ANZLIC Best Practice Guideline

SPATIAL INFORMATION—PRIVACY ISSUES

Discussion paper

Version 2.0 (Final)

13 February 2004

CONTENTS

ACKNOWLEDGMENTS iii

INTRODUCTION 1

Spatial information and privacy 1

Benefits of an ANZLIC Privacy Best Practice Guideline 3

APPLYING PRIVACY LAWS AND RULES TO SPATIAL INFORMATION 4

Privacy laws and rules in Australia and New Zealand 4

Shared features of privacy regimes 5

Protecting 'personal information' 5

Promoting openness as well as confidentiality 9

Supplementing other relevant legislation 9

Recognising other public interests 9

Based on Privacy Principles 10

ACKNOWLEDGMENTS

Content was developed as a result of a national workshop held on 25 November 2002 attended by the following jurisdictional representatives.

Jurisdiction	Name	Email Address	Role
Facilitator	Gaby Jaksa	Jaksa.gaby@saugov.sa.gov.au	DAIS
Consultant	Lindy Smith	Lindysmith@privacymanagement.com.au	Privacy Management
ACT	Robert Twin	robert.twin@act.gov.au	Geographic Information Management, Urban Services
ANZLIC	Steve Blake	steve.blake@anzlic.org.au	ANZLIC
ANZLIC	Paul Kelly	paul.kelly@anzlic.org.au	ANZLIC
Cwlth	Judy Huxley	Judy.Huxley@osdm.gov.au	Office of Spatial Data Management
NT	Tony Gill	tony.gill@nt.gov.au	Information Services, DIPE
NSW	Julie King	Julie.king@ditm.nsw.gov.au	DITM
NZ	Stephen Walsh	anzlic-desk@linz.govt.nz	LINZ
Qld	Bronwyn Huitfeldt	bronwyn.huitfeldt@nrm.qld.gov.au	Information Policy, DNRM
SA	Geoff Yeomans	Yeomans.Geoff@saugov.sa.gov.au	DEH
SA	John Behncke	Behncke.john@saugov.sa.gov.au	DAIS
Tas	John VanderNiet	john.vanderniet@dpiwe.tas.gov.au	Office of the Surveyor General, DPIWE
Vic	Bruce Thompson	Bruce.thompson@nre.vic.gov.au	Land Victoria, DNRE
Vic	Cathy Chipchase	Cathy.chipchase@nre.vic.gov.au	Land Victoria, DNRE
WA	Jim Rhoads	JimR@walis.wa.gov.au	WA Land Information System (WALIS)

ANZLIC wishes to acknowledge the coordinating and management role played by Land Victoria in preparation of this document. Special thanks go to Cathy Chipchase, Bruce Thompson and Lindy Smith.

Draft papers were circulated to all jurisdictions and made available through the ANZLIC website for most of 2003. Substantive comments were received from the Victorian Privacy Commissioner, which are gratefully acknowledged. Version 2 of the papers reflects all feedback received.

INTRODUCTION

Spatial information and privacy

Technological developments that have enabled government agencies to make public sector spatial information more widely available, cheaper to access, and of better quality; have also fuelled concerns about privacy.

These concerns are not directed at the handling of spatial information in particular — surveys of community attitudes show widespread anxiety about the general impact of technology on all areas of our lives.[1] ANZLIC recognised the trend in 1992, when it produced its first privacy issues discussion paper.[2] Now privacy laws and rules are established features of the environment within which the spatial information industry operates — not just nationally, but internationally as well.

There are two fundamental risks to privacy associated with improvements to the access and usability of public sector spatial information.

First, there is the risk that personal information collected in land dealings, property transactions, and land regulation and administration can be used for purposes that are unrelated to the purpose for which it was originally provided. Examples include:

- Using name and contact information for direct marketing;
- Searching for and locating individuals either for malicious purposes or out of simple curiosity;
- Compiling profiles or dossiers by combining the information with personal information from other sources in order to make decisions about the person's access to services, suitability for employment or eligibility for other opportunities.

This risk has always existed. Technological developments, and especially the provision of this information online, have increased it considerably.

Second, there is the risk that spatial information containing no personal information can be manipulated and combined with other information to reveal details about an identifiable individual. Examples include:

- Person location tracking using mobile communication media;

[1] See, for example, *Community Attitudes towards Privacy in Australia*, Office of the Federal Privacy Commissioner, July 2001. The report is available from the Commissioner's web site <http://www.privacy.gov.au>.

- Data matching using the person's address as a common identifier.

This risk was probably negligible until relatively recently, yet has grown steeply and probably represents the greater risk in future. Continuing improvements in the capacity to locate and track individuals in real time, combined with the considerable potential to apply this technology for public benefit and commercial gain, will keep the pressure on government agencies to manage public sector spatial information responsibly.

How effectively government agencies can address these risks is limited because a great deal of the information is accessible to the public. Although government agencies can influence how the information is used by setting the conditions under which it is made available, they cannot determine or predict the behaviour of the recipients.

The passage of privacy legislation covering the private sector should assist to the extent that it imposes community-wide obligations and provides avenues of redress for people who feel their privacy has not been respected. However, government agencies remain responsible for reducing the risks where they can for at least three important reasons.

- The personal information collected is frequently required by law to be provided and kept for many years. It is held in trust. The individual concerned has no further control of that information, so there is a responsibility to protect it from misuse.

- If the information is not protected from misuse, people may find or demand ways to avoid revealing their personal details to government agencies and this can affect the quality and usefulness of the data in future. For example, in response to concerns about misuse of personal information, requests to be taken off the publicly available version of the electoral roll are increasing,[3] as are the number of people wanting their details removed from public telephone directories.[4]

- Some jurisdictions are required to comply with privacy legislation that includes specific rules for the handling of personal information on public registers. In all jurisdictions with privacy laws, Privacy Commissioners are monitoring the activities of public sector agencies closely and are responsive to community criticism of apparently unfair practices. For example, both

[2] *Privacy, Confidentiality and Access to Land Information Systems*, Issues in Land Management Paper No. 5, ANZLIC, July 1992.

[3] Victorian Electoral Commissioner, evidence to the Scrutiny of Acts and Regulations Committee, Inquiry into a Privacy Code of Conduct for Victorian Members of Parliament, 30 August 2001.

[4] Roger Clarke, *Privacy and 'Public Registers'*, Xamax Consultancy Pty Ltd, 11 May 1997.

the Victorian Privacy Commissioner and the Federal Privacy Commissioner have issued discussion papers this year on public register information.[5]

Benefits of an ANZLIC Privacy Best Practice Guideline

In 1992, when ANZLIC issued its first paper on privacy issues, the only jurisdiction with privacy legislation in place was the Commonwealth Government. Since then, all jurisdictions have introduced laws or policies to protect the privacy of personal information, or plan to do so. Some have additional legislation protecting other forms of privacy, such as video surveillance laws.

These laws and policies provide frameworks and standards to apply to spatial information privacy issues. However, while there are strong similarities, the standards differ from one jurisdiction to the next. Also, some of the jurisdictions are required by their privacy legislation not to transfer personal information across borders unless the recipient will protect it to similar standards. The different standards create uncertainty that can hamper the free flow of data.

The uncertainty is compounded when personal information is passed to the private sector, as only a small proportion is covered by the privacy legislation in Australia (note: the private sector in New Zealand is fully covered by privacy legislation).

The *ANZLIC Privacy Best Practice Guideline* can:

- Provide a clear, common approach to privacy protection, which is likely to meet the requirements of the differing privacy rules operating within and across the jurisdictions.
- Help the flow of information between jurisdictions that have privacy laws and those that do not.
- Establish a common approach to the sharing of personal information with the private sector.
- Help to avoid or manage the privacy risks that all jurisdictions may encounter when considering new systems, products, proposals, technologies and requests for services and information.
- Articulate a nationally agreed understanding of how the definition of 'personal information' applies to spatial information.

[5] Office of the Federal Privacy Commissioner, *Privacy and Collection of Publicly Available Personal Information*, Consultation Paper for Information Sheet, June 2002; Office of the Victorian Privacy Commissioner, *Public Registers and Privacy: Building Permit Data*, Issue Paper 01.02, January 2002; Report 01.02, August 2002.

APPLYING PRIVACY LAWS AND RULES TO SPATIAL INFORMATION

Privacy laws and rules in Australia and New Zealand

All government agencies either comply with an information privacy law or policy, or intend to do so soon.

- New Zealand's Privacy Act applies to both the public and private sectors.[6]
- Commonwealth, ACT, Victorian and NSW public sector agencies are required to comply with privacy legislation, though based on different standards.[7] The ACT and Victoria also have separate privacy legislation for health information, and similar legislation is currently before the NSW parliament.[8]
- Privacy legislation for the NT public sector is currently before parliament, and is proposed for the Tasmanian public sector.[9] The standards in both cases are similar to those for the Victorian public sector.
- Queensland public sector agencies, except the Department of Health, comply with a mandatory information standard aligned with the Commonwealth public sector legislation. The Queensland Department of Health follows a mandatory information standard aligned with the private sector privacy legislation.[10] Local government is not covered by the Queensland scheme.
- South Australia complies with a mandatory privacy policy generally based on the Commonwealth public sector legislation.[11]
- Western Australian public sector agencies voluntarily follow the Commonwealth public sector legislation as an example of best practice.[12]
- Private sector organisations with an annual turnover of more than $3 million, and all traders in personal information and providers of health services, are covered by the Commonwealth

---

[6] *Privacy Act 1993.*

[7] *Privacy Act 1988* (Cwlth); *Information Privacy Act 2000* (Vic); *Privacy and Personal Information Protection Act 1998* (NSW).

[8] *Health Records (Privacy and Access) Act 1997* (ACT); *Health Records Act 2001* (Vic); NSW Health Records and Information Privacy Bill 2002.

[9] NT Information Bill 2002; *Tasmanian Information Privacy Legislation*, Issues Paper, Department of Premier and Cabinet, November 2001.

[10] Information Standards 42 and 42A.

[11] Cabinet Administrative Instruction No. 1 of 1989.

[12] 'The Privacy Situation in Western Australia,' webpage, Department of Industry and Technology, August 2002.

privacy legislation. They comply with different standards to those applying to the Commonwealth public sector.[13]

The various standards have been compiled and compared in a separate document, which was prepared in conjunction with this issues paper: 'Privacy Principles: Comparison of Current Laws and Rules.'

Shared features of privacy regimes

Although there are differences, there is a great deal of similarity among the various schemes. All of them:

- Protect 'personal information'
- Promote openness as well as confidentiality
- Supplement other relevant legislation
- Recognise other public interests
- Are based on Privacy Principles

Protecting 'personal information'

All of the privacy regimes protect 'personal information'. Definitions of 'personal information' differ, but all are adopted or adapted from the Commonwealth *Privacy Act 1988*:

> 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.

The *ANZLIC Privacy Best Practice Guideline* uses this definition as well.

The most significant inconsistency and source of confusion about the various definitions is whether or not 'personal information' includes information on public registers. Even where public register information is clearly not included, it is usually protected — as far as possible — as if it is.

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 is unlikely to hold any information about an

[13] Commonwealth government agencies comply with 11 Information Privacy Principles at s 14 of the *Privacy Act 1988* (Cwlth); private sector organisations comply with 10 National Privacy Principles at Schedule 3 of the Act.

identifiable person. However, if it is 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 this 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.

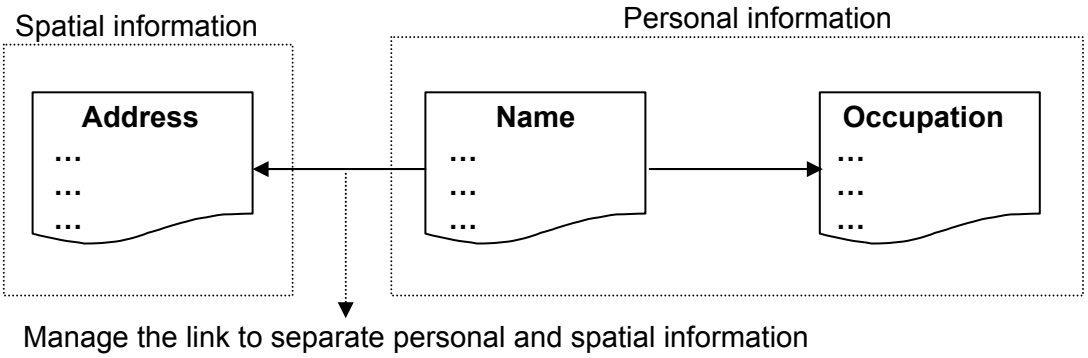
Cadastral data is an example of the linkages between personal and spatial information because it contains information about the person as well as information about the property with which he or she is connected. When these two types of information are combined or linked, they fall within the definition of 'personal information'. However, if information about the property is extracted and separated from the information about the person, it is no longer 'personal information.' Most, but not all, cadastral data is available on public registers, as required by law. Ensuring that cadastral information is readily available for legitimate and reasonable purposes yet protected from being misused requires clear and consistent rules about which data elements can be accessed, by whom, why, and under what conditions. Such rules have always existed, but they are given greater significance by the introduction of privacy legislation and are placed under greater pressure by the application of new technology.

New Zealand and New South Wales privacy laws contain specific principles for the handling of public register information. They support access and use for purposes that are consistent with the purpose for which the register was created and the person's reasonable expectations. Other countries have encountered the same challenge. In France, personal information on the cadastral register is public, but may not be used for commercial purposes. Greece decided to change the organisation of its cadastral register from being based on an alphabetical index of property owners to being based on the properties themselves. The intention is to prevent users from carrying out searches on the property owned by a single individual. Access to the cadastral register requires proof of legitimate interest.

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.



For the purposes of developing the *ANZLIC Privacy Best Practice Guideline*, spatial information is divided into three categories.

- ***Personal information***

  Personal information means 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. It is information that depends solely on the individual's identity and personal circumstances and is independent of his or her location.

- ***Spatial information***

  Spatial information means 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***

  Personal spatial information means *personal information* combined with, linked to, or contained within *spatial information*. Examples are: a mailing list of names and addresses, and 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.

These categories are represented in the following diagram, with some examples included at Table 1.

Components of spatial information
for the purposes of the *ANZLIC Privacy Best Practice Guideline*

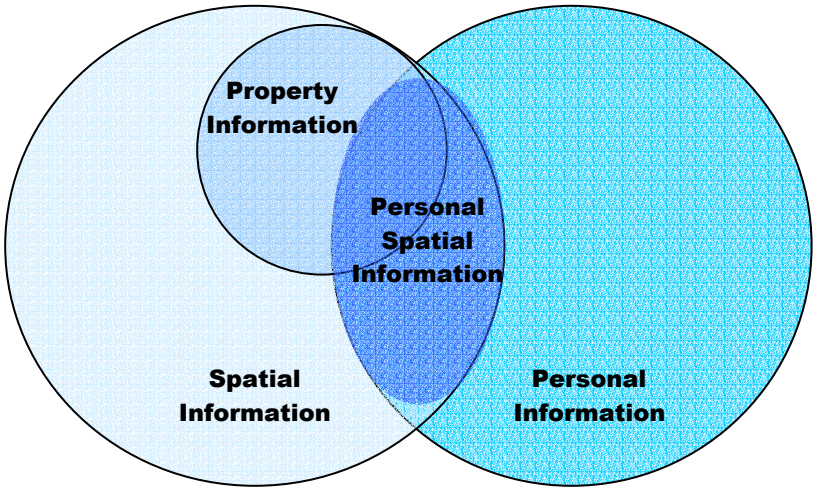


Table 1 **Examples of components of spatial information.**

Personal information	Spatial information	Property information
Name	Land administration boundaries	Sale price history
Phone number	Land use development zones	Valuation
Occupation	Topographic, oceanographic and geological map data	Land use improvements
Mortgage, lease and licence conditions	Marine and coastal boundaries	Street address
Professionals/businesses representing the person	Digital elevation models and bathymetry	Property identifier
Identification of the person as bankrupt or a judgment debtor	Aerial and satellite imagery	Volume/folio number
Identification if represented pursuant to an order under guardianship legislation	Geodetic control networks and geoid models	Council property number
	Statistical boundaries	Dimensions
		Construction material
		Date of construction
		Utility providers
		Car parking (commercial sites)

Promoting openness as well as confidentiality

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.

One possible option, for example, is to be more open with the public about who has had access to their information on a public register. It would not only make the process clearer, it could make the users more accountable.

It is proposed that the *ANZLIC Privacy Best Practice Guideline* appears on the ANZLIC web site alongside other policy documents.

Supplementing other relevant legislation

Privacy laws and policies do not override other legislation that regulates how personal information is handled. Government agencies have many Acts that authorise the collection, use and disclosure of information. Those that are relevant to spatial information need to be identified. Organisations have to inform people of any laws that require information to be collected from them. Also, when relying on a law for the authority to disclose personal information, it is good to be sure about what provision actually applies.

This could be a major task for government agencies. Queensland alone has reported that 188 separate pieces of legislation define or affect the administration or management of property rights in Queensland, though not all would involve the collection, use or disclosure of personal information.

Recognising other public interests

There is no absolute right to privacy. Privacy laws and policies recognise that the public interest in protecting privacy needs to be balanced with other public interests. They tend to accommodate a variety of interests, but those about which government agencies have expressed most concern are law enforcement and health and safety.

The *ANZLIC Privacy Best Practice Guideline* reflects this position and recommends that protocols or other agreements be prepared to facilitate liaison with law enforcement bodies. However, the Guideline does not intend to override the privacy regime in any jurisdiction. Government agencies would remain able to respond as authorised by their regime to support other public interests.

Based on Privacy Principles

All of the privacy laws and policies are based on Privacy Principles. These Principles set parameters within which organisations can exercise judgment about how to handle personal information in different circumstances. They are reasonably similar from one jurisdiction to the next, but not all are relevant to ANZLIC. For example, there are special provisions for 'health information' and 'sensitive information,' as defined in the legislation.

The *ANZLIC Privacy Best Practice Guideline* has been prepared by assessing the highest standards required of all the Privacy Principles combined. The aim is to be reasonably sure that any ANZLIC member operating in accordance with the Guidelines is not breaching any privacy law or rule. The Principles are presented as 'Best Practice Guideline Standards' with a commentary to inform and guide best practice and to address the privacy risks.