calgary Health Region, Orders F2005-017 & H2005-001*, 19 June 2006, Review Number 3353 & H0307, available at http://www.gov.ab.ca.

[290] *Re: Calgary Health Region, Orders F2005-017 & H2005-001*, 19 June 2006, Review Number 3353 & H0307, para 74, available at http://www.gov.ab.ca.

[291] The *Information Privacy Act* allows organisations to disclose personal information without the child's consent in a number of situations. Access by parents to their child's school records has already been discussed elsewhere in these Guidelines (see paras KC:46 and 2:23). The *Information Privacy Act* permits disclosure to parents where the disclosure is authorised under one of the grounds specified in IPP 2.

IPP 7: Unique identifiers

7.1 IPP 7 deals with the assignment, adoption, use and sharing of unique identifiers. This Principle is expressly intended to act as a safeguard against pervasive data matching across government:

> Principle 7 provides a safeguard against the creation of a single identifier that could be used to cross match data across all government departments.[292]

7.2 Information privacy law has some of its roots in human rights law, which in turn is a response to systematic abuses of human rights often characterised by abuse of unique identifiers. The public's distrust of unique identifiers is deep seated and was one element of resistance to a national identification card in the 1980s – the "Australia Card debate".[293] Community concern led to the demise of the proposed identity card and a compromise was ultimately struck involving the introduction of the federal *Privacy Act* and a strengthened tax file number system with strict controls on the collection, recording, use and disclosure of tax file number information. More recently, the concern over the use of unique identifiers has been reignited with the use of a national health identifier as part of the "e-health" access system.[294]

7.3 IPP 7 addresses most directly the concerns behind the expression "just a number in a system". Privacy is part of the way a person builds and maintains his or her unique identity. To be an individual, treated as such, is an aspect of human dignity. Assigning numbers to people may threaten to dehumanise them.

7.4 A significant risk in using unique identifiers is the possibility of "function creep", in that the incremental use of an identifier can lead to more personal information being gradually linked over time to that identifier. For more discussion on function creep, see KC:77-KC:80.

Meaning of "unique identifier"

7.5 A "unique identifier" is defined in the Schedule to the IPA to mean:

> an identifier (usually a number)
>
> assigned by an organisation to an individual
>
> uniquely to identify that individual
>
> for the purposes of the operations of the organisation
>
> but does not include an identifier that consists only of the individual's name
>
> but does not include an identifier within the meaning of the *Health Records Act 2001*.

7.6 An identifier can be a sequence of numbers, letters and/or characters used to identify or refer to a person. An individual's name is not considered to be a unique identifier under the definition in the *Information Privacy Act*. However, an identifier that is comprised in part of a person's name or initials may be regarded as a unique identifier. For example, a statistical linkage key comprised of a person's initials and date of birth (eg, JWH-26071939) is likely to be regarded as a unique identifier. Statistical linkage keys are discussed further at paras 7:14-7:15.

7.7 The most common Victorian example of a unique identifier is a driver's licence number issued by VicRoads. Identifiers are often found on identity or entitlement documents issued by public and private sector agencies. Examples include student identity cards, health care and concession cards, library cards, membership cards, credit cards, and passports. Identifiers are usually included on certificates that mark various events in one's life, such as birth, marriage, or the attainment of citizenship. Identifiers are also used in conjunction with registration schemes for professionals, police, and others who must obtain permission to work in the community (such as volunteers who work with children).

7.8 Tax File Numbers are also a good example of unique identifiers but, as noted earlier, are treated differently from most other unique identifiers in that these identifiers are subject to purpose-built legislation that specifically prohibits collection, use or disclosure except for limited purposes.[295] The handling of tax file numbers is also subject to specific, binding guidelines issued by the Australian Privacy Commissioner under section 17 of the Commonwealth *Privacy Act 1988*.

7.9 IPP 7 will not apply to unique identifiers that fall within the meaning of "identifier" in the Victorian *Health Records Act 2001*. Instead, Health Privacy Principle 7 will apply to the assignment, adoption, use and disclosure of identifiers. For example, a patient identifier assigned to a person undergoing medical treatment will be regulated by the *Health Records Act* rather than the *Information Privacy Act*. The exclusion of health identifiers from the definition of unique identifier in the *Information Privacy Act* was expressly intended to ensure that there is no duplication in the regulation and handling of personal information under both laws.[296]

7.10 A unique identifier may also be comprised of a biometric. Biometrics are unique patterns of bodily features that can be used for the purpose of identification or recognition. Examples include biometric data obtained when taking fingerprints, iris scanning, DNA profiling, facial imaging, and using voice recognition technology. Biometrics have been, and are likely to continue to be, used to identify individuals and/or verify their entitlement for various purposes, such as to access a secure facility. For example, some prisons and remand centres in Victoria utilise a combination of fingerprint and iris scanning to verify the identity of visitors and staff.[297]

Data matching and the IPPs

7.11 Organisations considering the use of unique identifiers in order to engage in data matching, whether in order to carry out research or "cleanse" data or some other purpose, should refer to the relevant sections in these Guidelines relating to data matching. See, for example, the discussion of data linkage and research at paras 2:82-2:87 and data cleansing at paras 3:38-3:48. See also the discussion of using de-identified or coded data at paras KC:24-KC:28.

7.12 Transparency and notice will be important in any data matching exercise, so regard should be given to obligations under IPPs 1.3, 1.5 and 5. Further, where data matching is likely to lead to the aggregation of information (or profiles), consideration should be given to minimising collection to what is necessary, fair and not unreasonably intrusive (IPPs 1.1 and 1.2). The rationale for data matching various information sources should be articulated and any collection or re-use of data should be lawful and clearly authorised (IPPs 1.2 and 2).

7.13 IPP 7 aims to strike a balance between the potential privacy invasiveness of data matching, linking and profiling with the clear benefits to organisations in assigning or adopting identifiers to efficiently administer their functions. Consent plays a part (in IPPs 7.2 and 7.3), facilitating transparency of, and individual control over, some data matching activities that are carried out. The potential for agencies to unnecessarily collect identity documents or identifiers is reduced by the tests of necessity (in IPPs 7.1, 7.2 and 7.3) and, in IPP 7.4, relevance or separate legislative authority. Where appropriate, organisations should refer to the discussion of "consent" and "necessary" in the Key Concepts section of these Guidelines (see paras KC:38-KC:71 and KC:81-KC:87, respectively).

Statistical linkage keys

7.14 In some cases, using a code or stripping identifiers from the data may not be sufficient to de-identify a person to external parties, or to render the information anonymous or unidentifiable (and thereby removing it from the reach of the *Information Privacy Act*). For example, a statistical linkage key comprised of an individual's initials and date of birth may not adequately anonymise a person, especially if the key can be "unlocked" by anyone holding these details (which are routinely provided by individuals, for example, to access government services or benefits).

7.15 A scoping audit conducted by OVPC in February 2005 found that statistical linkage keys were used by 1 out of every 4 government agencies surveyed.[298] Organisations should ensure that linkage keys are not purported to be used to anonymise data where re-identification is reasonably possible.

IPP 7.1: Assignment of a unique identifier

7.16 IPP 7.1 states that an organisation must not assign unique identifiers to individuals unless that assignment is necessary to enable the organisation to carry out any of its functions efficiently.

7.17 The discussion of "necessary for functions" in IPP 1.1 should be referred to. Again, an organisation should be clear about both the need and the function. Necessity requires more than desire or convenience. Adapting the test suggested in the *Ng case*,[299] an organisation should ask whether the assignment of a unique identifier is reasonably required or legally ancillary to the accomplishment of the organisation's functions. It is important to be clear and specific about which functions the assignment is in aid of, and whose functions are being carried out. IPP 7.1 does not authorise organisations to assign identifiers to assist in the efficient conduct of another organisation's functions. Identifiers should only be assigned where relevant to the assigning organisation's functions.

7.18 Organisations should also ask whether issuing a unique identifier is necessary in order that the organisation can carry out its functions "efficiently", that is, with minimum waste or effort. The test of efficiency in carrying out any function will require an assessment of efficiency from the perspective of both the organisation and those with whom it deals.

7.19 A sense of proportionality should always be maintained. Needing to distinguish between a few similar names should not inevitably lead to the conclusion that everyone dealing with the organisation needs a unique identifier. To illustrate, suppose there are two Jane Smiths from the same suburb. Rather than assigning a unique identifier to the organisation's entire client base, a more proportionate response should be adopted. After practical steps like consulting the two Janes, they can be Jane Smith A and Jane Smith B in the organisation's database and everyone else can remain as names not numbers. Another response may be to confirm the currency of the information, as it may be that the two Janes are the same person appearing twice in the database, or one is no longer a client or employee and should be removed. The assignment of unique identifiers without reviewing the integrity of the data may have inadvertently contributed to data quality issues going undetected.

7.20 In some sensitive or delicate contexts, unique identifiers may be better for privacy than names. An individual's case can be coded with a number or other identifier so that its facts can be dispersed within a wider group in the organisation for more contributions and a perhaps better result. Only a limited few need ever know the name behind the number. If carefully coded, the identity of the individual concerned should not be reasonably ascertainable to the recipients. Using de-identification and coded information is discussed earlier at paras KC:24-KC:28.

IPP 7.2: Adoption of an existing unique identifier

7.21 The potential privacy risks associated with profiling and data matching grow when a unique identifier assigned by one organisation is adopted by other organisations. The risks are reduced by limiting the proliferation of any one identifier across multiple agencies.

7.22 This is the aim of IPP 7.2, which states:

An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless -

(a) it is necessary to enable the organisation to carry out any of its functions efficiently; or

(b) it has obtained the consent of the individual to the use of the unique identifier; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.23 Limiting the spread of particular identifiers also acts to reduce the potential extent of harm where identity theft occurs. If a unique identifier is inappropriately accessed or disclosed, whether inadvertently or by theft, it can potentially be used to obtain access to, and to misuse, other information holdings. See Case Study 7-1, where a phone company adopted an identity number as a default password for an online service.

CASE STUDY 7-1: Identity card number adopted as default password[300]

A mobile phone company provided an online billing service to customers through its website. In order to log into the system, a customer had to enter his or her mobile phone number and a password. The customer would then have access to his or her account information, including detailed call records. However, the default password consisted of the first six digits of the customer's Hong Kong Identity Card number. A customer complained that a debt collector accessed his account through the online service and made nuisance calls to him and his friends.

The Hong Kong Privacy Commissioner cautioned against the use of identity card numbers as default passwords as, for various reasons, the number may be disclosed and known to others. If an organisation decides to use identity card numbers in this way, additional security steps should be taken to safeguard the data. Customers should be made fully aware of the default password arrangement and reminded of the importance of changing the password to prevent unauthorised access to their accounts.

"Adopt as own" distinguished from recording identifiers

7.24 Unique identifiers and identity documents are commonly requested by organisations seeking to establish or verify identity. If anonymity is not a lawful and practicable option, sometimes it may be sufficient to simply sight an identity document and perhaps note the fact that it was sighted, in which case the *Information Privacy Act* will not apply as the information is not recorded. At other times, it may be necessary to retain a copy of the identity document or make a note of the identifier, in which case the *Information Privacy Act* will apply.

7.25 IPP 7.2 will not prevent an organisation from recording identifiers as evidence of identity, or prevent an organisation from requiring identification required by law. However, the organisation is not permitted to incorporate those identifiers into its own system to organise its own information holdings or match with data held by other organisations unless IPP 7.2(a), (b) or (c) applies.

IPP 7.2(a): Necessary to efficiently carry out functions

7.26 The authority in IPP 7.2(a) for using identifiers where necessary to efficiently carry out the organisation's functions has already been discussed earlier under IPP 7.1 (see paras 7:16-7:20).

IPP 7.2(b): Consent

7.27 Consent ensures transparency and gives individuals an opportunity to assess the legitimacy of the proposed use and the risk of unacceptable profiling or data matching. The organisation that must get consent is the organisation that wants to adopt the unique identifier, not the organisation that assigned it. In IPP 7.3(c), the consent of the individual must be to the particular use or disclosure proposed. Consent will need to be specific, informed, voluntary, current and given by someone with the necessary legal capacity. Consent for the adoption of another organisation's unique identifier should not be part of "bundled" consent. See the earlier discussion of consent in the Key Concepts section of these Guidelines (paras KC:38-KC:71).

IPP 7.2(c): Outsourcing

7.28 A unique identifier assigned to individuals by a contracted service provider may be adopted by the outsourcing organisation if the unique identifier was created by the service provider in the performance of its obligations to the organisation under a State Contract. The effect should be to restrict the creation of unique identifiers to the outsourcing organisation, the result aimed at in IPP 7.1.

7.29 IPP 7.2(c) does not operate in reverse. That is, a contracted service provider may not *adopt as its own* the unique identifier used by the outsourcing organisation. If it were otherwise, a contracted service provider to, say, VicRoads, might be able to adopt as its own the drivers' licence numbers of millions of Victorians.

7.30 A service provider may, in the course of performing obligations to the outsourcing organisation under a State Contract, come to have knowledge of an organisation's unique identifiers for individuals.[301] But the service provider cannot adopt the unique identifier as its own. Organisations should ensure that contracts with service providers deal appropriately with the security and return or disposal of unique identifiers that the service provider may acquire in the course of the contract.

IPP 7.3: Use or disclosure of a unique identifier

7.31 The aim of IPP 7.3 is to limit the spread of identifiers in order to avoid the creation of a universal identifier. IPP 7.3 states:

> 7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless -
>
> (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or
>
> (b) one or more of paragraphs 2.1(d) to 2.1(g) applies to the use or disclosure; or
>
> (c) it has obtained the consent of the individual to the use or disclosure.

7.32 While IPP 7.2 restricts an organisation from adopting existing unique identifiers as its own, IPP 7.3 more broadly restricts the use and disclosure of any identifier that the organisation holds. For example, if an organisation conducts an identity check and records a driver's licence number, IPP 7.2 restricts that organisation from then categorising the person's information by reference to his or her driver's licence number, while IPP 7.3 restricts the organisation from otherwise using or disclosing the driver's licence number for its own purposes or to other organisations.

7.33 Use and disclosure of other organisations' unique identifiers is only permitted in the three circumstances outlined in IPP 7.3(a)-(c).

IPP 7.3(a): Necessary to fulfil obligations to the other organisation

7.34 IPP 7.3(a) allows use or disclosure of an identifier assigned by another organisation where this is necessary for the organisation holding the identifier to fulfil its obligations to the organisation that assigned the identifier.

7.35 The meaning of "necessary" has been discussed already (see paras KC:81-KC:87, 7:16-7:20 and 7:26). The term "obligations" connotes more than an understanding, habit, arrangement, course of conduct or administrative practice. It encompasses statutory and contractual obligations.

7.36 To illustrate: A school collects certain information from a teacher when employing her, including a teacher registration number issued by the Victorian Institute of Teaching (VIT). The school has a statutory obligation to inform VIT if any action is taken against the teacher in response to an allegation of serious misconduct. In communicating with VIT about a disciplinary action taken, the school's disclosure of the teacher's registration number would be in accordance with IPP 7.3(a).

IPP 7.3(b): Use or disclosure in certain public interests

7.37 IPP 7.3(b) allows an organisation to use or disclose unique identifiers for certain public interest purposes listed in IPP 2.1(d)-(g), namely where:

a IPP 2.1(d) – the organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious (and, in the case of individuals, imminent) threat to life, health, safety or welfare;

b IPP 2.1(e) – the use or disclosure is a necessary part of the organisation's own investigation into reasonably suspected unlawful activity, or in reporting its concerns to relevant persons or authorities;

c IPP 2.1(f) – the use or disclosure is required or authorised by or under law;

d IPP 2.1(g) – the organisation reasonably believes that the use or disclosure is reasonably necessary to assist a law enforcement agency to carry out certain law enforcement functions.

7.38 These IPP 2.1 grounds are discussed at paras 2:93-2:158 and 2:161-2:165.

IPP 7.3(c): Use or disclosure by consent

7.39 IPP 7.3(c) allows the organisation to use or disclose a person's unique identifier where it has obtained the consent of the individual.

7.40 Consent has already been discussed in some detail (see paras KC:38-KC:71). The organisation that wants to use or disclose the identifier must obtain the individual's consent, not the organisation that assigned the identifier. Consent must be voluntary, informed, specific, current and given by someone with legal capacity. The consent of the individual must be to the particular use or disclosure proposed.

Other uses are not authorised under IPP 7.3

7.41 Note that IPP 7.3 is narrower in scope than IPP 2.1. Although some of the IPP 2.1 grounds have been carried over, not all have. Notably, use and disclosure under IPPs 2.1(a), (b) and (h) have not been incorporated into IPP 7.3.

7.42 If a unique identifier is sought by ASIO and ASIS (IPP 2.1(h)), for example, then organisations should look to another heading, such as the investigation of unlawful activity (IPP 2.1(g)) or authority under law (IPP 2.1(f)).

7.43 Non-consensual use and disclosure of a person's unique identifier is not otherwise permitted, whether for public interest research (IPP 2.1(c)) or for reasonably expected related purposes (IPP 2.1(a)). If an organisation wishes to use or disclose an identifier outside of the law enforcement and public safety context or without authority of law, then consent should generally be sought.

IPP 7.4: Demanding identifiers be provided in order to obtain a service

7.44 IPP 7.4 states that an organisation must not require an individual to provide a unique identifier in order to obtain a service unless:

a the provision of the unique identifier is required or authorised by law; or

b the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

7.45 IPP 7.4, like other paragraphs in IPP 7, aims to reduce the prospect of unique identifiers being adopted across government and thereby becoming a de facto universal identity number. More specifically, IPP 7.4 aims to prevent organisations from coercing individuals into providing their identifiers by threatening to otherwise withhold services. Organisations must not make service delivery contingent on individuals providing their identifier unless they have authority under law, or the identifier is relevant to the purpose for which it was assigned.

7.46 For example, a university may require a student to provide their student identity number in order to access various student services such as library borrowing, use of the sports facility, access to counselling services or child care. Here, the student identity number is relevant to establishing eligibility to access services provided by or on behalf of the university.

7.47 However, making services such as library borrowing or use of the gym facilities contingent on a student providing their driver's licence number, for example, is unlikely to be permissible under IPP 7.4. Similarly, a council providing free parking permits or travel vouchers to employees working in the local area are unlikely to need the employees' driver's licence as eligibility is based on the place of employment, irrespective of whether the employee drives or is driven to work.

7.48 Organisations who require service users to provide their driver's licence or other identifiers should ask whether, and if so how, the organisation's service is connected to the reason for which the identifier was assigned. For example, how is the organisation's service related to being eligible to drive (in the case of a licence) or travel (in the case of a passport) or receive health benefits (in the case of Medicare or health care cards)? If a connection is not apparent, then organisations should check whether they have authority under law. See Case Study 7-2, which involves a decision of the Hong Kong Privacy Commissioner relating to the demand that identity card numbers be provided when residents applied for an entrance card to access their apartment building.

CASE STUDY 7-2: Demanding residents provide identity card numbers to obtain electronic access cards unnecessary and excessive[302]

A property management company in a private housing estate installed electronic readers that required residents to have a door access card or door key to enter the building. Residents applying for a door access card had to register their names, telephone numbers, and Hong Kong Identity Card numbers with the management company. One resident objected to the collection of his identity number and complained to the Hong Kong Privacy Commissioner.

The property management company argued that it was necessary to collect the number in order to prevent any harm to residents and to safeguard against damage or loss on the part of the company in case the access card fell into the wrong hands. If that occurred, the company would be able to identify the resident and seek an indemnity for any claims that might be made by a victim of some crime.

The Hong Kong Privacy Commissioner found that the possibility and extent of loss or damage speculated by the management company should be realistically justified. If an access card were misused for criminal purposes, the management company would be able identify or trace the responsible cardholder through the original flat owner who had applied for the card, or take action directly against the flat owner where appropriate. The Privacy Commissioner considered it was unnecessary and excessive to collect the identity card numbers of all residents simply because an electronic door access system was installed.

7.49 If the identifier is neither relevant nor legally authorised, organisations should refrain from demanding identification be produced by individuals seeking to obtain a service. This includes situations where an organisation uses identity documents as "security" while someone is using a service. IPP 7.4 prohibits the organisation from demanding identifiers be produced, irrespective of whether the organisation subsequently records the information.

7.50 Excessive and unnecessary collection of unique identifiers may also be contrary to the obligations in IPP 1, which require collection of personal information to be minimised to what is necessary, relevant, fair and not unreasonably intrusive. An unnecessary and unauthorised demand for an identifier to be produced may also be contrary to IPP 8 (Anonymity).

IPP 7 Notes

[292] Second reading speech accompanying the introduction of the Information Privacy Bill into Parliament: Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000 (John Brumby, Minister for State and Regional Development), page 1907. See also the clause note to IPP 7 in the Explanatory Memorandum accompanying the Information Privacy Bill 2000.

[293] For a discussion of the Australia Card proposal, its subsequent defeat, and more recent proposals, see the federal Parliamentary online briefing paper by Roy Jordan (Law and Bills Section), *Identity Cards*, E-brief (online only), issued February 2006 and last updated 8 June 2011, http://www.aph.gov.au/library/intguide/LAW/IdentityCards.htm.

[294] See the *Healthcare Identifiers Act 2010* (Cth), *Healthcare Identifiers (Consequential Amendments) Act 2010* (Cth) and *Healthcare Identifiers Regulations 2010* (Cth). See the Office of the Victorian Privacy Commissioner's *Submission to the Senate Community Affairs Committee on the Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010*, March 2010, and Office of the Victorian Privacy Commissioner, *Submission to the Australian Health Mininster's Advisory Council on its Healthcare Identifiers and Privacy*, August 2009, available at http://www.privacy.vic.gov.au.

[295] See, for example, the *Taxation Administration Act 1953* (Cth), which makes it an offence for tax file numbers to be used or disclosed for unauthorised purposes, and places restrictions on unauthorised requests for a tax file number to be quoted. The use of tax file numbers is also regulated under the *Data-matching Program (Assistance and Tax) Act 1990* (Cth), which authorises the use of tax file numbers in data matching between the Australian Taxation Office and a number of Commonwealth agencies that provide welfare and assistance.

[296] See the clause note to section 107 in the Explanatory Memorandum accompanying the *Health Records Act 2001* (Vic).

[297] For a further discussion on biometrics and privacy, see Timothy Pilgrim, Deputy Privacy Commissioner, Speech delivered to the Biometrics Institute, 21 November 2007, available at http://www.privacy.gov.au.

[298] Office of the Victorian Privacy Commissioner, *Victorian Public Sector Data Matching Audit*, Audit 01.05, February 2005, page 3.

[299] *Ng v Department of Education* [2005] VCAT 1054 at para 84.

[300] *Identity card number adopted as default password, Case No. ar0203-8* [2002] HKPrivCmr 3.

[301] This may be a use or disclosure by the outsourcing organisation that conforms to IPP 7.3(a), where the contracted service provider is itself an organisation by virtue of section 9(j) of the *Information Privacy Act*.

[302] *Collection of identity card numbers of residents applying for electronic entrance cards by property management company, Case No. ar0405-2* [2004] HKPrivCmr 2.

IPP 8: Anonymity

8.1 IPP 8 states:

> Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

8.2 The underlying objective of the Anonymity Principle is to maximise the individual's control in his or her interactions with government and to minimise government's intrusion into the life of the individual. IPP 8 was explicitly intended to "preserve" and "protect", where lawful and practicable, individuals' ability to remain anonymous in transactions with government organisations.[303] This is particularly relevant as the use of monitoring and tracking technologies and surveillance becomes more prevalent.

Relationship between anonymity and other IPPs

8.3 Where an organisation allows individuals to transact anonymously, the benefits are mutual. The individual transacts without giving up any control over his or her personal information. The organisation does not incur any of the obligations that follow from collection of personal information under the other IPPs, such as ensuring appropriate data security under IPP 4. Where organisations purport to collect and use anonymous data, they should ensure that the information is not reasonably identifiable or reasonably capable of being re-identified through, for example, linkage to other data sets. (For a further discussion of the meaning of anonymous data, see the earlier section in Key Concepts at paras KC:24-KC:28. See also paras 7:14-7:15 and 7:20, for a discussion of the use of unique identifiers to de-identify a person's identity.)

8.4 Providing an anonymity option is also consistent with the obligations under IPP 1.1 that organisations should not collect personal information unless this is necessary for one or more of its functions or activities. If an organisation can achieve its intended function or activity without collecting personal information and allow an individual to remain anonymous, it should do so.

8.5 IPP 8 is also relevant to the conduct of human research under IPP 2.1(c). As discussed at paras 2:59-2:61, consent does not become an issue where researchers collect information anonymously – whether this is directly from the individuals concerned, or indirectly using existing data sets held by other organisations.

8.6 IPP 8 should be read in conjunction with IPP 5 and IPP 1.3(f). IPP 8 does not explicitly state that an organisation must "offer" an anonymity option; rather, an organisation must "have" an anonymity option where it is lawful and practicable. However, the concepts of transparency in IPP 5 and the requirement to take reasonable steps to notify individuals under IPP 1.3 when collecting information suggests that if an organisation has an anonymity option, it should be offered at the appropriate time to allow the individual to make an informed decision.

"Transactions"

8.7 "Transactions" should be interpreted broadly to include the interactions and dealings between the individual and the organisation, whether or not they involve an exchange in a commercial sense.

8.8 Examples of transactions where the preservation of anonymity can be an issue to be weighed up with any need to identify, surveil or track individuals include:

a paying for goods and services – can you offer the option of paying anonymously by cash? See Case Study 8-1.

b using a computer for word processing or internet browsing – do you really need to know what users are working on, or what websites they visit? Do you need to store a user's IP address?

c travelling on public transport or along public roadways – how do you ensure that members of the public can continue to travel anonymously, especially where valid tickets are held and no road laws are breached?

d walking along streets, through parks and attending other places open to the public – to what extent can law-abiding individuals remain anonymous in a crowd, when CCTV is installed?

e accessing and obtaining copies of publicly available government records – do you allow individuals to anonymously access to government policies and procedures, including where these are made available online over the internet?

f making inquiries to government authorities – do you need to record a name, utilise caller-ID, install a "cookie", or take a photograph of a person who calls, emails, or attends your office to request general information about accessing government services or exercising their rights?

g interacting with government online – can individuals interact anonymously, or do you require individuals to provide personal information before they are able to interact with, or contact, the organisation?

h expressing views and concerns at public meetings – do you have to record every speaker's identity in the minutes? Is it necessary to collect personal information about someone who complains about a general issue?

i use of monitoring or location-based tracking technology – if the organisation uses global positioning tracking of organisations' vehicles, does it allow a person to turn off the GPS at certain times, for example, on that person's lunch break?[304]

8.9 As always, whether the option of anonymity should be offered will depend on the context. In general, the option for transacting anonymously should be made available wherever this is "lawful and practicable". In many cases, collecting some of the above information will be unnecessary for one or more of the organisation's functions or activities under IPP 1.1 – see para 1:85.

IPP 8

CASE STUDY 8-1: Collection of personal information despite request for anonymity[305]

A complainant attended two performances at a theatre, a body established for a public purpose under statute. On both occasions, he was asked for his name, address, email address and telephone number, despite paying with cash. Staff of the theatre informed him that refusal or failure to provide the requested information would result in him being refused entry to the venue. The complainant complained at the time about the collection of his personal information, but the complaint was not logged and was not escalated further. He was admitted to the venue, however, as he already had an account under his name with the theatre.

The complainant complained to OVPC, arguing that the theatre had breached IPP 1.1 by collecting unnecessary personal information about him, and failing to provide him with the option of transacting anonymously with the organisation under IPP 8.1.

In response to the complaint, the theatre argued that the staff at the ticketing booth at the time were interviewed and there was some question as to whether the incident had occurred. However, the theatre did have a transaction record under the complainant's name for the performances in question. The theatre also stated it did not have a chance to respond to the complaint, as the complainant had only complained to staff at the box office, and had not escalated the complaint higher.

Given the factual disagreements between the parties and the issues raised under the *Information Privacy Act*, the Privacy Commissioner considered that she could not exercise her discretion to decline the complaint, and referred the matter to conciliation. The Commissioner noted that the failure to escalate a complaint within the organisation was a not sufficient reason to decline the complaint.

The matter was resolved at conciliation, with the organisation agreeing to review its procedures for collecting personal information from customers.

"Lawful and practicable"

8.10 "Lawful" and "practicable" have already been considered in these Guidelines – see paras 1:35-1:37 and KC:91-KC:93, respectively.

8.11 An organisation may not be in a position to offer an anonymous option if that would be contrary to law. An Act or regulation may require that identifying information be collected before an individual is permitted to transact with the organisation. Registering for a profession or applying for a licence are examples where anonymity is simply not an option.

8.12 However, there will be many cases where identification is not required by law, giving organisations an opportunity to consider whether it is practicable to give individuals the option to remain anonymous.

8.13 Assessing whether it is practicable to offer an anonymous option will involve a weighing up of a number of considerations. Cost is likely to be an issue, but it is not the only issue. Prudence will need to be exercised when examining the various public interests in favour of anonymity, as compared to any countervailing interests. Just as there are legitimate uses of anonymity, so too are there legitimate reasons for seeking identification or making anonymous options conditional.

8.14 Anonymity has long been recognised as supporting privacy and other public interests such as voters using secret ballots, those with drug and alcohol dependencies seeking counselling, police encouraging witnesses of crime to come forward, members of the community informing authorities of public health and safety incidents and whistleblowers reporting concerns about corruption or serious misconduct.

8.15 Conversely, it has also been recognised that anonymity is not always an appropriate option. There are often legitimate reasons justifying the identification of individuals: investigating incidents involving serious criminal activity, combating money laundering through financial institutions, ensuring the transparency of donations to political campaigns, and preventing the spread of infectious diseases.

8.16 Every organisation subject to the IPPs will need to give some thought to providing the option of anonymity but the conclusions they reach about whether it must be offered in particular contexts will depend on the functions of the organisation, the purpose of the interaction and the role of identifying information in the interaction.

8.17 It may be that some necessary information can be collected to, for instance, determine the quality of, or need for, services. Consider carefully what information you require and whether this needs to be collected in an identified way. For example, it may be sufficient to ask a person for their suburb or postcode, or to survey individuals anonymously about their views about a service provided or an event attended.

8.18 Where identification is required to establish eligibility for a service or benefit, it might be sufficient just to sight a document and perhaps record that the particular document was sighted, rather than to record or copy the personal information contained on the document. Again, whether or not the collection of the information is necessary for the organisation's functions or activities under IPP 1.1 should be considered. See OVPC's Information Sheets 07.08, *Confirming Identity and Privacy: A Guide for Organisations*, December 2008 and 08.08, *Establishing Your Identity and Privacy: A Guide for Individuals*, December 2008.

8.19 Consistent with the importance of control in privacy and with the role of consent in other IPPs, an individual can waive the option to remain anonymous and provide their identifying information.[306] The important thing is that organisations provide the option of anonymity and, where individuals choose to identify themselves, to ensure that any identifying information is appropriately handled in accordance with the IPPs. See Case Study 8-2.

CASE STUDY 8-2: Mishandling of identifying information after anonymity option declined[307]

A woman residing in a small rural community contacted the customer service officer of a local council to report a leaking tap in the public toilets and the fact that her son had tripped and hit his head on the wet floor. The woman was asked at the outset whether she wanted to make her report anonymously. She decided to identify herself, saying later that she did so because she wanted a record of the incident concerning her son, but that she did not expect that in doing so, an employee of the council without a "need to know" would have access to it.

The customer service officer forwarded a report, including the woman's name, to the relevant business unit supervisor. The supervisor then forwarded the report to an employee who was asked to coordinate the repairs. The alleged unauthorised disclosure was by this employee to his spouse.

The woman heard about the disclosure when the employee's spouse brought up the incident with the woman in the presence of friends at a local community facility. The employee's spouse allegedly accused the woman of complaining about her husband's work. The woman was concerned that as a result of the disclosure, another member of the small community wrongly believed that the complaint had been about a particular person's work, rather than about a public facility that posed a safety risk.

Although the complaint primarily concerned the Data Security Principle (IPP 4) and whether the council had taken reasonable steps to protect information from unauthorised disclosure, the Privacy Commissioner commented that, in circumstances such as this, in which a council is required to respond to a report of a fault in a public facility, it is not necessary to the efficient repair of the fault for the identity of the person who reported the fault to be so widely circulated among council employees. In other circumstances, such as where the fault relates to the property of the person making the report, it is likely to be necessary (and often expected) that identifying information will be circulated to a wider range of employees or contractors so that repairs can be undertaken efficiently and with consultation.

The Commissioner noted that the impact of wide circulation of personal information within organisations and unauthorised disclosure outside them can be greater in small communities where people are more likely to know each other and names are more easily recognised.

The council agreed to amend its incident reporting procedures to limit who has access to personally identifying incident reports, and to provide appropriate training for relevant employees. The council also undertook to continue its policy of allowing members of the public to anonymously report public health and safety matters.

8.20 See also OVPC's Information Sheet 03.05, *Personal Information in Complaint Handling*, September 2005, which deals with offering anonymous options and minimising the circulation of necessarily collected identity details in the broader context of handling complaints from the community about neighbourhood and other disputes.

8.21 In determining whether it is appropriate to offer the option of remaining anonymous, consider first whether the practice to date has been one of anonymity. Is a new technology or initiative about to be implemented that alters this state? In principle, the same options for anonymous transactions should be available in the online world as in the offline world. That is, if individuals can access information in a library without identifying themselves, they should be able to do the same where the information is made available over the internet. Websites also should not have mandatory fields where they are not required (for example, when an individual registers on a website).

8.22 As the key test for collection is necessity under the *Information Privacy Act* (IPP 1), organisations should continually be on the lookout for opportunities to introduce (or reinstate) an ability for individuals to engage in anonymous transactions. Reviewing information flows and *why* the organisation collects and needs certain personal information may highlight areas in which an individual could transact anonymously. Not allowing anonymous interactions and requiring individuals to provide personal information increases the risk of data loss in the case of a data security breach.

8.23 Where unqualified anonymity is not practicable, alternative means of promoting the interests underpinning IPP 8 should be considered, such as using pseudonymity and limited retention of identifiable information. The use of pseudonyms, where lawful and practicable, can enable individuals to transact by using a fictitious name that conceals their true identity. For example, individuals may use a fictitious or "pen name" to make an email inquiry or request for information. However, where pseudonymity is being considered, consider whether the information needs to be collected at all. Data quality issues under IPP 3 might also be relevant where the organisation is collecting information that may not necessarily be accurate.

8.24 Organisations that are determining how best to give effect to IPP 8 should also consider the relevance of other rights (such as those under the Victorian *Charter of Human Rights and Responsibilities 2006*).

8.25 Providing an anonymous option will not always be appropriate. Determining the circumstances when anonymity will be appropriate requires a careful balancing between what can be done within existing legal and technological constraints, and what should be done to promote and protect privacy and other fundamental rights and public interests. Any restriction on the ability to transact anonymously should be limited to what is necessary and proportionate to protect the various interests at stake, while ensuring that less restrictive means are always considered.

IPP 8 Notes

[303] See the note to IPP 8 in the Explanatory Memorandum, and the Second Reading Speech to the *Information Privacy Bill 2000*, Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000, page 1907 (John Brumby, Minister for State and Regional Development).

[304] See Office of the Victorian Privacy Commissioner Information Sheet 02.08, *Privacy and Global Positioning System Technology*, June 2008.

[305] *Complainant AV v A Body Established For A Public Purpose* [2011] VPrivCmr 4.

[306] Note that collection must nevertheless be necessary to the organisation's functions or activities. Consent cannot be used to sanction a breach of IPP 1.1.

[307] *Complainant N v Local Council* [2004] VPrivCmr 8.

IPP 9: Transborder data flows

9.1 IPP 9 regulates the transfer of data to someone who is outside of Victoria – either interstate or overseas. In this context, the term "data" means personal information. The flow of data must be from the organisation to a person or body who is outside Victoria.

9.2 The development of new technologies, the most obvious of which has been the internet, combined with a rise in the outsourcing of services, has meant that transborder data flows between organisations have become increasingly common.

9.3 IPP 9 will not restrict transfers to the individual who is the subject of the information. As with other disclosures, organisations should be mindful of any overriding statutory or other duties of confidentiality or secrecy that might restrict such a transfer, as well as ensuring that data security obligations under IPP 4 are met.

9.4 IPP 9 does not apply where both the sender and the recipient are part of the same organisation, such as when an organisation communicates with or transfers information to staff who are located or travelling interstate or overseas. The remaining protections of the *Information Privacy Act* apply to Victorian public sector organisations regardless of the location of their information collection and handling practices.[308]

9.5 IPP 9 aims to ensure that, when personal information travels, privacy protection travels with it. Quality (IPP 3), security (IPP 4), proper use (IPP 2) and accountability all still matter when personal information is transferred outside Victoria. But Victoria's privacy law will not apply to information after it is received by someone who is not subject to the *Information Privacy Act*. IPP 9 is about organisations taking steps to ensure that safeguards are in place *before* the information leaves the protections of the *Information Privacy Act*.

9.6 A Victorian law that requires transborder transfers of personal information will override IPP 9 to the extent of any inconsistency.[309] Commonwealth laws may also prevail over the *Information Privacy Act*. Mutual assistance laws, for example, may provide an alternative mechanism for authorising international data transfers relating to criminal investigations and prosecutions, and recovery of the proceeds of crime.[310] Exemptions in the *Information Privacy Act* may be relevant as well, such as where police reasonably believe it is necessary not to comply with IPP 9 when carrying out particular law enforcement activities, or where courts or tribunals carry out their judicial or quasi-judicial functions.

9.7 Other than under other Victorian or Commonwealth laws, personal information may be transferred under any of six grounds set out in IPP 9:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply—

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

9.8 In June 2006 the OVPC released guidelines on *Model Terms for Transborder Data Flows of Personal Information*. The Guidelines list and discuss in detail the six bases on which personal information may be transferred to someone outside Victoria. IPP 9.1(a)-(f) are alternatives. Only one need be met, although in practice several may be fulfilled at once.

9.9 IPPs 9.1(a) and (f) will commonly overlap. Consent (and implied consent) play a role in IPPs 9.1(b) and (c). Two other grounds will require the organisation to anticipate the interests of an individual who is not party to the contract (IPP 9.1(d)) or the likelihood that the individual would give consent if it were practicable to seek it from him or her (IPP 9.1(e)).

9.10 Unlike IPPs 9.1(a) and (f), transfers under IPPs 9.1(b)-(e) are not expressly required to be accompanied by privacy protections. While such transfers must only occur where it is in the interest or for the benefit of the individual, there remains a risk that the individual's information may, once outside of Victoria, be used or otherwise handled in a manner that is inconsistent with the IPPs. Inconsistent handling of personal information may, in some circumstances, adversely affect the personal privacy of individuals, and individuals may have no (or only a limited) avenue for seeking redress outside Victoria.

9.11 IPP 9.1 – like other provisions in the *Information Privacy Act* – will be interpreted in a manner that is compatible with the privacy and other rights of the individual, in so far as this is consistent with the purpose and objects of the *Information Privacy Act*.[311] Where possible, organisations should endeavour to ensure privacy protections accompany any transfer. Where such protections are not in place, and the organisation seeks to rely on IPPs 9.1(b)-(e) for the transfer, it is expected this would only occur where the individual's interests in favour of the transfer override their interest in protecting the privacy of their information, or where the privacy risk is relatively small. Examples of transborder data flows that might involve a serious risk to personal privacy include those that:

a involve vast amounts of personal information;

b involve information of uneven quality;

c involve information about vulnerable persons;

d involve sensitive information (defined in the IPPs to include personal information such as racial and ethnic origin, political opinions, sexual preferences, and criminal record);

e utilise insecure methods of transfer;

f store information on foreign servers or in the "cloud";

g carry a risk of broader dissemination to entities that are not required or otherwise committed to protecting individuals' privacy, such as being transferred to a jurisdiction that allows a foreign government to access the data;[312]

h carry a risk of identity theft or financial harm; or

i carry a risk of harm to a person's life, safety, liberty, reputation or livelihood.

9.12 In principle, these types of transfers should be accompanied by a similar level of privacy protection as can be found in the IPPs.

9.13 An organisation that proposes to transfer information outside of Victoria must also comply with the other IPPs. For instance, it should consider whether it would be reasonable to take any additional steps prior to the transfer to safeguard the data from misuse and loss, and from unauthorised access, modification and disclosure as required by IPP 4. In some cases, it may not be possible to take reasonable steps to comply with IPP 4 given the lack of control over the data, and therefore it would not be reasonable to transfer the data.

Outsourcing and agency

9.14 Organisations are increasingly outsourcing some of their functions or services to external service providers (usually, but not always, a private sector organisation). Where a Victorian government organisation outsources a function or service to a service provider, it can either:

a bind the service provider to the *Information Privacy Act* by including a "section 17"[313] clause in a State contract (making the service provider a 'contracted service provider' for the purposes of the *Information Privacy Act*); or

b permit the service provider to act as the Victorian government organisation's agent.

9.15 Where such an agency arrangement exists, IPP 9 will not usually apply, even if the service provider is located overseas and personal information is transferred outside of Victoria. A typical example of an agency arrangement (where IPP 9 will not apply) is where a Victorian government organisation seeks to store personal information in a server outside of Victoria with a cloud service provider. If the cloud service provider is merely storing the data so that the Victorian government organisation can access it remotely (known as "at rest" data), the cloud service provider will most likely be an agent of the government organisation, rather than a contracted service provider.

9.16 Acts that are done or practices that are engaged in on behalf of a Victorian public sector organisation by its employees or agents, acting within the scope of their actual or apparent authority, are taken to be acts or practices of the Victorian public sector organisation.[314] An organisation will remain entirely responsible for any breach that occurs, even if the breach is caused by the service provider. This increases the risk for organisations as it may not have physical control of the data and yet be entirely liable. For more information, see Privacy Victoria's *Outsourcing and Privacy: A Guide to Compliance Under the Information Privacy Act*, Edition 1, May 2011.

9.17 Note that even though IPP 9 does not usually apply to agency arrangements where information is transferred or held overseas, the privacy protections travel with it as the other IPPs must be complied with (for example, IPP 4). For more information on cloud computing, see the OVPC, Information Sheet 03.11, *Cloud Computing,* May 2011.[315]

9.18 Even with an agency arrangement, an organisation should have a contract in place to ensure that the organisation's agent complies with the IPPs. The OVPC's *Model Terms for Transborder Data Flows of Personal Information* (discussed below in more detail) contains some useful guidance and standard clauses that can be used in contracts, such as ensuring access and correction, audit rights and breach notifications.[316]

IPP 9.1(a): Recipient bound by principles substantially similar to the IPPs

9.19 IPP 9.1(a) permits organisations to transfer data where they reasonably believe the recipient is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of information that are substantially similar to the IPPs.

9.20 Organisations should check whether the proposed recipient is covered by a privacy law that is comparable to the *Information Privacy Act*. Note that not all Australian jurisdictions have privacy laws in force. As at 1 September 2011, privacy statutes exist in Victoria, New South Wales, the Northern Territory, Tasmania, Queensland and the Commonwealth (which also covers public sector organisations in the Australian Capital Territory).[317] South Australia has no privacy laws currently in place, but has adopted administrative privacy standards which have some application to South Australian state public sector organisations. These standards may not, however, provide enforceable rights for individuals whose privacy is breached. Western Australia has neither a privacy law nor administrative standards in place. In 2007, the *Information Privacy Bill 2007* (WA) was introduced to the Western Australian Parliament, but it was not passed.

9.21 If you have queries about the application or coverage of privacy laws operating in other jurisdictions, you are encouraged to seek independent legal advice. You may also wish to contact the relevant oversight body or responsible government agency – see the Table on page 168, current as at 1 September 2011. You can also refer to OVPC's Information Sheet 05.10, *Privacy Regulation Across Australia,* December 2010, which compares the privacy principles that operate under the Victorian and Commonwealth privacy laws.

	Privacy Laws or Standards	Oversight Body	Responsible Government Agency
VIC	*Information Privacy Act 2000* (Vic) www.legislation.vic.gov.au	Office of the Victorian Privacy Commissioner www.privacy.vic.gov.au	Department of Justice, Victoria www.justice.vic.gov.au
	Health Records Act 2001 (Vic) www.legislation.vic.gov.au	Office of the Health Services Commissioner, Victoria www.health.vic.gov.au/hsc	Department of Human Services, Victoria www.dhs.vic.gov.au
NSW	*Privacy and Personal Information Protection Act 1998* (NSW); *Health Records and Information Privacy Act 2002* (NSW) www.legislation.nsw.gov.au	Office of the New South Wales Privacy Commissioner www.lawlink.nsw.gov.au/pc	Attorney-General's Department, New South Wales www.lawlink.nsw.gov.au/agd
QLD	*Information Privacy Act 2009* (Qld) http://www.legislation.qld.gov.au	Office of the Information Commissioner, Queensland www.oic.qld.gov.au	Department of Justice and Attorney-General, Queensland www.justice.qld.gov.au/dept/privacy.htm
TAS	*Personal Information Protection Act 2004* (Tas) www.thelaw.tas.gov.au	Ombudsman, Tasmania www.ombudsman.tas.gov.au	Department of Justice, Tasmania www.justice.tas.gov.au
SA	No privacy law, but see Cabinet Administrative Instruction to comply with Information Privacy Principles (originally issued in 1989, re-issued in 1992) www.archives.sa.gov.au/privacy/principles.html	Privacy Committee, South Australia www.archives.sa.gov.au/privacy/committee.html	State Records of South Australia www.archives.sa.gov.au/privacy
WA	No privacy law or administrative privacy regime	Not applicable	Department of the Attorney-General, Western Australia www.justice.wa.gov.au
NT	*Information Act 2002* (esp Part 5) www.dcm.nt.gov.au	Office of the Information Commissioner, Northern Territory www.infocomm.nt.gov.au	Department of Justice, Northern Territory www.nt.gov.au/justice
ACT	*Privacy Act 1988* (Cth) www.comlaw.gov.au	Office of the Australian Information Commissioner www.oaic.gov.au	Attorney-General's Department, Commonwealth www.ag.gov.au
	Health Records (Privacy and Access) Act 1997 www.legislation.act.gov.au	Australian Capital Territory Community and Health Services Complaints Commissioner www.healthcomplaints.act.gov.au/hcc	Department of Health, Australian Capital Territory www.health.act.gov.au
CTH	*Privacy Act 1998* (Cth) www.comlaw.gov.au	Office of the Australian Information Commissioner www.oaic.gov.au	Attorney-General's Department, Commonwealth www.ag.gov.au

IPP 9

9.22 Where a privacy law operates in the recipient's jurisdiction, organisations should be aware that, while there is likely to be many similarities, there may also be some significant differences that can impact on a particular data transfer. For example, the recipient may be exempt under the privacy law operating in their jurisdiction, or that law may authorise certain uses or disclosures that may not be regarded as appropriate or legitimate in Victoria. These types of issues are discussed further in the sections that follow.

9.23 The Victorian Privacy Commissioner has no legislative authority to deem a privacy law, scheme or contract as providing substantially similar privacy protection for the purposes of IPP 9. Nor does the Victorian Privacy Commissioner have any authority to issue a "whitelist" of persons or bodies who would be regarded as subject to adequate protections (or "safe harbours") for the handling of personal information. Each case will need to be assessed on its merits, taking into account the circumstances of the particular data transfer that is proposed or has been undertaken.

9.24 Judgments will need to be made in each case about the extent to which the recipient is subject to the relevant law, binding scheme or contract; the extent to which principles are upheld effectively under that law, binding scheme or contract; and the degree to which the relevant principles are sufficiently similar to Victoria's IPPs to merit the description "substantially similar". These elements are essentially about:

a *Form of obligation*: what form of regulatory mechanism is used to impose fair handling obligations on the recipient – law, binding scheme or contract?

b *Content of principles:* which privacy or data protection rights are included in the fair handling principles that the recipient is required to uphold?

c *Enforceability:* are the fair handling principles binding on the recipient and capable of being effectively upheld; that is, are they enforceable?

Is the recipient subject to a law, binding scheme or contract?

9.25 In principle, this element of IPP 9.1(e) may be satisfied where, for example, the recipient is:

a bound by a privacy or data protection law that applies in the recipient's jurisdiction;

b required to comply with some other law that imposes data collection and handling obligations in respect of personal information – for example, some criminal law and taxation statutes include provisions that expressly authorise and prohibit specified uses and disclosures, permit retention of some data and require destruction after a set time or under specified circumstances, and preserve a right of access to the person's own information;

c subject to an industry scheme or privacy code that is enforceable once entered into, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme or code;

d party to a contract that successfully incorporates section 17 of the *Information Privacy Act*; or

e party to a contract that effectively incorporates the *Model Terms*[318] issued by the Privacy Commissioner – discussed further below.

9.26 Recipients may not, however, be regarded as "subject to" a law, binding scheme or contract where, for example:

a the privacy or data protection law or regulations (or other law or regulations) exempt the recipient from having to comply with some or all of the fair handling principles;

b there is an existing or proposed authority (such as a public interest determination or direction issued by a privacy commissioner or minister) allowing the recipient to breach any or all of the fair handling principles;

c the data being transferred is not protected under the recipient's privacy or data protection law, for example, due to a difference in definition or coverage;

d the recipient is able to opt out of the binding scheme without notice and without returning or otherwise appropriately disposing of the data which had been transferred; or

e the agreement is unenforceable – such is often the case with a Memorandum of Understanding or shared protocols.

9.27 Where privacy law coverage is patchy or non-existent in the recipient's jurisdiction, and there is no relevant industry scheme or code in place, organisations may seek to comply with IPP 9 by using a contract adapted from the OVPC, *Model Terms for Transborder Data Flows of Personal Information*:

> The Model clauses may be adopted (with or without adaptation) in an organisation's contract with a recipient of personal information being transferred by the organisation outside Victoria.... This Guide and the Model Clauses are not prescriptive. They are a tool to assist an organisation in complying with Victoria's IPP 9. Each organisation will need to make a judgment as to whether or not the Model Clauses are appropriate for use in the particular context in which the organisation is operating. It will depend on the nature of the personal information being transferred outside Victoria, the rights and obligations of the parties to the relevant agreement, the recipient, and the actual circumstances in which the relevant agreement will operate.[319]

9.28 The *Model Terms* Guidelines point out, if a binding contract appropriately reflects the Model Clauses, this would assist organisations in complying with IPP 9(1)(a) or (f) in that:

a the recipient is subject to a contract that effectively upholds principles for the fair handling of the information that are substantially similar to the IPPs – in accordance with IPP 9.1(a); or

b the adapted Model Clauses and the way the parties have followed them during their dealings are evidence of reasonable steps by the organisation to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the IPPs – in accordance with IPP 9.1(f).[320]

c The *Model Terms* establish a relatively high level of protection by including, for instance, matters not expressly dealt with by the IPPs but which may nevertheless arise in the context of compliance actions or complaint-handling. For example, the *Model Terms* include obligations for the recipient to notify the organisation of a security breach, and to not engage in data matching without the organisation's prior authority.[321] Clauses such as these protect an individual's privacy, promote clarity about what is (and is not) authorised by the contract, and assist the organisation in meeting its other obligations (eg, under IPPs 2 and 4). Organisations are, of course, able to modify and adapt the *Model Terms* to fit their circumstances. Organisations may choose not to adopt some of the more stringent protections prescribed in the *Model Terms* where they exceed the obligations expressly set out in the IPPs. Or, organisations may decide to adopt or adapt the *Model Terms*, and/or include additional measures, where the circumstances warrant the inclusion of stronger safeguards.

Does the relevant law, binding scheme or contract effectively uphold fair handling principles?

9.29 It is not enough that fair handling principles be in place. These principles must be capable of being "effectively upheld". This means that the principles should be enforceable. Mechanisms should be in place to promote compliance with the principles, to enable complaints about alleged breaches to be independently investigated, and to provide appropriate redress to complainants for harm suffered as a result of the recipient's failure to effectively uphold the principles.

9.30 For example, many privacy laws that exist in Australasia, Canada and Europe already provide for independent regulators and tribunals to promote compliance and investigate non-compliance. Mechanisms are included to enable complaints to be made and investigated, and avenues are available for seeking redress. Binding codes may have a code administrator who can receive complaints, and provision might be made to provide remedies for privacy breaches.

9.31 Contracts can be more problematic, however, as they are not usually able to be enforced by the individuals whose data is being transferred. Organisations relying on contracts should endeavour to incorporate mechanisms to allow these individuals to, for example, exercise their usual rights of access and correction, or to complain and seek redress for a breach of their privacy. Organisations seeking to use contracts as a way to comply with IPPs 9.1(a) or (f) should refer to the Privacy Commissioner's *Model Terms* guidelines. For example, the *Model Terms* provide that the recipient agree to the following:

a establish mechanisms enabling access and correction rights to be exercised (Model Term 6.2(d));

b complaints be independently investigated and appropriate redress to be provided for harm arising from a privacy breach (Model Term 6.3(c));

c compliance audits to able to be undertaken (Model Term 6.3(d)); and

d awareness measures to be taken to promote compliance within the recipient organisation (Model Term 6.3(e)).

Are the fair handling principles substantially similar to the IPPs?

9.32 IPP 9.1(a) does not require the recipient to be bound to uphold principles that are identical to the IPPs, nor must these principles be as stringent as the IPPs.[322] The fair handling principles applying to the recipient must be "substantially similar". The use of this term suggests that some allowance will be made for variations in the wording and perhaps scope of privacy principles in recognition that these may have been tailored to meet specific needs and conditions of other jurisdictions, industries or parties to a data transfer. This may result in stronger protections being in place, or lesser ones, and such principles may be regarded as substantially similar to the principles set out in the IPPs in the circumstances of a particular data transfer.

9.33 The approach for assessing substantial similarity is likely to involve the following steps:

a In considering whether the fair handling principles applying to the recipient are substantially similar to the IPPs, the principles should be compared side by side, and their similarities and differences noted.

b The importance of any similarities or differences should then be assessed, having regard to the essential features of the IPPs, the relevance of particular principles to the data transfer under consideration, and the objects of the *Information Privacy Act*.[323]

c Where it is necessary for the Privacy Commissioner to consider the issue,[324] the identification of an essential feature will depend partly on the judgment of the Privacy Commissioner and partly on the material placed before the Commissioner. Regard will be given to the right to privacy protected under the Victorian *Charter of Human Rights and Responsibilities Act 2006*,[325] and the Privacy Commissioner may consider relevant international law and decisions of domestic or overseas courts and tribunals.[326]

d Whether there is substantial similarity is a question of fact.

In general, personal information that has been transferred out of Victoria should only be used and disclosed for legitimate purposes. For example, a fair handling principle that allows a recipient to use or disclose personal information for direct marketing purposes without the individual's consent may not be regarded as substantially similar to the restrictions on Use and Disclosure specified in IPP 2. Interstate and overseas transfers of sensitive information (such as personal information relating to sexual preferences, racial or ethnic origin, and criminal records) should strictly comply with the restrictions in the IPP 2. Organisations are of course free to seek consent to transfers that serve purposes not specified in IPP 2.1, and this is an express ground for authorising transborder data flows under IPP 9.1(b) – discussed below. Specific exemptions may, of course, be relevant to particular data transfers.

IPP 9.1(b): Individual gives consent

9.34 IPP 9.1(b) allows organisations to transfer information interstate or overseas where they have an individual's consent. Consent should be informed, voluntary, specific, current and made with legal capacity. The concept of consent is discussed further in the Key Concepts section of these Guidelines (see paras KC:38-KC:71). Also refer to the discussion of Use and Disclosure by consent under the section dealing with IPP 2.1(b) – see paras 2:49-2:58.

9.35 In order for consent to be informed and specific, when seeking consent from an individual for a transborder data transfer, the destination of the data should be specified, including which country the data will be kept. This may be problematic for some data storage services in the cloud where data is fragmented across several jurisdictions.

9.36 Where data is to be transferred as part of a research project, refer to the use of consent and other mechanisms discussed in the section dealing with IPP 2.1(c), especially paras 2:59-2:64.

9.37 IPP 9.1(b) would allow an organisation to obtain consent from an individual to a transfer of their information to an interstate or overseas recipient who is not subject to substantially similar privacy protections. As this creates a potential reduction in privacy protection of the information after it is transferred, organisations should ensure that individuals are properly informed of any reasonably foreseeable privacy risks associated with the transfer prior to obtaining the individual's consent.

IPP 9.1(c): Necessary to perform a contract with the individual or for implementation of pre-contractual measures at the individual's request

9.38 IPP 9.1(c) allows organisations to transfer information outside of Victoria where the transfer is necessary for:

a the performance of a contract between the individual and the organisation; or

b for the implementation of pre-contractual measures taken in response to the individual's request.

9.39 The transfer must actually be necessary, or at least require a close connection between the data subject and the purpose of the contract. IPP 9.1(c) cannot be used for transfers of additional, non-essential information. Nor can IPP 9.1(c) be used to authorise transfers of information for a purpose unrelated to the performance of the contract or pre-contractual measures. Transfers of information carried out to implement pre-contractual measures must be initiated by the individual, not by the organisation or recipient.

9.40 The meaning of "necessary" is discussed elsewhere in these Guidelines – see especially paras KC:81-KC:87 (in Key Concepts), 1:21-1:31 (necessary to collect) and 2:153-2:158 (reasonably necessary use/disclosure for law enforcement).

9.41 In many cases, consent may be an alternative basis for the transfer. For instance, the organisation may expressly seek consent in the contract, or consent may in some circumstances be implied. See Case Study 9-1.

CASE STUDY 9-1: Consent for transborder data flow implied[327]

The complainant wished to transfer funds to a family member overseas. When undertaking the transfer, the Money Transfer Service, which was owned by an overseas parent company, found that the complainant's name matched a name on a list of 'persons of interest'. The Australian subsidiary of the Money Transfer Service advised the complainant that once their identity could be verified, the transfer would be completed. The complainant provided the additional personal information which the Australian subsidiary provided to the parent company by facsimile. It was established that the initial identity match was false and the money transfer was subsequently completed.

The complainant complained to the Australian Privacy Commissioner about, in part, the transborder transfer of the complainant's personal information. The Australia Privacy Commissioner's considered whether the disclosure of the complainant's personal information to the Money Transfer Service's parent company in a foreign country was consistent with National Privacy Principle 9 (which is similar to IPP 9 in the *Information Privacy Act*).

The Australian Privacy Commissioner found that the complainant had impliedly consented to the transfer of personal information. The complainant had been advised that their transaction had been halted until they could provide necessary documentation which would be disclosed to the Money Transfer Service. The Australian Privacy Commissioner therefore decided that the complainant's consent to the transfer could be implied from the complainant's actions, and for this reason, the transfer complied with NPP 9.

9.42 Note that when considering whether consent has been implied, the notice given to the individual under IPP 1 may also be relevant.

IPP 9.1(d): Necessary to perform a contract with a third party in the individual's interest

9.43 Under IPP 9.1(d), an organisation may transfer information outside of Victoria to conclude or perform a contract concluded with a third party in the interest of the individual who is the subject of the information being transferred.

9.44 IPP 9.1(d) contemplates transfers that are beneficial to the interests of the individual (that is, "in the interest of the individual"), not adverse or prejudicial to the individual's interests. The individual's interest in protecting their privacy is one among many other interests.

9.45 Again, necessity must be established. There should be a close and substantial link between the individual's interest and the purposes of the contract.

9.46 The transfer should not be carried out solely in the interest of the organisation or recipient. The individual's interest must be served and the test for necessity must be met.

IPP 9.1(e): For the individual's benefit where impracticable to obtain consent or consent likely to be given

9.47 IPP 9.1(e) allows for transborder data flows where it is for the benefit of the data subject and it is impracticable to obtain consent, and the organisation reasonably believes that the data subject would give consent.

9.48 The transfer must be for the particular individual's benefit. For example, IPP 9.1(e) is likely to permit the transfer of essential personal information to assist in identifying and assisting a seriously injured person who is involved in an overseas or interstate accident or other disaster.

9.49 While such transfers for the benefit of the individual might ordinarily occur by consent, IPP 9.1(e) allows the transfer to proceed without consent if it is impracticable to obtain that consent and, if sought, the individual would likely give consent. If the organisation is aware of the individual having previously expressed a wish not to have their information transferred in the circumstances, then IPP 9.1(e) will not authorise the transfer.

9.50 Refer to the discussion of "consent", "practicable" and "impracticable to seek consent" at paras KC:38-KC:71, KC:91-KC:93 and 2:71-2:74, respectively.

IPP 9.1(f): Reasonable steps taken to ensure data will not be handled inconsistently with the IPPs

9.51 IPP 9.1(f) authorises a transborder data flow if the organisation has taken reasonable steps to ensure that the information transferred will not be held, used or disclosed by the recipient inconsistently with the IPPs.

9.52 Generally speaking, the steps required to satisfy IPP 9.1(a) will amount, in practice, to what is required by IPP 9.1(f).

9.53 However, IPP 9.1(f) also allows transfers where the recipient is not bound by a law, binding scheme or contract that requires it to effectively uphold fair handing principles that are substantially similar to the IPPs. The primary focus of IPP 9.1(f) is on the reasonable steps taken by the organisation, rather than on the more formal and substantive privacy obligations binding the recipient.

9.54 IPP 9.1(f) might be satisfied where the organisation takes practical steps to, for example, limit the amount of information transferred, arrange for agreements to be entered into to clarify permissible and prohibited uses and disclosures, and secure the information from the time of transfer until its eventual return or destruction. Various methods might be used (often in conjunction) to satisfy IPP 9.1(f), including law, technology and administrative practices. Again, compliance with other IPPs (such as whether the recipient is able to ensure appropriate security for the transferred data) may also dictate whether or not a transborder data flow is permissible.

IPP 9 Notes

[308] The intended extra-territorial reach of the *Information Privacy Act* is illustrated in section 4(1) of the *Information Privacy Act*, which expressly states that an organisation is taken to hold information "irrespective of where the document is situated, whether in or outside Victoria."

[309] *Information Privacy Act* s 6(1).

[310] For information on the operation of mutual assistance laws, see the Fact Sheets, key legislation and other related documents available from the Commonwealth Attorney-General's Department's website at http://www.ag.gov.au/extraditionandma.

[311] Section 32 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) requires all statutory provisions [including those contained in the *Information Privacy Act*] to be interpreted in a way that is compatible with human rights, including the right to privacy, so far as it is possible to do so consistently with the statute's purpose.

[312] For example, the *USA PATRIOT Act* (2001) allows the United States government to access data held in a data centre in the US. There have been suggestions that this may extend to data centres in other non-US jurisdictions that are owned by US companies.

[313] *Information Privacy Act 2000* (Vic) s 17(2) provides: "A State contract may provide for the contracted service provider to be bound by the Information Privacy Principles and any applicable code of practice with respect to any act done, or practice engaged in, by the contracted service provider for the purposes of the State contract in the same way and to the same extent as the outsourcing organisation would have been bound by them in respect of that act or practice had it been directly done or engaged in by the outsourcing organisation."

[314] *Information Privacy Act 2000* (Vic) s 68.

[315] Available at http://www.privacy.vic.gov.au.

[316] Office of the Victorian Privacy Commissioner, *Model Terms for Transborder Data Flows of Personal Information*, Guidelines, June 2006.

[317] Health privacy laws have also been enacted in the ACT, New South Wales, Victoria and Queensland. The Queensland *Information Privacy Act 2009* applies to the health department, who must comply with the National Privacy Principles in that Act.

[318] Office of the Victorian Privacy Commissioner, *Model Terms for Transborder Data Flows of Personal Information*, Guidelines, June 2006.

[319] Office of the Victorian Privacy Commissioner, *Model Terms for Transborder Data Flows of Personal Information*, Guidelines, June 2006, page 1.

[320] Office of the Victorian Privacy Commissioner, *Model Terms for Transborder Data Flows of Personal Information*, Guidelines, June 2006, page 5.

[321] Note that the Privacy Commissioner has no power under the *Information Privacy Act* to issue binding guidelines. In contrast, legally binding guidelines can be issued by the Health Services Commissioner under the *Health Records Act 2001* (Vic) and the Federal Privacy Commissioner under the *Privacy Act 1988* (Cth). Organisations can nevertheless choose to bind service providers to comply with any particular relevant guidance issued by the Victorian Privacy Commissioner by, for instance, adapting the relevant model clause in the *Model Terms* guidelines as appropriate.

[322] In contrast, any Code of Practice developed and approved under Part 4 of the *Information Privacy Act* must prescribe standards that "are at least as stringent as the standards prescribed by the Information Privacy Principles" (sections 18(2) and 19(3)(b), *Information Privacy Act 2000* (Vic)).

[323] Section 60 of the *Information Privacy Act 2000* (Vic) requires the Privacy Commissioner to have regard to the objects of the *Information Privacy Act* in performing his or her functions and exercising his or her powers under the Act. The objects of the *Information Privacy Act* are set out in section 5 and are: (a) to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector; (b) to promote awareness of responsible personal information handling practices in the public sector; and (c) to promote the responsible and transparent handling of personal information in the public sector.

[324] For example, if a complaint is received or a compliance investigation is undertaken under Parts 5 and 6, respectively, of the *Information Privacy Act*.

[325] The Privacy Commissioner, like other Victorian public authorities, is obliged to give proper consideration to relevant human rights when making a decision (section 38, *Charter of Human Rights and Responsibilities Act 2006* (Vic)).

[326] Section 32 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) requires all statutory provisions [including those contained in the *Information Privacy Act*] to be interpreted in a way that is compatible with human rights, so far as it is possible to do so consistently with the statute's purpose.

[327] *E v Money Transfer Service* [2006] PrivCmrA 5.

IPP 10: Sensitive information

10.1 IPP 10 restricts the collection of personal information that falls within the definition of "sensitive information" at the start of the Schedule to the *Information Privacy Act.*

10.2 The handling of sensitive information is also subject to greater restrictions under IPP 2.1(a), which requires reasonably expected uses and disclosures to be *directly* related to the primary purpose for collecting the information. IPP 2.1(a) is discussed further at paras 2:29-2:48.

10.3 The *Information Privacy Act*, like privacy and data protection laws in many other jurisdictions, imposes additional restrictions on the collection and handling of sensitive information. The rationale for these restrictions is based on the notion that certain types of personal information carry inherent risks to individuals' privacy and other rights, therefore justifying special treatment.[328]

10.4 One of the most obvious risks associated with the collection and handling of sensitive information is that of discrimination on the basis of, for example, racial or ethnic origin, sexual preferences or practices, or political opinions. Unnecessary or unlawful collection or use of these types of sensitive information may therefore give rise to parallel rights under both privacy and anti-discrimination laws. The Privacy Commissioner may, however, decline to entertain a complaint that could be, has been, or is being adequately dealt with under another statute,[329] such as under federal or state anti-discrimination laws.

10.5 The collection of sensitive information should be considered carefully, as a breach involving sensitive information may be even more damaging to individuals than non-sensitive information and may lead to further encroachments on an individual's rights.

Meaning of sensitive information

10.6 The definition of "sensitive information" can be found in the Schedule to the *Information Privacy Act*:

"sensitive information" means information or an opinion about an individual's –

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record –

that is also personal information.

10.7 In many privacy and data protection laws, health information is usually regarded as another category of sensitive information. In Victoria, health information has been excluded from the definition of "personal information" but its collection and handling is nevertheless subject to additional restrictions contained in the *Health Records Act 2001* (Vic).

10.8 Information that is "sensitive information" under the *Information Privacy Act* is not further defined. For assistance in interpretation of terms, guidance can be found in anti-discrimination cases. The meaning of various categories of sensitive information should be broadly interpreted, consistent with the general approach towards applying beneficial legislation in favour of those whose rights are to be protected.

10.9 IPP 10, like other provisions of the *Information Privacy Act*, will be interpreted and applied in a manner that is compatible with the human rights that are protected under the Victorian *Charter of Human Rights and Responsibilities Act 2006*, so far as it is possible to do so consistently with the *Information Privacy Act*'s purpose.[330] Relevant international law and decisions of domestic or overseas courts and tribunals relevant to these human rights may be considered.[331]

10.10 Sensitive information must also be personal information. IPP 10, like the remainder of the *Information Privacy Act*, will not operate where the information an organisation collects or handles is not about a person whose identity is apparent or is reasonably ascertainable. See the discussion of "personal information" in the Key Concepts section of these Guidelines (at paras KC:4-KC:37).

Racial or ethnic origin

10.11 The term "ethnic origin" has been regarded by the courts as having a wider meaning than strictly "racial". The meaning was considered by the House of Lords in an early complaint of racial discrimination under UK legislation involving the refusal by a school headmaster to admit a Sikh boy unless he removed his turban and cut his hair.[332] The House of Lords found that Sikhs were an "ethnic group" for the purposes of the legislation, and that the meaning of "ethnic" should not be restricted to simply racial or biological characteristics. Lord Fraser adopted the approach originally set out in a New Zealand Court of Appeal decision[333] and stated:

> For a group to constitute an ethnic group...it must, in my opinion, regard itself, and be regarded by others, as a distinct community by virtue of certain characteristics. Some of these characteristics are essential others are not essential but one or more of them will commonly be found and will help to distinguish the group from the surrounding community. The conditions which appear to me to be essential are these: (1) a long shared history, of which the group is conscious as distinguishing it from other groups, and the memory of which it keeps alive (2) a cultural tradition of its own, including family and social customs and manners, often, but not necessarily associated with religious observance.[334]

10.12 Other characteristics identified by Lord Fraser as relevant included a common geographical origin or descent from a small number of ancestors, a common language, a common literature peculiar to the group, a common religion differing from neighbouring groups or the surrounding community.[335]

10.13 This approach was adopted by the Federal Court of Australia in *Jones v Scully* [2002] FCA 1080, a racial vilification case brought under the *Racial Discrimination Act 1975* (Cth) (RDA), where Justice Hely found that Jews were an "ethnic group". In coming to his decision, Justice Hely referred to the House of Lords and New Zealand Court of Appeals cases and noted these cases were expressly endorsed in the explanatory material accompanying relevant amendments made to the RDA by the *Racial Hatred Act 1994* (Cth). The explanatory memorandum to that amending legislation stated that "ethnic origin" is to be broadly interpreted and Australian courts should follow the approach adopted by the House of Lords and the New Zealand Court of Appeals cases discussed earlier.[336]

10.14 Citizenship has not been regarded as an element of "race".[337]

Membership of a political association

10.15 In *Complainants R, S, T, U and V v Local Council* [2005] VPrivCmr 4, the Privacy Commissioner considered the meaning of the third category of sensitive information and found that information about two of the complainants' membership of a local ratepayers association fell within the category "membership of a political association". In that case, the Privacy Commissioner noted that "political" is not defined in the *Information Privacy Act* but has been interpreted by the Victorian Supreme Court in anti-discrimination cases[338] as being a matter or activity which has a bearing on government.

10.16 Individuals involved in a group protesting a particular government project might be considered members of a political association if the protest has a bearing on government or government activity. Collecting information about protestors therefore could fall within the definition of sensitive information.[339]

Religious beliefs or affiliations

10.17 "Religious belief" may include the holding, or *not holding*, of a religious belief. In *Dixon v Anti-Discrimination Commissioner of Queensland* [2004] QSC 58, the plaintiff was employed for a number of years as a co-ordinator of family support services for a community organisation. Her employment was terminated after she refused to sign a new employment contract that required her to, among other things, be actively involved in the Baptist Church. The Queensland Supreme Court held that discrimination because of a person's lack of religious belief amounted to discrimination on the ground of religion under the relevant Queensland legislation. Justice Douglas suggested that, to say someone is not eligible because she is not a worshipper in the Baptist Church is equivalent to saying only Baptists need apply.

10.18 In Victoria, the *Equal Opportunity Act 2010* expressly defines "religious belief or activity" to mean holding or not holding a lawful religious belief or view; or engaging or not engaging in a lawful religious activity.[340]

Membership of a trade union

10.19 In *Seven Network (Operations) Limited v Media Entertainment and Arts Alliance (MEAA)* [2004] FCA 637, the Federal Court of Australia accepted that information collected from Seven Network employees during a telephone poll carried out by a call centre on behalf of a union (MEAA) included sensitive information. The call centre's polling script asked a number of questions, including whether the employee was a member of the union, whether he or she would be willing to take part in various forms of industrial action, and whether he or she wanted further contact with the union.

Criminal record

10.20 "Criminal record" should be broadly interpreted to mean "any information associating an identifiable individual with criminal behaviour, whether or not charged, convicted, or found guilty."[341]

10.21 Photographs taken by police of individuals while in custody have been regarded as forming part of an individual's criminal record: *Smith v Victoria Police (General)* [2005] VCAT 654.

10.22 The collection of criminal histories is increasingly common for job applicants via police checks. Given that consent is required to collect criminal record information, the need for a police check should either be a requirement of law, or inherent to the job (ie, the nature of the job is one which could not be undertaken without a police check). This requirement should be made clear at the outset. Accordingly, an applicant that applies for a job with the prerequisite of a police check could be said to have impliedly consented to the collection of that person's criminal history.

10.23 Care should also be taken when collecting criminal history in compliance with IPP 1; that is, information about an individual's criminal record should only be collected if it is relevant to that individual's employment. Similarly, a police check should only be undertaken at the point at which an organisation is prepared to make the potential employee a job offer, rather than collecting such information unnecessarily at an earlier stage in the recruitment process, even if the police check is a requirement of the job.

10.24 Additional guidance on the collection and handling of criminal record data can be found in OVPC's Information Sheet 03.09, *Handling Criminal Records in the Public Sector*, April 2009.

Limiting the collection of sensitive information

10.25 IPP 10 states that sensitive information must not be collected unless one of the grounds in IPPs 10.1(a)-(d) or IPP 10.2 apply. IPP 10 should be read in conjunction with IPP 1. That is, when an organisation is proposing to collect sensitive information, it can only do so where:

a under IPP 1, the collection is:

i. necessary to the organisation's functions or activities (IPP 1.1);

ii. by lawful and fair means, and in a manner that is not unreasonably intrusive (IPP 1.2);

iii. directly from the individual, where this is reasonable and practicable (IPP 1.4); and

iv. with proper notice about who is collecting the information and why, to whom the information is usually disclosed, any legal basis for requiring the information, any usual disclosures, the individual's right of access, and consequences for the individual if he or she does not provide any or all of the information (IPP 1.3); and

b under IPP 10, the collection is by consent; is required by law; or is necessary to establish, defend or exercise legal and equitable rights; or, where consent cannot be obtained, the collection is:

i. necessary to prevent or lessen a serious and imminent threat (IPP 10.1(c); or

ii. necessary for research or statistics relevant to government funded targeted welfare or educational services, and no other reasonably practicable alternative for collecting the information is available (IPP 10.2(a)(i), (b)); or

iii. involves information about racial or ethnic origin collected to provide government funded targeted welfare or educational services, and no other reasonably practicable alternative for collecting the information is available (IPP 10.2(a)(ii), (b)).

10.26 A breach of IPP 1 may taint a collection under IPP 10. See the cases discussed below, involving respectively a failure to give adequate notice when collecting trade union information by consent, and an unlawful collection when obtaining sensitive information for use in legal proceedings.

IPP 10.1(a): Individual gives consent

10.27 Organisations can collect sensitive information under IPP 10.1(a) where the individual gives his or her consent. Consent must be informed, current, specific and made with legal capacity. It must also be voluntarily given. If an individual has no real choice but to consent to the collection of sensitive information, then that consent may not be regarded as voluntary. For example, the validity of consent may be questionable where the individual is likely to suffer serious detriment for refusing to, or later revoking, consent (such as the collection of criminal record histories for job applicants). This would also apply where consent is "bundled", which would likely not be informed consent.[342] See the discussion elsewhere in these Guidelines of the meaning of consent in Key Concepts at paras KC:38-KC:71, and use and disclosure by consent under IPP 2.1(b) at paras 2:49-2:58.

10.28 In *Seven Network (Operations) Limited v Media Entertainment and Arts Alliance (MEAA)* [2004] FCA 637, the Federal Court of Australia accepted that employees consented to participate in a telephone poll conducted on behalf of a union (MEAA), despite the call centre failing to make full disclosure about its identity or giving notice of other matters under NPP 1.3 (which is equivalent to IPP 1.3). The Court took the view that, when the call centre represented itself as being from the union, this representation was in accordance with the reality of the situation as it was acting as the union's agent. The Court found that, although there was a failure to comply with the notice obligations at the time of collection, this did not affect the quality of consent in this case. The Court suggested that consent was voluntarily given: "The questions were clear enough. The individuals had a choice as to whether to answer. There is no breach of the [Sensitive Information Principle]."

10.29 The quality of consent, however, will be affected if an organisation fails to comply with the notice obligations under IPP 1. This is particularly the case where individuals may not have provided their information had they known the reason for the collection or the eventual uses that might be made of their information. Collecting sensitive information without telling individuals why it is being collected, to whom it is usually disclosed, and whether they have a choice whether to provide the information will very likely affect whether any purported consent was informed and voluntary. Moreover, if individuals are misled into believing they must compulsorily provide their information when they are not in fact required to do so, any resulting collection might also be regarded as unfair (as explained at paras 1:40-1:41 and 1:84-1:85). These issues are discussed further in the sections dealing with the giving of direct or indirect notice under IPP 1 (at paras 1:61-1:96).

10.30 Consent is expected to be one of the principal ways in which organisations collect sensitive information from identifiable individuals. For example, an individual who identifies themself as belonging to a particular racial or ethnic group so that he or she is able to access a targeted government service relating to that racial or ethnic group could be asked to consent so that the organisation could use that information for certain future purposes. Reliance on consent ensures individuals know who is collecting sensitive details about their racial or ethnic origin, criminal records, sexual preferences or practices, religious beliefs or affiliations, political views and the like. Where consent cannot be sought, or where consent cannot be validly given, then organisations should consider whether they are permitted to collect sensitive information under one of the other grounds set out in IPPs 10.1 or 10.2. Relevant exemptions may also apply, such as where the collection is required under law.

Use of sensitive information in research

10.31 Organisations wishing to collect sensitive information for use in research can only do so by consent from the person whose information is sought, unless that research is carried out in accordance with IPP 10.2 (that is, in relation to government funded targeted welfare and educational services) or is conducted under a legislative mandate consistent with IPP 10.1(b). As stated earlier in these guidelines (at para 2:62), consent is foundational in human research and is the preferred basis on which such research is conducted. Race, religion and other types of sensitive information carry inherent risks for individuals, whose views should be sought where possible and taken into account in any research using identifiable information.

10.32 Organisations are of course not prohibited from collecting sensitive information about persons who are not identifiable, as this will fall outside of the ambit of the *Information Privacy Act*. See for example, *WL v La Trobe University* [2005] VCAT 2592, discussed at paras KC:18-KC:20 and in Case Study KC-1, where VCAT considered information collected in the course of a longitudinal health and relationships study (which explored, for example, issues relating to reproductive and sexual health behaviours and attitudes) was not reasonably identifiable.

IPP 10.1(b): Required by law

10.33 IPP 10.1(b) recognises organisations can collect sensitive information where collection is required under law.

10.34 Unlike IPP 2.1(f) which allows information to be used or disclosed where "required or authorised by or under law", IPP 10.1(b) limits the authority for collection of sensitive information to when it is "required under law" – not when such collection is simply "authorised". The requirement to collect sensitive information must be mandatory, and not simply permissive or discretionary.

10.35 See paras 2:121-2:133 for further guidance on the meaning of, and distinction between, "authorised" and "required" by law.

10.36 In the absence of a legislative mandate, organisations seeking to collect sensitive information should obtain the individual's consent or look to one of the other grounds specified under IPPs 10.1 or 10.2.

IPP 10.1(c): Necessary to lessen or prevent serious and imminent threats to the life or health of any individual

10.37 IPP 10.1(c) allows sensitive information to be collected where this is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where consent cannot be obtained from the individual whom the information is about because that person is either physically or legally incapable of consenting, or that person cannot physically communicate his or her consent.

10.38 This ground is similar to the authority for use and disclosure under IPP 2.1(d). However, unlike IPP 2.1(d), the threat under IPP 10.1(c) must be to an individual, not just in respect of the public at large. And, like IPP 2.1(d)(i), the threat to the individual must be both serious and imminent.

10.39 Relevant terms have been discussed in the section dealing with IPP 2.1(d). See paras 2:94-2:97 for guidance on the meaning of "imminent"; and paras 2:98-2:113 for when the collection might be regarded as "necessary" to lessen or prevent the threat.

IPP 10.1(d): Necessary for legal or equitable claims

10.40 Organisations may collect sensitive information where the collection is necessary for the establishment, exercise or defence of a legal or equitable claim. See the earlier discussion of the meaning of "necessary" at paras KC:81-KC:87 and 1:21-1:31.

10.41 IPP 10.1(d) may be relevant to situations where, for example, an organisation is defending itself against a claim of unlawful discrimination or unfair dismissal.

10.42 Establishment, exercise or defence of legal or equitable claims would encompass situations where it is necessary to collect sensitive information for the purpose of obtaining legal advice in connection with an existing or potential legal proceeding in a court or tribunal. There should either be a legal proceeding on foot or a real possibility that the organisation will need to exercise or defend its legal or equitable rights at a future date. In other words, sensitive information should not be collected "just in case" there is a future legal claim or defence.

10.43 As noted earlier, IPP 10 should be read in conjunction with IPP 1. IPP 10.1(d) will not permit collection of sensitive information for use in legal proceedings where that information is unlawfully obtained. See Case Study 10-1.

CASE STUDY 10-1: Unlawful collection of sensitive information for use in criminal trial[343]

The Director of Public Prosecutions (DPP) requested police to obtain any information relevant to the character of a doctor they were prosecuting for culpable driving. A police officer obtained a subpoena from a local court, signed by a justice of the peace and another police officer. She then presented this subpoena to the NSW Medical Board, the doctor's employer and a regional health service and obtained sensitive and other information about the doctor.

It was admitted that the process for obtaining the information was invalid, giving rise to an unlawful collection. The process should have been in the form of a District Court subpoena, issued and sealed by the court, with the documents presented directly to that Court. Police acknowledged that the collection was not a trifling or trivial matter, had conducted a substantial internal investigation into the incident, and were taking steps to ensure officers were aware of the lawful use of subpoenas to avoid the problem from recurring.

However, the Court found that the police were not required to answer for the contravention of the privacy legislation since they were carrying out a "law enforcement function" [which, unlike the *Information Privacy Act*, provides police with an unconditional and complete exemption from having to comply with the NSW privacy principles].[344]

IPP 10.2: Research or statistics about, or delivery of, government services

10.44 Sensitive information may be collected without consent, without a legislative mandate, outside of serious threats to individuals, and apart from the conduct of legal proceedings where the collection meets the following conditions:

(a) the collection -

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services;

or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.

10.45 Note that the use of the term "and" means that all of the subsections must be fulfilled for IPP 10.2 to apply.

"Government funded targeted welfare or educational services"

10.46 The authority in IPP 10.2 is limited to particular types of services ("welfare or educational services") that are "funded" by government and which are "targeted".

10.47 "Welfare or educational services" are likely to include the provision of schooling and educational support services, and programs aimed at promoting physical and social well-being – especially for those in financial or social need. For example, welfare services might include the provision of health, counselling and support services, as well as assistance programs in obtaining employment and housing.

10.48 The funded service must be "targeted". This may mean that the service is aimed at a particular person or group of persons, such as referral and support services for victims of crime. The term may also mean that the service is being carried out with a particular objective or result in mind, such as reducing homelessness or unemployment across Victoria.

10.49 "Government funded" services can include services that are funded by any combination of local, state and/or federal governments. This can occur through government grants or through more direct funding arrangements, such as under a service agreement or contract. It is not necessary under IPP 10.2 for the government to have any control over the service provider or the delivery of the funded services.[345] Nor does IPP 10.2 require the funded services to be related to the particular functions of the funding organisation,[346] although the services must be of an educational or welfare kind.

IPP 10.2(a)(i): Sensitive information necessary for research or statistics about government services

10.50 IPP 10.2(a)(i) equips Victorian government agencies (and, where relevant, their contracted service providers) with information necessary to carry out research or compile and analyse statistics about the services the government funds. This has the obvious benefit of enabling government to assess whether public monies are being effectively spent.

10.51 The collection of identifiable sensitive information must be "necessary" for the research or statistics to be carried out. This term is discussed elsewhere in these Guidelines – see especially paras KC:81-KC:87 and 1:21-1:31.

10.52 As discussed elsewhere in these Guidelines, researchers and statisticians may be able to use de-identified or anonymous data. (See the discussion of de-identified data and use of information for research and statistics at paras KC:24-KC:28 and 2:61.)

IPP 10.2(a)(ii): Information about racial or ethnic origin to deliver government services

10.53 IPP 10.2(a)(ii) authorises the collection of information about an individual's racial or ethnic origin where this is collected for the purpose of providing a government funded targeted welfare or educational service. It does not, however, authorise the collection of other types of sensitive information for the purpose of service delivery.

10.54 The non-consensual collection of information about racial and ethnic origin should only occur in very limited circumstances, such as where it is actually necessary for the effective delivery of government welfare programs.[347]

IPP 10.2(b): No reasonably practicable alternative to proposed collection

10.55 IPP 10.2(b) emphasises the need to keep non-consensual collection of sensitive information to a minimum by directing organisations to consider all practicable alternatives. For example, organisations might consider whether the research, statistics or service delivery can be conducted by using information that is not "sensitive information" or, where it is necessary to collect sensitive information, doing so by consent. Organisations should routinely consider whether they can (consistent with their obligations under IPPs 1.1 and 8) use information that is anonymous or otherwise not reasonably identifiable.

IPP 10.2(c): Impracticable to seek consent

10.56 See the discussion of the meaning of "practicable" in the Key Concepts section (paras KC:91-KC:93) and the guidance on the impracticability of seeking consent in the research context (paras 2:71-2:74).

10.57 As stated earlier, impracticability should not be confused with undesirability. That is, IPP 10.2(c) does not permit consent to be waived where consent can readily be sought but the organisation would prefer not to do so (for instance, because a high rate of participation is desired and the organisation fears individuals would refuse their consent, if asked).

IPP 10 Notes

[328] Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108)*, explanatory note to Article 6 (Special categories of data), para 43, available at http://conventions.coe.int.

[329] Section 29(1)(f) and (b), *Information Privacy Act*.

[330] The Privacy Commissioner, like other Victorian public authorities, is obliged to give proper consideration to a relevant human right when making a decision (s 38, *Charter of Human Rights and Responsibilities Act 2006* (Vic)).

[331] Section 32 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) requires all statutory provisions, including those contained in the *Information Privacy Act*, to be interpreted in a way that is compatible with human rights, so far as it is possible to do so consistently with the statute's purpose.

[332] *Mandla v Dowell Lee* [1983] 2 AC 548.

[333] *King-Ansell v Police* (1979) 2 NZLR 531.

[334] *Mandla v Dowell Lee* [1983] 2 AC 548, per Lord Fraser at 562.

[335] *Mandla v Dowell Lee* [1983] 2 AC 548, per Lord Fraser at 562.

[336] *Jones v Scully* [2002] FCA 1080 at paras 110-113.

[337] *Re Carl* [2003] NSWSC 756, a case involving a complaint about a decision refusing the plaintiff entry to a selective high school because he was not an Australian or New Zealand citizen or a permanent resident of Australia.

[338] *Nestle Australia Ltd v The President and Members of the Equal Opportunity Board* [1990] VR 805 per Vincent J at 819; and *CPS Management Pty Ltd v Equal Opportunity Board* [1991] 2 VR 107 per Marks J at 111.

[339] See Office of the Victorian Privacy Commissioner Report 01.11, *Protestors and the right to privacy,* Review of the collection and handling of protestors' personal information by the Department of Sustainability and Environment, AquaSure Pty Ltd and Melbourne Water Corporation pursuant to the *Information Privacy Act 2000*, September 2011.

[340] *Equal Opportunity Act 2010* (Vic) s 4.

[341] Office of the Victorian Privacy Commissioner, *Controlled Disclosure of Criminal Record Data*, Report to the Attorney-General pursuant to section 63(3) of the *Information Privacy Act 2000,* June 2006, page 2.

[342] See *KJ v Wentworth Area Health Service* [2004] NSWADT 84; *JK v Department of Transport Infrastructure Development* [2009] NSWADT 307.

[343] *HW v Commissioner of Police, New South Wales and Anor* [2003] NSWADT 214.

[344] The Court noted (at para 30), however, that certain other acts and practices are likely to fall outside of "law enforcement functions" and be characterised as part of police's "administrative function".

[345] This is in contrast to the application of the *Freedom of Information Act 1982* (Vic), which extends to prescribed authorities defined in section 5 of that Act to include "an incorporated company or association or unincorporated body **which is supported directly or indirectly by government funds or other assistance or over which the State is in a position to exercise control"** (emphasis added).

[346] IPP 10.2 does not require a "State contract" to be on foot, where an outsourcing organisation engages the service provider to provide a service "in connection with the performance of functions of the outsourcing state or local government organisation". Where the service is carried out under a "State contract", then organisations would be expected to consider binding the service provider to the *Information Privacy Act 2000* (Vic) through the use of a clause under section 17(2) of the *Information Privacy Act 2000* (Vic). For further guidance on outsourcing, see the Office of the Victorian Privacy Commissioner, *Outsourcing and Privacy Guidelines*, Edition 1, May 2011.

[347] See the clause note to IPP 10 in the Explanatory Memorandum to the *Information Privacy Act*. Also see Second Reading Speech to the *Information Privacy Bill 2000* (Vic), Victoria, Victoria, Legislative Assembly, *Parliamentary Debates*, 26 May 2000, page 1907 (John Brumby, Minister for State and Regional Development).

Appendix 1: The Information Privacy Principles

THE INFORMATION PRIVACY PRINCIPLES[348]

In these Principles –

"sensitive information" means information or an opinion about an individual's –

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record –

that is also personal information;

"unique identifier" means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name.

Principle 1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of –

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

Principle 2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless –

(a) both of the following apply –

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual –

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information; or

(d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent –

(i) a serious and imminent threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health, public safety, or public welfare; or

(e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(f) the use or disclosure is required or authorised by or under law; or

(g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(h) the Australian Security Intelligence Organization (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested the organisation to disclose the personal information and –

(i) the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and

(ii) an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(g), it must make a written note of the use or disclosure.

Principle 3 Data quality

3.1 An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

Principle 4 Data security

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.

Principle 5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

Principle 6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that –

(a) providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) providing access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice –

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders –

by or on behalf of a law enforcement agency; or

(j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (j) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, the organisation –

(a) must advise an individual who requests access to personal information that the organisation will provide access on the payment of the prescribed fee; and

(b) may refuse access to the personal information until the fee is paid.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

6.8 If an individual requests access to, or the correction of, personal information held by an organisation, the organisation must –

(a) provide access, or reasons for the denial of access; or

(b) correct the personal information, or provide reasons for the refusal to correct the personal information; or

(c) provide reasons for the delay in responding to the request for access to or for the correction of personal information--

as soon as practicable, but no later than 45 days after receiving the request.

Principle 7 Unique identifiers

7.1 An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.

7.2 An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless –

(a) it is necessary to enable the organisation to carry out any of its functions efficiently; or

(b) it has obtained the consent of the individual to the use of the unique identifier; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless –

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or

(b) one or more of paragraphs 2.1(d) to 2.1(g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4 An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

Principle 8 Anonymity

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

Principle 9 Transborder data flows

9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if –

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply –

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

Principle 10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless –

(a) the individual has consented; or

(b) the collection is required under law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns –

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if –

(a) the collection –

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.

[348] Schedule 1 of the *Information Privacy Act 2000* (Vic).

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

W

Table of Cases

Commonwealth

New South Wales

Victoria

Hong Kong

New Zealand

United Kindom

Notes

Notes

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 organisation's 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 individual's 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

The Information Privacy Principles are simply...

the right information,
to the right people,
for the right reason,
in the right way,
at the right time.

privacy victoria

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