ANZLIC SPATIAL INFORMATION PRIVACY BEST PRACTICE GUIDELINE

Version 2.0 (Final)

14 February 2004

CONTENTS

INTRODUCTION

Purpose

ANZLIC is working to improve the quality and accessibility of public sector spatial data and encourage the development of an innovative and competitive spatial information industry.

Above all, ANZLIC fosters responsible management of this critical national resource. ANZLIC recognises that advances in information technology are fuelling community concern about the impact on privacy; and is striving to ensure that the benefits from easier access to, and better utilisation of, spatial information are realised without adding to this concern.

Almost all government agencies are required to comply with privacy laws or government directives on the handling of personal information. The rest soon will be. While similar in many respects, the standards differ from one jurisdiction to the next. The *ANZLIC Privacy Best Practice Guidelines* reflect the highest standards across all jurisdictions.

By developing and implementing these Best Practice Guidelines, we aim to:

- Ensure each government agency is confident that any personal information shared with another will continue to be protected to the same or a higher standard.
- Encourage good privacy practices throughout the spatial information industry.
- Build community trust in our commitment to protect privacy.

Coverage

This policy applies only to spatial information — specifically, spatial information that is linked to personal information. Not all information that government agencies handle is spatial information. Similarly, not all personal information that government agencies collect is related to spatial information. It varies according to the range of functions each organisation performs.

Status

This document represents best practice guidelines. It has no legal force and is not intended to override accountabilities where jurisdictional legislation or directives in relation to privacy apply.

Implementation advice

The Privacy Commissioners have issued guidelines and other materials to help organisations comply with the Privacy Principles on which their respective privacy laws are based; and on which the Policy Standards in this document are based. Government agencies that are not covered by privacy legislation are advised to consult the comprehensive collection of advice available from the Federal Privacy Commissioner.

Federal Privacy Commissioner <www.privacy.gov.au>

NSW Privacy Commissioner <www.lawlink.nsw.gov.au/pc.nsf/pages/index>

Victorian Privacy Commissioner <www.privacy.vic.gov.au>

New Zealand Privacy Commissioner <www.privacy.org.nz>

Target audience

These privacy guidelines are designed for public sector agencies that are custodians of; or collect, maintain or distribute; information with a spatial content.

DEFINITIONS

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 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.

Personal spatial information

Personal spatial information means 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.

Consent

Consent[*] means express consent or implied consent.

Generally available publication

Generally available publication[†] means a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public.

Public register

Public register[‡] means 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.

Law enforcement agency

Law enforcement agency[§] means:

(a) the Australian Federal Police; or

(b) the Australian Crime Commission; or

(c) the Australian Customs Service; or

(d) the Australian Prudential Regulation Authority; or

(e) the Australian Securities and Investments Commission; or

(f) another agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or prescribed law; or

(g) another agency, to the extent, that it is responsible for administering a law relating to the protection of the public revenue; or

(h) a police force or service of a State or a Territory; or

---

[*] Definition of *consent* taken from Part II Interpretation, Section 6 of the *Privacy Act 1988* (Cwlth).

[†] Definition of *generally available publication* taken from Part II Interpretation, Section 6 of the *Privacy Act 1988* (Cwlth).

[‡] Definition of *public register* taken from Part 1 Section 3 of the *Information Privacy Act 2000* (Victoria).

[§] Definition of *law enforcement body* taken from *enforcement agency* Part II Interpretation, Section 6 of the *Privacy Act 1988* (Cwlth).

(i) the New South Wales Crime Commission; or

(j) the Independent Commission Against Corruption of New South Wales; or

(k) the Police Integrity Commission of New South Wales; or

(l) the Criminal Justice Commission of Queensland; or

(m) another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries; or

(n) a State or Territory authority, to the extent that it is responsible for administering , or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or

(o) a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue.

Unique identifier

Unique identifier means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name.

BEST PRACTICE GUIDELINE STANDARDS

1. Collect only what is necessary

Personal spatial information is not collected unless:

- The information is collected for a lawful purpose that is directly related to a function or activity of the collector; and
- The collection of the information is necessary for that purpose.

Wherever it is lawful and practicable, individuals have the option of not identifying themselves when entering transactions.

Commentary

Properly anonymous and properly de-identified information is likely to be *personal information* within the meaning of privacy laws. The more personal information you collect, the more organisations must spend resources on complying with other aspects of privacy law.

Organisations may collect specific personal information from prescribed forms, or forms they have devised in-house and certain personal information from these forms may find its way onto public registers. In many instances not all of the information collected on the forms will need to be included in the public register. For example, an individual may have a choice about providing a residential or work address or private or work telephone number. Forms should state clearly which information must be provided compulsorily and which is optional.

2. Collect fairly and lawfully

Personal spatial information is not collected by means that are unlawful or unfair or that intrude to an unreasonable extent upon the personal affairs of the individual concerned.

3. Collect directly from the person

Personal spatial information is collected directly from the individual or someone they have authorised to provide the information (such as a legal representative).

Exceptions apply:

- When the personal information is contained in a public register; or

- When the personal information is published in a magazine, book, newspaper or other generally available publication, whether in paper or electronic form; or
- When the collection from another source is required or authorised by law.

Commentary

Government agencies usually collect personal spatial information directly from the person or from someone who is acting on their behalf with their knowledge. For example, the purchaser's mortgagee rather than the purchaser often provides land title registration details.

The exceptions allow for circumstances where it is not practicable or possible to collect from the person. Some jurisdictions allow for other circumstances. This policy does not override them: it sets out best practice.

4. Inform the person about the collection

At or before the time (or, if that is not practicable, as soon as practicable after) personal spatial information is collected from the individual concerned, reasonable steps are taken to ensure that the individual is aware of:

- The fact that the information is being collected; and
- The name and address of the organisation collecting it; and
- The name and address of the organisation holding it; and
- The purpose for which the information is being collected; and
- If the collection of the information is authorised or required by law – the fact that the collection is so authorised or required and the title of the particular law; and
- The main consequences (if any) for the individual if all or part of the information is not provided; and
- Any person to whom, or organisation to which, it is the collector's usual practice to disclose personal information of the kind collected and (if known to the collector) any person to whom, or organisation to which, it is the usual practice of the first-mentioned person or organisation to pass on that information; and
- The individual's rights of access to and correction of the information.

If personal information is collected about an individual from someone else, reasonable steps are taken to ensure that the individual is, or has been, made aware of these things.

Commentary

This requirement applies not only to the collection of personal spatial information but also to the collection of personal information about individuals who access personal spatial information held on public registers.

Some jurisdictions require individuals to be notified of fewer matters than those listed in this policy do, and in different combinations. Meeting this standard should mean that all requirements across government agencies are met.

Where a third party provides *personal spatial information*, either the third party should notify the person of the things listed above or the relevant government agency should do so. For example, agents acting on behalf of the person could be given a brochure to pass on.

Purpose of collection

Examples of the purposes for which government agencies collect personal spatial information are:

- To record and administer property transactions; or
- To administer taxes, rates and other government charges connected with property ownership or occupancy; or
- To administer laws connected with the ownership and occupancy of property; or
- To support the provision of utilities and local government services to properties, and for health concerns where uninterrupted supply is critical; or
- To maintain a transparent market in land as a means of protecting land title.

Right of access

It should be noted that individuals have right of access and correction of their personal spatial information. Personal spatial information held by public sector organisations will be able to be accessed informally through administrative processes without the need to make a formal freedom of information (FoI) request. 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 formal FoI requests may be avoided.

Complaints

Public sector organisations need to make known to individuals their internal complaints handling structure for resolving individuals concerns about the management of personal information within the spatial industry. 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.

5. Use and disclosure for authorised purposes

Personal spatial information that was obtained for a particular purpose is not used or disclosed for any other purpose or in a way that intrudes to an unreasonable extent upon the personal affairs of the individual concerned.

Exceptions apply:

- For a purpose that is directly related to the purpose for which the information was collected and the individual concerned would reasonably expect it to be used or disclosed for that purpose; or
- When the individual concerned has consented; or
- When required or authorised by or under law; or
- When reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue (in which case a record is kept of the use or disclosure); or
- When necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person or to public health or safety; or
- When disclosure is at the request of the person who initially provided the information.

Personal spatial information is used only for a purpose for which the information is relevant.

Commentary

Decisions about which data elements are made available, to whom, for what purposes and under which conditions need to be based on step by step analysis.

The exceptions allow for circumstances when it is in the person's interest or the public interest to use or disclose personal information for purposes that are unrelated to the purpose for which it was collected. Some jurisdictions allow for additional circumstances. The circumstances outlined in this policy are those that are most likely to apply to government agencies when handling spatial information.

Using and disclosing only for the purpose of collection

Meeting this standard is difficult when the personal information is held on a public register. Not only is the purpose of the register unlikely to be defined in the relevant legislation, the information is required by law to be available for inspection by any member of the public.

Government agencies have been making spatial information more readily accessible to the public and wish to maximise its usefulness. However, we also recognise that quicker, cheaper and easier accessibility increases the risk that personal information will be drawn from public registers for reasons that are seen as intrusive or inappropriate. Some agencies are specifically required by privacy legislation to address this risk.

Therefore, the procedures and technical conditions for access to spatial information need to support this Best Practice Guideline standard. Where personal spatial information is permitted or required to be available on a public register, the register should be administered in accordance with clear business rules that:

- Support and promote spatial data management and transactions; and
- Restrict searches on, compilation of, and subsequent use and disclosure of, personal information.

For example, the standard conditions for permitting searches on, and compilation of, personal information could include:

- Allowing access to personal spatial information held on public registers only on a record-by-record basis; in other words, not making this information available on a volume or bulk basis; or
- Not permitting searches using personal information.

Exceptions to the standard conditions should be allowed only for users that have a legitimate, identified, purpose and have access under licence or, if a government agency, under a memorandum of understanding or similar agreement. Licences would require compliance with the Commonwealth Privacy Act (see 'Promote Responsible Use of Spatial Information' below).

Other conditions of non-standard access could include:

- Regularly publishing lists of all organisations that have access to personal spatial information under licence or other agreement, and their reason for gathering the information; or
- Establishing audit trails of access to personal spatial information that could be made available to the individual on request (except where this would frustrate law enforcement functions); or
- Allowing individuals to opt-in of any non-standard access to their personal information for secondary commercial purposes.

Actions required or authorised by or under law

This exception recognises that government agencies administer legislation that requires or permits disclosure, such as the laws establishing public registers. It also recognises that other government agencies can exercise statutory powers to require disclosure, such as those exercised by the Australian Taxation Office.

Law enforcement

Government agencies support the work of law enforcement agencies. Ongoing arrangements are best formalised in memoranda of understanding. These can clarify the expected types of requests for assistance and allow ease of access for authorised personnel.

Health and safety

We consider our responsibilities to the community to include making spatial information readily available on request to emergency services organisations.

Public registers

Once personal information reaches a public register it is difficult to ensure that the information is only being accessed for the purpose it was intended. Nevertheless it is still possible to take reasonable steps to ensure that the personal information contained in public registers is protected against misuse, loss, and from unauthorised access modification or disclosure. In this context, organisations responsible for public registers may wish to consider:

- Having someone within the organisation responsible for the management of public registers;

- Providing the person who is responsible for the management of the register with training on privacy legislation;
- Making users of the public register aware, perhaps through statements or notices, that the register is available to be searched for a particular purpose and requiring users to confirm, by name and up-front, that they will use the information for that purpose only; and
- Limiting the bulk release of personal information, especially in digital form. Ideally public register information should be available on a record-by-record basis to those who have a purpose to search for them, without the ability to reproduce an entire database.

6. Manage transborder data flows

Personal spatial information is not transferred to anyone who is not subject to a law, binding agreement or contract which effectively upholds principles for fair handling of the information that are substantially similar to those with which Government agencies comply.

Exceptions apply:

- When required by law; or
- At the individual's request (in writing); or
- When the individual consents (in writing); or
- When required or authorised by law.

Commentary

Some jurisdictions allow additional exceptions. This policy does not override them, but sets out the circumstances that are most likely to apply to government agencies when handling spatial information.

When implementing transborder data flows, where practicable government agencies should provide evidence of consent by the individual for the transfer of their personal spatial information.

This includes transfers outside Australia or New Zealand, between jurisdictions, or between a jurisdiction and a private sector organisation.

7. Ensure data quality

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

- Accurate; and

- Up to date; and
- Complete; and
- Not excessive; and
- Relevant to the purpose for which it is collected or used, and
- Not misleading.

Commentary

In some cases, keeping information up to date has long been a statutory requirement. Such laws continue to take precedence over this policy.

The *ANZLIC Policy Statement on Spatial Data Management* includes a principle on conformity and quality. Good quality data is essential to the spatial information industry and ANZLIC is developing and updating national technical standards. In addition, a proposed ANZLIC paper on the issue of liability arising from the use of information containing errors, and from applying data to a purpose for which it was not originally intended, may give rise to recommendations for improvement.

8. Keep personal information secure

Personal spatial information is 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.

If it is necessary for the organisation to give personal spatial information to a person in connection with the provision of a service to the organisation, everything reasonably within its power is done to prevent unauthorised use or disclosure of information in the record.

Commentary

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.

9. Retain only as long as required

Personal spatial information is destroyed securely or permanently de-identified if it is no longer needed for an authorised purpose.

Commentary

The requirements to retain public sector information vary, and tend to be reflected in law.

10. Be open about practices

Any person can ascertain whether personal spatial information is held about them, the nature of the information, purposes for which it is used and how to gain access.

Documented policies on the management of personal spatial information are available to anyone on request. They explain:

- The nature of the information; and
- The purpose for which each type of information is kept; and
- The classes of individuals about whom it is kept; and
- How long each type of record is kept; and
- How it holds the information; and
- How it discloses it; and
- Who has the right to have access to it and under what conditions; and
- How to go about seeking access.

Commentary

ANZLIC places all of its policy documents on its website, and will include this policy as well. Individual members, representing key agencies responsible for the management of spatial information within their jurisdiction, will also prepare and publish their own privacy management policies.

Details about personal information held by the ACT and Federal Government agencies are collected by and available from the Federal Privacy Commissioner (pursuant to the Information Privacy Principle 5 of the *Commonwealth Privacy Act 1988*).

11. Provide a right of access and correction

Individuals have the right to seek access to personal spatial information held about them and to have it corrected if necessary

Commentary

Personal spatial information held on public registers about a person is available for their inspection, as authorised or required by law. Personal spatial information not held on public registers is accessible under separate freedom of information and/or privacy legislation. Government agencies are unlikely to hold personal spatial information that the individual concerned is not able to see, other than perhaps any evidence of current investigations by law enforcement agencies.

12. Promote responsible use of spatial information

A condition of all licences to use spatial information that either contains personal spatial information—or that the licensee can conceivably combine with personal information or any other information to produce personal spatial information—is that the licence holder is accountable under privacy legislation.

Commentary

This provision addresses two fundamental risks to privacy arising from the application of new technology to spatial information.

- The risk that personal spatial information collected can be used for purposes that are unrelated to the purpose for which it was originally provided; and
- The risk that spatial information containing no personal information can be manipulated and combined with other information to reveal details about an identifiable individual.

The New Zealand Privacy Act applies to the entire private sector. The Australian Government Privacy Act applies only to private sector organisations with an annual turnover of more than $3 million and all those that trade in personal information or provide health services. Nonetheless, private sector organisations that are not covered may opt-in.

Private sector organisations need to be aware that if they undertake government contracts they may have to operate within State, Territory or Federal privacy frameworks designed for the public and private sectors. *Without such a condition in the contract the outsourcing organisation will be responsible for any breaches of privacy by their service providers.*

By including this requirement in licences, the personal spatial information that any Australian private sector organisation handles must be protected in accordance with the National Privacy Principles in the Privacy Act. Anyone who believes their personal spatial information has not been handled in accordance with the National Privacy Principles would have a right of redress.