

Spatial Information Privacy Guidelines

Part of Victoria's Spatial Information Management Framework
Second Edition

The Victorian Spatial Council was established under the Victorian Spatial Information Strategy 2004-2007 to support the advancement of Victoria's social, economic and environmental goals through the provision and application of spatial information. It does this by providing a coordinated approach to spatial information policy, development and management, and facilitating opportunities for greater partnership building, collaboration, cooperation and education.



Victorian Spatial Council
C/- Spatial Information Infrastructure
Department of Sustainability and Environment
570 Bourke Street, Melbourne 3000
PO Box 500, East Melbourne 3002

Tel: 8636 2529, 8636 2307
Fax: 8636 2813

Victorian.SpatialCouncil@dse.vic.gov.au
<http://www.victorianspatialcouncil.org/>

September 2009

CONTENTS

VSC CHAIRMAN’S FOREWORD.....	4
INTRODUCTION.....	5
THE SPATIAL INFORMATION MANAGEMENT FRAMEWORK	5
THIS DOCUMENT	7
PART A – OVERVIEW	8
BACKGROUND.....	8
HOW TO READ THIS DOCUMENT.....	9
PRIVACY POLICY.....	9
PART B – THE INFORMATION PRIVACY PRINCIPLES (VICTORIA)	10
<i>Principle 1—Collection</i>	10
<i>Principle 2—Use and Disclosure</i>	10
<i>Principle 3—Data Quality</i>	11
<i>Principle 4—Data Security</i>	11
<i>Principle 5—Openness</i>	12
<i>Principle 6—Access and Correction</i>	12
<i>Principle 7—Unique Identifiers</i>	13
<i>Principle 8—Anonymity</i>	14
<i>Principle 9—Transborder Data Flows</i>	14
<i>Principle 10—Sensitive Information</i>	14
PART C – GUIDELINES.....	16
PART D – INFORMATION PRIVACY PRINCIPLES EXPLANATORY NOTES	20
FURTHER REFERENCE MATERIAL.....	24
APPENDIX 1 – DEFINITIONS.....	25
APPENDIX 2 – SAMPLE NEWSPAPER COLUMN ADVERTISEMENT.....	27
APPENDIX 3 – SAMPLE PRIVACY STATEMENT.....	28
GLOSSARY	30

VSC CHAIRMAN'S FOREWORD

The Victorian Spatial Information Management Framework consolidates the policies, principles and guidelines for information management that were articulated by both the Victorian Geospatial Information Strategy 2000-03 and the Victorian Spatial Information Strategy 2004-07.

The Framework aims to support the effective use of spatial information to support Victoria's social, environmental and economic goals through the establishment of institutional arrangements for developing spatial information; creating and maintaining spatial information; making spatial information accessible and available; and strategic development of technology and applications.

The custodian of spatial information is at the heart of the Spatial Information Management Framework. Its policies set out the minimum requirements for custodians to manage their datasets, while a set of underlying principles provide the foundation for enabling them to maintain these datasets and ensure all Victorians are aware of and have ready access to them.

These principles address all elements of the Spatial Data Infrastructure of Victoria: *governance, custodianship, framework information, business information, quality, metadata, awareness, access, pricing and licensing, and privacy.*

The Framework is accompanied by ten Guideline documents to assist custodians in the implementation of these policies and principles. These *Privacy Guidelines* provide an introduction to Victoria's approach to privacy: how it is defined, how should be managed, and how custodians may make their spatial information accessible while complying with the Victorian Information Privacy Act 2000.

The Guideline documents are also intended to be accessible to the general reader by setting out fully the basis on which the Framework will be delivered.

The Victorian Spatial Council is Victoria's principal coordinating body for spatial information, with a mandate to develop policy and promote best practice for spatial information management. These *Privacy Guidelines* are a key contributor to the Spatial Information Management Framework's objective to make spatial information accessible and useable. It is intended that they will be informed by practical experience, and contributions to future editions are welcome from practitioners and readers alike.



Olaf Hedberg

Chair, Victorian Spatial Council

INTRODUCTION

The Spatial Information Management Framework

The Spatial Information Management Framework is Victoria's best practice approach for establishing and retaining consistency in the management of spatial information across all organisations – whether public or private – with a role or interest in doing so.

Its objective is that spatial information be made as accessible as possible.

The Victorian Spatial Council has endorsed the development of the Framework because a coordinated approach to information management will provides the greatest opportunity to:

- reduce duplication of datasets, systems and processes, and increase consolidation, leading to more efficient spending on spatial information
- optimise investment and develop partnerships across the spatial information community (public, private and academic sectors)
- deliver higher quality datasets
- improve access to spatial information

Management of spatial information by participants in the Framework should facilitate its effective use, based on four key principles: that the spatial information will:

- represent the definitive and authoritative source of the data it contains
- be managed by designated custodians
- be accessible and available to all members of the community, except where confidentiality and commercially sensitive conditions apply
- be able to be combined with other spatial information products for the purposes of analysis and decision making

The Spatial Information Management Framework provides a holistic approach to managing spatial information in Victoria, encompassing the

1. **institutional arrangements for developing spatial information;**
2. requirements for **creating and maintaining spatial information;**
3. mechanisms for **making spatial information accessible** and available; and
4. **strategic development of technology and applications.**

Together, these components of the Framework create Victoria's Spatial Data Infrastructure (SDI).

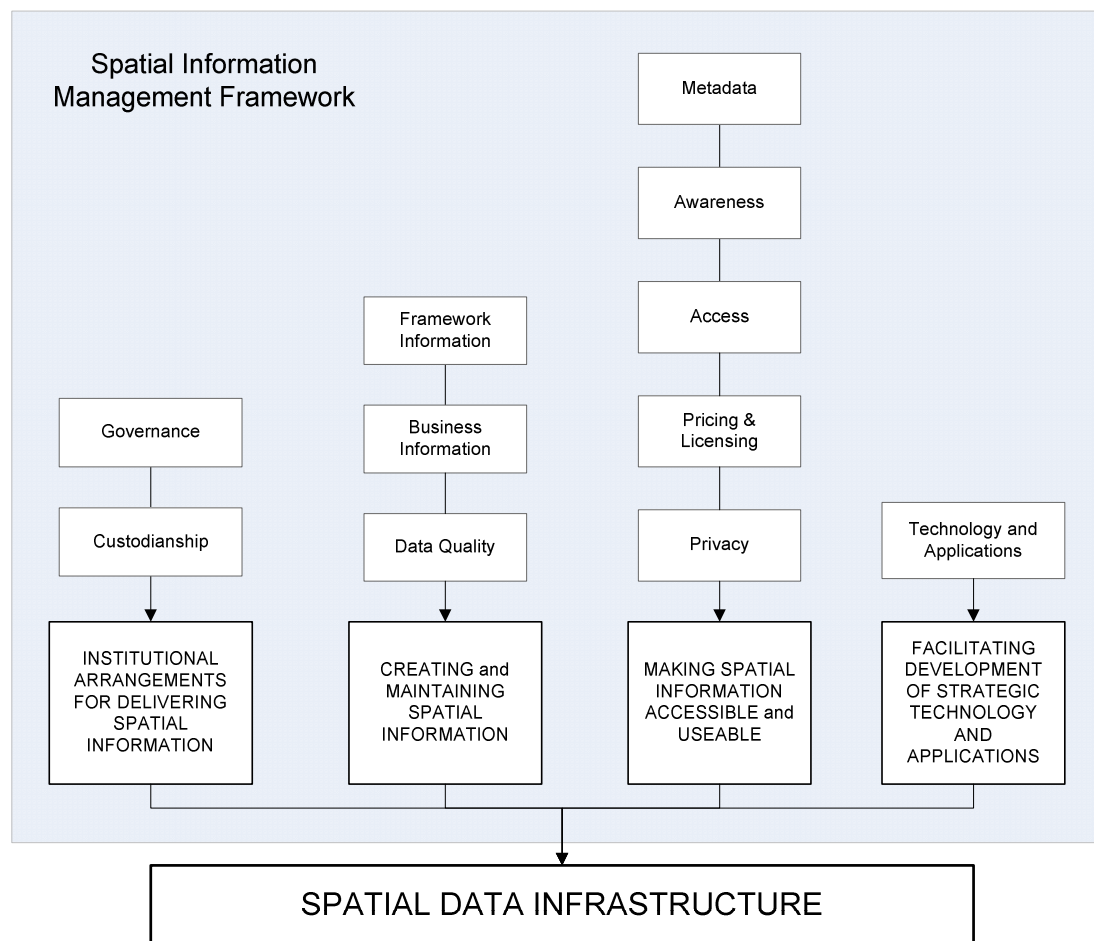
The SDI is an enabler – a mechanism for making data available and for sharing and exchanging it to enhance the achievement of social, environmental and economic goals. Behind it are the myriad of activities that create the conditions in which that sharing and exchange can take place, ie the development of the data, technology, policies, institutional arrangements and capacity building (ie equipping people to use the technology and information).

The Framework allows for the management of these elements in an integrated way to provide an environment for the effective use of spatial information.

This integrated approach is illustrated in Figure 1.

The Framework is supported by policies and guidelines that provide the formal requirements for implementing it, and tools and resources to support those responsible for that task.

Figure 1: The Victorian Spatial Information Management Framework



Separate Guidelines have been prepared for the following components of the Framework:

- Governance
- Custodianship
- Framework Information
- Business Information
- Data Quality
- Metadata
- Awareness
- Access
- Pricing and Licensing
- Privacy

The purpose of the Guidelines is to explain the policies and principles outlined in the relevant component of the Framework, and to describe activities that will support their application in implementing it.

It is envisioned that these Guidelines will vary over the life of the Framework as new information, policies, and procedures are developed, and as new issues arise.

This Document

It is intended that the Guidelines be read in conjunction with the document '*Victoria's Spatial Information Management Framework and Directory of resources*', also produced by the Victorian Spatial Council.

These Privacy Guidelines have four sections.

- Part A is an overview of the spatial information management principles discussed in the Guideline as they relate to privacy.
- Part B sets out the Victorian Information Privacy Principles (IPPs).
- Part C outlines how the IPPs can be applied to spatial information.
- Part D provides explanatory notes to support the IPPs.

PART A – OVERVIEW

Background

These *Spatial Information Privacy Guidelines* address issues related to spatial information as a result of the *Information Privacy Act 2000*, which came into operation in September 2002. Many elements of spatial information are considered ‘personal information’ where the information makes it reasonably possible to identify an individual.

The Guidelines outline the processes for determining access to spatial information for ‘public good’ purposes, de-personalisation of spatial information through the removal of personal information or data aggregation, and where access to the information should be limited.

They are based on the ANZLIC Best Practice Privacy Guidelines (2004), with additional input from the Office of the Victorian Privacy Commissioner.

The Victorian Information Privacy Act 2000

The Victorian *Information Privacy Act 2000* came into effect from 1 September 2001. The *Act* sets the standards for the management and protection of personal information by the Victorian public sector.

The *Information Privacy Act* began as a data protection bill for the public and private sectors. It was developed in Multimedia Victoria and promoted initially by the then Treasurer in his capacity as Minister for Information Technology and Multimedia. The impetus was the wish to encourage economic and government activity online by protecting individuals’ information privacy under state law.

When the *Commonwealth Privacy Act* was amended to cover part of the private sector (effective 21 December 2001), Victoria’s scheme was cut back to cover state government agencies and local councils. The *Privacy Act 1988* covers the Commonwealth and ACT governments and some parts of the private sector, as well as all health care providers. Private sector organisations with an annual turnover of more than \$3 million and/or who trade in personal information are covered by this Act. Private sector organisations not covered by the *Act* can choose to ‘opt-in’ and be bound by the *Act*.

When the Information Privacy Bill passed the Victorian Parliament in October 2000, responsibility passed to the Attorney-General.

The Victorian *Information Privacy Act* sets standards for the way Victorian government organisations, statutory bodies and local councils collect and handle personal information. Ten Information Privacy Principles (IPPs) are the practical core of the *Information Privacy Act*. With limited exceptions, all Victorian government organisations, including local councils, must comply with these principles or have an approved code of practice. Non-government organisations that work for government under contract may also be covered, depending on the contract.

ANZLIC Best Practice Guidelines

In February 2004, ANZLIC-the Spatial Information Council released the *ANZLIC Best Practice Privacy Guidelines* and the *Spatial Information Privacy Issues Discussion Paper*. These documents provide guidance to public sector agencies about the privacy issues and principles related to spatial information.

Much of the personal information held by the public sector can have a spatial component; however, not all spatial information held by the public sector will contain personal information. For example, mapping, survey and geodetic data are unlikely to hold any information about an identifiable person. However, if they are linked to or combined with personal information, such as when a person activates a GPS location device registered in their name, it becomes ‘personal information.’

While the *Spatial Information Privacy Issues Discussion Paper* specifically focuses on spatial information it is important to note that spatial information is no different to any other type of information and can be managed

under information management principles. However, spatial information, due to its nature, can be readily linked to personal information through processes as simple as, for example, a link between a name and residential address.

The key objectives of the ANZLIC paper are underpinned by four main principles derived from the difficult judgements faced by the public sector:

- The public sector has a responsibility to use the data available to it in the most efficient and effective way possible to achieve its goals;
- In looking at information requirements, the public sector should adopt the least intrusive approach – i.e. where the public sector can achieve improvements in services or efficiency without requiring more data and affecting personal privacy, it should do so, recognising that the protection of privacy is in itself a public service;
- Wherever possible – and where the benefits of better use of personal data are for the person using the service – citizens should have greater choice in the use of their personal information to deliver public services; and
- Ensuring that where data are used or shared without the consent of the individual (for example, in law enforcement), there is openness, transparency and consultation in the policy-making process with the aim of striking a balance between individual rights and the wider public interest.

How to read this document

Unlike the other Spatial Information Guidelines that support the Spatial Information Management Framework, the *Spatial Information Privacy Guidelines*, are based on legislation. Compliance with privacy legislation is a requirement of all organisations that manage, store, and distribute, personal information, or information that could be used to determine personal information. The objective of these Privacy Guidelines is to assist data managers and custodians in determining if their data is affected by this legislation, and to provide direction to complying with this legislation.

They can be read in conjunction with the ANZLIC Best Practice Privacy Guideline which gives further examples of application of Privacy legislation.

While the Privacy Guidelines are aimed at the public sector, they can also be of assistance to the private sector.

Privacy Policy

The Spatial Information Management Framework is based on the application of consistent information management principles across a distributed network of autonomous data custodians operating throughout the whole spatial information community.

Many elements of spatial information may be considered ‘personal information’ where the information makes it reasonably possible to identify an individual. Therefore, custodians need to ensure that they consider the need for de-personalising their information before the collect it and make it available.

This requirement is expressed in the policy that has been set out in the Spatial Information Management Framework:

Custodians will recognise privacy requirements in the management of their spatial information.

PART B – THE INFORMATION PRIVACY PRINCIPLES (VICTORIA)

Extract from SCHEDULE 1 of the Information Privacy Act 2000 (Version 0.21)

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.

PART C – GUIDELINES

Protecting privacy is as much about being open as it is about keeping personal information secure. It is about handling information in accordance with the person's expectations. Privacy laws and policies all require organisations to inform the person about what information is collected about them, why and what will happen to it. In this way, shared expectations can develop.

For government agencies, this means ensuring that their information management practices are transparent. They must be able to produce documented privacy policies, demonstrate that they are being implemented, and tell anyone who asks whether any personal information is held about them.

This information will assist data managers and custodians in determining if their data is subject to privacy legislation, and the best way to comply.

The following information draws heavily from the Office of the Victorian Privacy Commissioner paper *Submission to ANZLIC, the Spatial Information Council, on its draft Privacy Best Practice Guideline*, December 2003, the ANZLIC publications *Spatial Information Privacy Issue Discussion Paper* and *ANZLIC Spatial Information Privacy Best Practice Guideline*, February 2004, and information from the Office of the Federal Privacy Commissioner website.

Spatial Information that could be Personal Information

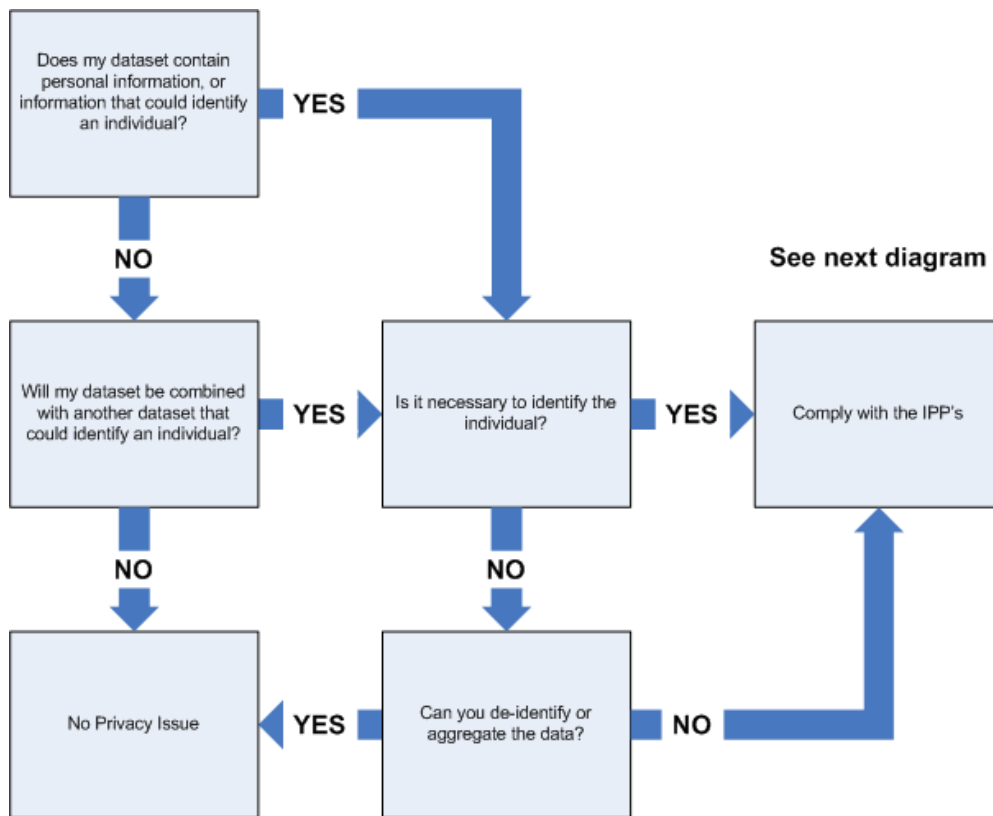
Spatial information, in some contexts, can be personal information as defined under privacy legislation. Any information that describes the location of an individual is personal information. The most obvious is address; another is geographic coordinates. Other examples might be

- a person's name linked with their address,
- the linking of a mobile phone owner's name, mobile phone number, and the geographical 'cell' within which the phone is being used,
- if there is only one individual living at a property in an isolated area, referring to the relevant street address could make it possible to identify an individual

Aerial photography and satellite imagery can also be personal information as it provides imagery of an individual's 'personal space' – their backyard. Contrary to popular belief, and depiction on TV and in movies, satellite imagery cannot be used to identify an individual. However, aerial photography and high resolution imagery (usually very expensive and only acquired over a small area) can identify a house footprint, the number of trees in the yard, if there is a swimming pool, or a car parked in the driveway.

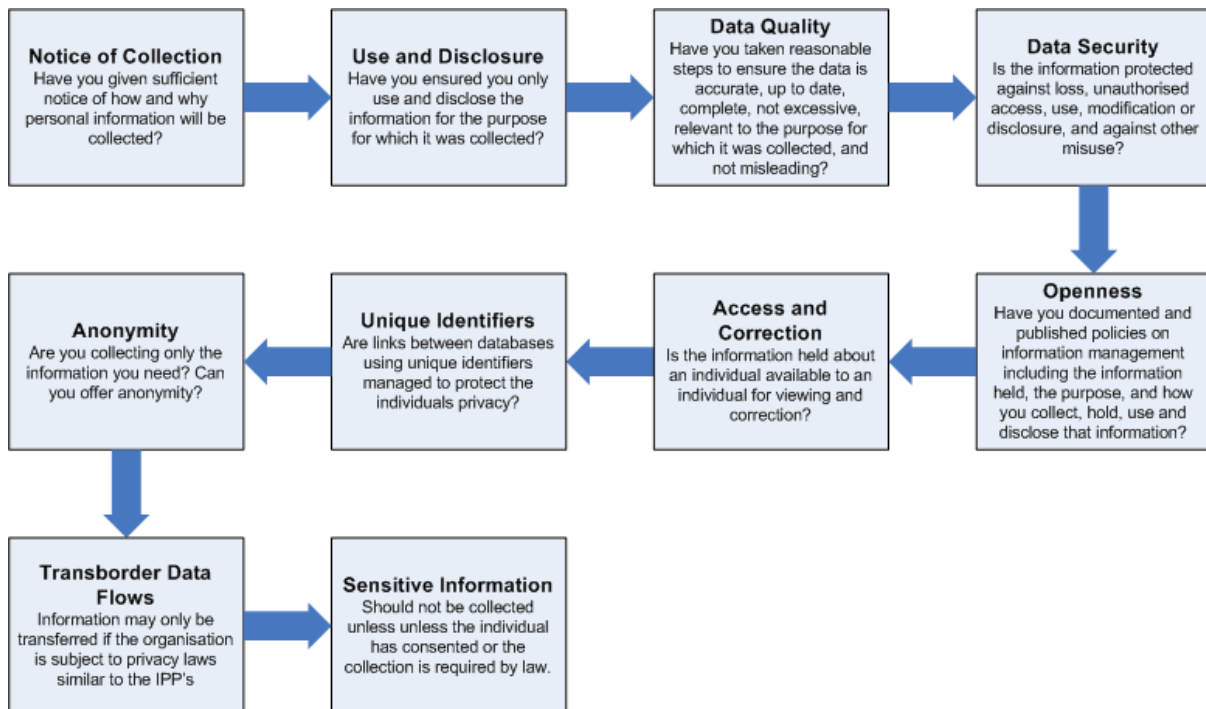
If layers of spatial information can be combined with each other, a unique identifier, or other information, and can lead to the determination of the identity of an individual, then that spatial information is subject to privacy legislation.

Is my data subject to Privacy Legislation?



Addressing Privacy Concerns

Compliance with the IPP's



De-identification and Aggregation of Personal Information

Properly de-identifying and aggregating data is an effective means of removing the necessity to comply with the *Information Privacy Act*. De-identification of data requires the removal of all identifiers from data such that an individual's identity cannot be reasonably ascertained. Aggregation of data includes incorporating data into a larger group of data. The key concern of de-identification and aggregation of data is to ensure that the data cannot be re-identified or de-aggregated at a later date such as to identify an individual.

De-identification

Permanently de-identifying information means removing from the record any information by which an individual may be identified. Simply removing the name and address may not be sufficient to de-identify the information. Permanent de-identification also means that an organisation is not able to match the de-identified information with other records to re-establish the identity of individuals.

Tips for compliance

The test for whether information is identifiable is whether the identity of the individual is apparent, or may reasonably be ascertained, from the information using the definition of 'personal information' in section 6 of the Privacy Act.

A de-identification procedure would not be complete if, from the resulting information, the identity of an individual could be reasonably ascertained. Reasonable steps to de-identify information may include:

- considering the capacity of the organisation to re-identify the information;
 - careful consideration of the identifying nature of every aspect of the information; and
 - setting up safeguards that ensure that future collection or uses will not re-identify the information.
- An organisation may need to include in contractual arrangements with a receiving organisation that the receiving organisation will not re-identify the information.

Australian Government, Office of the Privacy Commissioner Information Sheet 6 - 2001 Security and Personal Information, source <http://www.privacy.gov.au/materials/types/infosheets/view/6565>

Data aggregation

Aggregated data describes data combined from various sources to form another larger piece of data. A well known example of aggregated data is the Census data prepared by the Australian Bureau of Statistics (ABS). Privacy and confidentiality of data collected during a Census is of the utmost importance to the ABS. It is imperative that the Australian population has confidence in the privacy of the personal data they provide. Each household is allocated to a Census Collection District (CD) incorporating a minimum of 100 individuals, with an average of 220 households. All data from within this CD is aggregated. This is the smallest unit of information available. CD's can then be aggregated into larger statistical units covering larger areas. The forms used to collect the information are then pulped so there is no possibility of identifying an individual.

Other forms of aggregation could be assigning information to a locality or Local Government Area or an address range. The options for aggregation are almost unlimited. The key issue is that the aggregated data cannot be de-aggregated, and cannot be used to reasonably ascertain the identity of an individual.

Privacy Impact Assessment

The following information is taken from *Privacy Impact Assessments – a guide*, Edition 2, April 2009, Office of the Victorian Privacy Commissioner.

A Privacy Impact Assessment (PIA) is ‘an assessment of any actual or potential effects that the activity of proposal may have on individual privacy and the ways in which any adverse effects may be mitigated’ (p.4)

A PIA can give confidence to those taking action—and those who will be affected by it—that the impact on privacy has been considered, and any risks arising have been appropriately addressed. (p.4)

A Privacy Impact Assessment is often described as an “early warning system” for your organisation. It allows you to detect potential privacy problems, take precautions and build tailored safeguards before, not after, you make heavy investments in time and perhaps in technologies. PIAs help identify inherent privacy risks that may be costly to address later in the project. The PIA affirms that privacy issues have been addressed and that reasonable steps have been taken to provide an adequate level of privacy protection at the time of assessment. The PIA also provides a mechanism for reviewing the privacy impact of projects as changes occur. (p.7)

A proper PIA can give the general public confidence that their privacy has been adequately considered and addressed. Demonstrating that your organisation has identified and managed privacy issues in a particular project builds and sustains trust with the public and other agencies. If you demonstrate that you take privacy seriously, you are demonstrating respect for people. People who are confident that they and their privacy are respected are more likely to provide the information and co-operation that will make your projects successful. The PIA should be seen as a source of information and action to allay fears about loss of privacy or about protection of personal information.

It can also assist in anticipating public reaction to the privacy implications of a given proposal. (p.9)

The point of a PIA is to influence decision-making on a project. The timing of the PIA must therefore be early enough so that the findings and recommendations can influence the final design of, and thinking about, the project. Ideally, a PIA should be initiated at the early stages of project development and planning. (p.10)

The nature and size of the proposal, project or system may determine whether an internal individual or team conducts the PIA, with or without external specialist advice. By-products of doing a PIA internally are the way it grows and reinforces the organisation’s knowledge base about privacy and data protection, and (depending on the seniority of the leader) the way it signals to the organisation’s staff the significance that senior management attaches to getting privacy right.

Where the PIA is undertaken by staff rather than a specialist external consultant, you may wish to consider incorporating external opinion on the result before finalising the PIA. Outsiders often ask useful questions that insiders have not considered because of their familiarity or assumptions. Some external involvement may be useful in building public confidence in the PIA later.

External consultants with particular skills may also be brought in to assist only with certain aspects. In either case it will still be important for the organisation to have overall responsibility for the PIA. (p.11)

Source: Privacy Impact Assessments: A Guide for the Victorian Public Sector, Edition 2 – April 2009, <http://www.privacy.vic.gov.au/privacy/web.nsf/content/guidelines>

PART D – INFORMATION PRIVACY PRINCIPLES

EXPLANATORY NOTES

1. Collection of data

The collection principle is mainly concerned with the manner of collection and the giving of notice, rather than with consent. Consent is not a requirement of the collection principle. Organisations do not have to seek consent or authorisation from individuals for the collection of personal spatial information. In many situations where the law requires an organisation to collect personal information, the individual has no choice. To say consent is needed to collect personal information will only breed confusion. Individuals may mistakenly believe that by withholding their consent they will be able to veto an organisation's ability to collect their information. In many administrative practices, organisations need to collect personal information.

The collection principle is important to transparency. It involves notice: giving an individual sufficient detail about how and why personal information will be collected.

A sample of a notification of collection of data is provided in Appendix 2.

2. Use and Disclosure

In general, organisations must only use or disclose personal information for the purpose for which it was collected or, otherwise, with the consent of the subject. However, they are entitled to use or disclose personal information for a secondary purpose where it is related to the primary purpose of collection and the use or disclosure is within the reasonable expectations of the individual. This would be the case, for example, where the information was used to manage, evaluate or improve particular government services in relation to which the information was originally collected.

Secondary uses/disclosures are otherwise permitted in cases where there is a strong public interest in doing so. These include, for example, where there is a serious threat to life, where disclosure is required by law or for research in the public interest.

Privacy principles also put a premium on notice and on openness. At a minimum, technologies that systematically observe and record (as do, for instance, satellites used in spatial information gathering and GPS) should be publicised. People should be put on notice of the purposes of the observation and the uses of the data gathered. Transparency is critical. A sample of a statement of use of data is provided in Appendix 3.

Assisting law enforcement agencies to carry out their law enforcement functions is entirely appropriate. But it is not necessarily appropriate for large datasets to be provided in bulk to law enforcement agencies, or for those agencies to be given remote access to the whole of the dataset for any purpose. Such assistance may be given with greater precision and less risk if given on a case-by-case- basis.

3. Data Quality

The focus of the Spatial Information Management Framework is to ensure that consistent standards for data quality are adopted and that the data is 'fit for purpose'. Good quality data is essential to the effective use of spatial information.

When collecting personal spatial information, and also before using it, reasonable steps should be taken to ensure that it is:

- Accurate
- Up to date
- Complete

- Not excessive
- Relevant to the purpose for which it is collected or used
- Not misleading

In some cases, keeping information up to date has long been a statutory requirement. Such laws continue to take precedence over this policy. For further information refer to the *Spatial Information Data Quality Guidelines*.

4. Data Security

Personal spatial information is to be protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse.

Many Victorian government organisations and local councils are entering into contracts with outside suppliers to provide services that may include a spatial information component or that may lead to access by the service provider or others to personal information useful to providing services. Drivers for such arrangements include better emergency services and natural resource management.

Contracts with service providers that handle personal information on behalf of government agencies should prohibit any use, retention or disclosure of the information except as required in delivering the service. Transaction logs or other records of access to personal information should be retained and audited.

Victorian contracted service providers will be bound by the *Information Privacy Act* if the outsourcing agency has included an enforceable provision in the contract making them subject to the IPP's or to an applicable code of practice. Without such a term, the outsourcing Victorian government organisation will be responsible for the privacy breaches of their service providers.

Private sector organisations need to be aware that if they undertake government contracts they might have to operate within State and Federal privacy frameworks designed for the public and private sectors. The frameworks contain similar principles, but where they differ may be significant in certain contexts.

5. Openness

Organisations are encouraged to be transparent by clearly documenting their policies on management of personal information, and to make those policies available to the public. Organisations must take reasonable steps to let people know, on request, what sort of personal information they hold, for what purpose and how they collect, hold, use and disclose that information.

Most public sector organisations in Victoria will already have various policies concerning the management of personal information as part of complying with the introduction of the *Information Privacy Act*. Organisations should ensure that what is reflected in policies is put into practice.

Part of managing personal spatial information will also involve being ready to deal with complaints to the organisation about any mismanagement of personal spatial information. Organisations should make known to individuals its internal complaints handling structure for resolving individuals' concerns about the management of personal information. Making known to the individual the name and contact details of an employee with responsibility to handle complaints is important given the technical nature of spatial information.

6. Access and Correction

Personal spatial information held on public registers about a person is to be available for their inspection, as authorised or required by law.

Personal spatial information not held on public registers should be accessible informally through administrative processes. If necessary, however, personal information can be accessed through freedom of information (FOI)

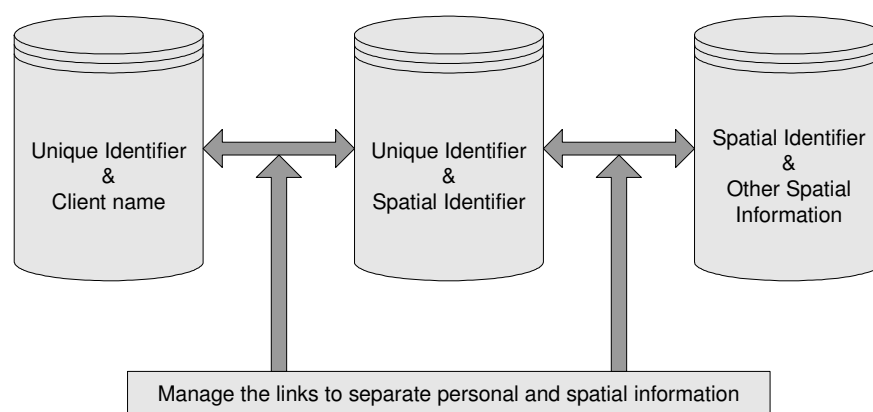
and/or privacy legislation. Whilst FOI requests are the enforceable way to seek access to information, if organisations take a practical and constructive approach to requests for access the need for a formal FOI request may be avoided. This saves time and expense, and builds confidence.

There are exceptions to the right of access to personal information about an individual, and these are listed in IPP 6.

7. Unique Identifiers

Under Victorian IPP 7 a unique identifier is 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. An example of a unique identifier in the spatial information industry may be the council's ratepayer number which it assigns to each ratepayer.

Unique identifiers may be both privacy enhancing and privacy invasive. There is value in unique identifiers being adopted by organisations instead of using individual's names because, in many sensitive or delicate contexts, numbers may be better for privacy than names. However, limits need to be placed on the use and disclosures of identifiers, once they have been assigned, so that they do not facilitate other interferences with privacy. Data linking, matching and profiling are much easier if unique identifiers are shared across different, separate stores of personal information. These activities are potentially privacy invasive. While that does not mean they should never occur (for example they may serve clear public interests), they should be the subject of express authorisation, transparency, purpose limitation and independent oversight.



The approach favoured in the *ANZLIC Privacy Best Practice Guideline* is to isolate the data elements that alone, or in combination with other data elements, fall within the definition of 'personal information,' and then manage them in a way that minimises the risk to privacy while allowing lawful access.

A key method for managing the data elements is to have each data element as a field or table in a database. Through managing the design of the database the linkages between personal and spatial information can be managed such that the personal information can be removed from the spatial information allowing for greater usage of the spatial information with no risk to privacy.

8. Anonymity

As part of the collection of information, organisations are encouraged to offer an individual the option of anonymity, if possible. Properly anonymous and properly de-identified information is unlikely to be 'personal information' within the meaning of privacy laws. Beginning with anonymity makes sense because in privacy

law, the more personal information you needlessly collect, the more organisations must needlessly spend resources on complying with other aspects of privacy law.

9. Transborder Data Flows

An organisation is only allowed to transfer personal information outside Victoria if it reasonably believes the recipient is subject to a law, or other binding obligation, which imposes restrictions on the use of that information which are substantially similar to the Information Privacy Principles. This includes transfers outside Australia or New Zealand, between jurisdictions, or between a jurisdiction and a private sector organisation.

Personal information may also be transferred with the individual's consent or if the transfer is necessary for the performance of a contract. If consent of the individual cannot practically be obtained, the organisation can only transfer the information if it is for the benefit of the individual and if the individual would be likely to consent.

10. Sensitive Information

Sensitive information is defined as information about an individual's racial or ethnic origin, political opinions, membership of a political, professional or trade association, philosophical or religious beliefs or affiliations, membership of a trade union, sexual preferences or practices, or criminal record.

It will be extremely rare that personal spatial information will be combined with sensitive information. However, custodians and data managers need to be aware of the legislation regarding sensitive information.

Publicly available information and public registers

In terms of Victorian privacy legislation, publicly available information is exempted from the Act and the IPPs.

This is not the case for public registers, which carry a qualified exemption. Victorian government organisations need to comply with the IPP's as far as reasonably practicable. Practicable means capable of being done or feasible. When practicability is at issue, cost is one consideration but it is not the only one.

Public registers hold varying amounts of personal information. As a group, they may bear many details of how an individual carries on their daily life from registering their pet, or extending their house, to joining a licensed profession. In Victoria alone hundreds of public registers are open to public inspection, although not necessarily published. Local councils maintain a range of public registers, as do various statutory authorities and state government departments.

The Land Titles register is a public register containing personal spatial information – specifically the name and address of the owner of a parcel of land. While the Land Titles register can be searched by anyone, searching is limited to single searches (no data mining) and a fee is charged per search. Other public registers containing personal spatial information, in most cases name and address of the occupant or owner, can also enhance privacy through limiting searches to single searches, charging a fee, or making personal information only available to authorised personnel, or not available at all.

The wide availability of personal information on public registers, either in paper or, now more commonly, in electronic format, can raise risks for the individuals whose personal information is registered. The option for an individual to seek suppression of their details when they have concerns about personal safety should be offered and requests must be seriously considered. It is the equivalent of the "silent number". Where spatial information is concerned, mistakes can have grave consequences.

FURTHER REFERENCE MATERIAL

Australian Government Office of the Privacy Commissioner website, www.privacy.gov.au

Office of the Victorian Privacy Commissioner website, www.privacy.vic.gov.au

- *Schedule 1 of The Information Privacy Act 2000 – The Information Privacy Principles*
- *Information Privacy Bill Explanatory Memorandum*
- December 2002, *Submission to the Review Panel on ‘A Regulatory and Administrative Framework for Survey and Spatial Information in Victoria’*
- April 2003, *Submission to Land Victoria on the draft ‘Victorian Spatial Information Strategy 2003-2006’*
- December 2003, *Submission to ANZLIC – the Spatial Information Council on its draft ‘Privacy Best Practice Guideline’*
- August 2004, *Public Registers and Privacy – Guidance for the Victorian Public Sector*
- April 2009, *Privacy Impact Statements. A Guide for the Victorian Public Sector, Edition 2*
- September 2006, *Guidelines to the Information Privacy Principles*
- December 2006, *Short Guide to the Information Privacy Principles*

ANZLIC – the Spatial Information Council website, www.anzlic.org.au

- February 2004, *Spatial Information Privacy Issue Discussion Paper*
- February 2004, *ANZLIC Spatial Information Privacy Best Practice Guideline*

Spatial Information Guidelines:

Spatial Information Access Guidelines

Spatial Information Awareness Guidelines

Spatial Information Business Information Guidelines

Spatial Information Custodianship Guidelines

Spatial Information Data Quality Guidelines

Spatial Information Framework Information Guidelines

Spatial Information Governance Guidelines

Spatial Information Metadata Guidelines

Spatial Information Pricing and Licensing Guidelines

All documents are available at <http://www.victorianspatialcouncil.org/>

APPENDIX 1 – DEFINITIONS

Spatial information - information that describes the location of objects in the real world and the relationship between objects that is not deemed to be personal spatial information.

Personal spatial information - information combined with, linked to or contained within any spatial object or location. Examples include: a persons name linked with their address, or the linking of a mobile phone owner's name, mobile phone number, and the geographical 'cell' within which the phone is being used.

Spatial information, in some contexts, will also be personal information as defined under privacy legislation. For example, situations will arise where property address information collected in a spatial information context might also be personal information. If there is only one individual living at a property in an isolated area, then by merely referring to a street address it could be possible to identify an individual.

The majority of the spatial information created, held and maintained by government agencies is not personal information. For example, mapping, survey and geodetic data is unlikely to hold any information that identifies a particular individual.

However this spatial information can be easily linked to personal information, including health and sensitive information. The personal spatial information is a combination of personal information and spatial information.

Source: ANZLIC Best Practice Guideline "Spatial Information—Privacy Issues" Discussion paper

Consent - express consent or implied consent.

Generally available publication - a publication (whether in paper or electronic form) that is generally available to members of the public and includes information held on a public register.

Law enforcement agency:

- (a) the police force of Victoria or of any other State or of the Northern Territory; or
- (b) the Australian Federal Police; or
- (c) the Australian Crime Commission; or
- (d) the Commissioner appointed under section 8A of the Corrections Act 1986; or
- (e) the Business Licensing Authority established under Part 2 of the Business Licensing Authority Act 1998; or
- (f) a commission established by a law of Victoria or the Commonwealth or of any other State or a Territory with the function of investigating matters relating to criminal activity generally or of a specified class or classes; or
- (fa) the Chief Examiner and Examiners appointed under Part 3 of the Major Crime (Investigative Powers) Act 2004;
- (fb) the Special Investigations Monitor appointed under Part 2 of the Major Crime (Special Investigations Monitor) Act 2004;
- (g) an agency responsible for the performance of functions or activities directed to—
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction for a breach; or
 - (ii) the management of property seized or restrained under laws relating to the confiscation of the proceeds of crime or the enforcement of such laws, or of orders made under such laws; or
- (h) an agency responsible for the execution or implementation of an order or decision made by a court or tribunal, including an agency that—

- (i) executes warrants; or
 - (ii) provides correctional services, including a contractor within the meaning of the Corrections Act 1986, or a sub-contractor of that contractor, but only in relation to a function or duty or the exercise of a power conferred on it by or under that Act; or
 - (iii) makes decisions relating to the release of persons from custody; or
- (i) an agency responsible for the protection of the public revenue under a law administered by it.

Personal information - information or an opinion (including information or opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Public register - a document held by a public sector agency or a Council and open to inspection by members of the public (whether or not on payment of a fee) containing information that —

- (a) a person or body was required or permitted to give to that public sector agency or Council by force of a provision made by or under an Act; and
- (b) would be personal information if the document were not a generally available publication.

sensitive information - 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 - 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.

Source: *Information Privacy Act 2000 – Section 3 “Definitions”*

APPENDIX 2 – SAMPLE NEWSPAPER COLUMN ADVERTISEMENT

Notification of Aerial Photography Capture

At we value and protect the personal information collected in the course of undertaking our work responsibilities and aim to demonstrate and achieve a strong culture of protecting the confidentiality and privacy of clients and members of the community.

The Coordinated Imagery Program (CIP) is now commencing its fourth year in operation. It is a program to coordinate the acquisition of aerial satellite imagery across the State of Victoria. The Program is managed by Spatial Information Infrastructure (SII) in the Department of Sustainability and Environment (DSE). The Program will streamline the acquisition, storage and access of aerial and satellite imagery.

This imagery will be used by Victorian Government agencies, statutory bodies, utilities and local government to enhance their GIS applications for growth tracking, asset management, data maintenance and to derive value-added products such as elevation models.

We were appointed to capture imagery over at ..cm pixel resolution between 2006 and 2007. At the end of the Program the imagery will be held by SII for distribution to program stakeholders. The product will not be of sufficient detail to identify individuals. SII assures us that it is committed to ensuring the use, distribution and licensing conditions of the imagery complies with the *Victorian Information Privacy Act 2000*.

Enquiries concerning any of the flying aspects of this project should be made to

Email:

APPENDIX 3 – SAMPLE PRIVACY STATEMENT

Land Channel Privacy and Security Statement

The Land Channel is committed to protecting your personal information consistently with principles set out in the Victorian *Information Privacy Act 2000*.

If you have any queries about our privacy policy please contact us at land.channel@dse.vic.gov.au or telephone (61 3) 8636 2333

The Land Channel delivers content and services on behalf of a number of government departments and agencies. This includes services and transactions delivered and maintained external to the Land Channel infrastructure by the individual government departments or agencies responsible for their provision.

While the privacy principles outlined above apply to all service applications delivered on this site, you are advised to refer to any specific privacy and security provisions associated with each individual application.

Collection of Personal and other information

The Land Channel collects only personal information that you voluntarily provide. Land Channel may request you to provide certain personal information that is necessary for that function or activity of Land Channel. For example, if you are making a purchase you will ordinarily be asked for your name, contact information and credit card details. If you do not provide that personal information the transaction can not be processed.

Land Channel also collects anonymous information through its Web server and via an external service [Nielsen/NetRatings](#) (see [Statistical Collection Methods](#)). The information is collected for statistical purposes only to assist us to improve our service. At no time can we personally identify you as the source of the data.

Security

The Land Channel and its e-commerce provider will take all reasonable actions necessary to protect your personal and credit card details with respect to confidentiality and security of data. Credit Card details are encrypted for your protection using Secure Socket Layer (SSL) technology. Both credit card and personal details are stored within a secure password protected environment. Your credit card number is not retained by Land Channel after the transaction. All data provided will only be used for the purpose authorised by or reasonably contemplated by an individual to whom it relates. These details will not be disclosed to a third party except as required by law.

As some of the Land Channel pages are displayed inside 'web frames', you will not see the closed padlock symbol when using Netscape or the key symbol when using Microsoft Internet Explorer. This is because the independent navigation 'web frames' surrounding the pages do not utilise SSL. This in no way affects the level of security offered by SSL on the credit card information you submit.

Your right to access and correct personal records

Account holders have the opportunity to update and amend information held by us. This information is only accessible through a user-created "User Name" and "Password". If you believe we hold personal information about you, you can ask for a copy of your personal data by sending an email to land.channel@dse.vic.gov.au or by writing to us at PO Box 500, East Melbourne, 3002. You can ask us to correct, update or amend the information we hold about you. Before we send you any personal data, you will need to provide evidence of your identity. If you do not provide evidence of your identity, the Land Channel reserves the right to refuse access to the personal information held.

Statistical Collection Methods

Clickstream Data

Clickstream data refers to visitor logs and statistics that provide useful information about users' online experience without identifying individuals. Typical clickstream data collected includes:

- visitor's computer address (i.e. Internet Protocol, or IP, address) and relevant domains;
- times and dates of site visits;
- pages accessed (including most visited and least visited) and files downloaded;
- browsers and operating systems used by visitors.

Land Channel uses clickstream data purely for statistical purposes (such as the most popular searches and the times of the day that Land Channel is used most/least) without identifying individual users.

Cookies

The Land Channel website uses 'cookies' (small data files) that are sent to your web browser. Cookies may give the server information about a computer's identity and website visiting patterns and preferences but do not collect personal information.

Most features of the site can be used without accepting cookies. Some interactive features and all account and purchasing services utilise cookies to establish a unique link between your browser and our service to enable delivery of the service. Once you have finished your visit the cookie is removed from your browser. No personal information is collected or maintained through the use of the cookie.

Web Beacons

A web beacon is a technology that records web page usage statistics. Land Channel uses web beacons to collect clickstream data, but does not use beacons to identify individual users.

GLOSSARY

Custodian	The entity responsible for a data set. That is, the organisation formally responsible for ensuring accuracy, currency, storage, security, and distribution of the data. The custodian need not be directly involved in maintaining or supplying the data, but should be in a position to direct such activities.
Data	The base level of information stored in electronic or other databases. Data can exist in many formats including digital data, imagery such as aerial photographs and satellite images, and hardcopy products such as maps or plans.
Dataset	Identifiable collection of data.
Global Positioning System (GPS)	A satellite-based timing and positioning service designed, implemented and maintained by the United States Department of Defence.
Information	The result of manipulating, analysing and interpreting data to produce a result which adds value or utility to the original data
Information Privacy Act (Victoria)	The standards for the way Victorian Government organisations, statutory bodies and local councils collect and handle your personal information. With limited exceptions, all Victorian Government organisations, including local councils, must comply with these principles or have an approved code of practice. Non-government organisations that work for Government under contract may also be covered, depending on the contract.
Land Channel	The Victorian Government web site providing integrated access to land, resource and property information and services for the State of Victoria.
Personal information	Recorded information or opinion, whether true or not, about an identifiable individual. Personal information can be almost any information linked to an individual, including name, address, sex, age, financial details, marital status, education, criminal record or employment history.
Privacy Principles	The Information Privacy Principles give Victorians privacy rights. The detailed Information Privacy Principles can be found at: http://www.privacy.vic.gov.au/
Spatial Data Infrastructure (SDI)	The technologies, policies and institutional arrangements that facilitate the availability of and access to spatial data.
Spatial Information Infrastructure	The spatial information essential to the social, economic, and environmental development of Victoria.
Spatial Information Management Framework	Victoria's best practice approach for establishing and retaining consistency in the management of spatial information. It provides a holistic approach to managing spatial information, encompassing the institutional arrangements for developing spatial information; requirements for creating and maintaining spatial information; mechanisms for making spatial information accessible and available; and strategic development of technology and applications.