AUSTRALIAN COMMUNICATIONS INDUSTRY FORUM

INDUSTRY GUIDELINE

PRIVACY PROTECTION IN ACIF PUBLICATIONS

ACIF G611
DECEMBER 2002

Industry Guideline– ***Privacy Protection in ACIF Publications***

First published as ACIF G611 2002.

ISBN: 1 74000 211 3

Disclaimers

1. Notwithstanding anything contained in this Guideline:
   (a) ACIF disclaims responsibility (including where ACIF or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:
      (i) reliance on or compliance with this Guideline;
      (ii) inaccuracy or inappropriateness of this Guideline; or
      (iii) inconsistency of this Guideline with any law; and
   (b) ACIF disclaims responsibility (including where ACIF or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Guideline.
2. The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

EXPLANATORY STATEMENT

INTRODUCTION

The Privacy Advisory Group (PAG) was established by the Consumer Codes Reference Panel (CCRP) in August 2000 to:

- act as a resource on privacy, available to all ACIF Reference Panels, Working Committees and able to assist with other activities as required;
- promote a consistent privacy practice across ACIF Codes and Standards; and,
- undertake specific tasks assigned to it by the CCRP on current privacy issues which may impact on ACIF processes or outputs.

The specific task undertaken by the PAG has been to advise the CCRP on consumer awareness of Calling Number Display and its privacy implications, as required under ACIF C522:2001 ***Calling Number Display*** Industry Code. The PAG has also advised the CCRP on the *Privacy Amendment (Private Sector) Act 2000* and its implications for the telecommunications industry.

Parts of the telecommunications industry have been subject to privacy protection requirements since 1988 when Telstra (then Telecom) was bound by the provisions of the *Privacy Act 1988*. The Privacy Act also covered all carriers and carriage service providers (CSPs) in relation to credit issues and the use of tax file numbers (TFNs). Since 1991, carriers and CSPs have generally been prohibited under telecommunications legislation from using or disclosing either the contents of a communication carried by a carrier or CSP, or personal information it has collected about individuals. The *Telecommunications Act 1997* (the Act) currently provides for this privacy protection.

In December 2001, the *Privacy Amendment (Private Sector) Act 2000* came into effect, extending privacy protection requirements to the private sector, with the exception of some small businesses. These are encompassed in the National Privacy Principles (NPPs). The Privacy Act is administered by the Office of the Federal Privacy Commissioner (OFPC), which can also handle complaints where there is an alleged breach of one or more of the NPPs. The amendments also allow for the development of privacy codes, which can be approved by the OFPC. The privacy code must provide equivalent or better protection for individuals than that provided by the NPPs.

The importance of the *Privacy Amendment (Private Sector) Act 2000* for the telecommunications industry is that privacy protection requirements, additional to those in telecommunications legislation, have been imposed on industry participants. Additionally, the Privacy Act requires that the Australian Communications Authority (ACA) consult with the OFPC before registering any industry code that has privacy implications.

This Guideline is intended to provide guidance for ACIF Reference Panels, Working Committees and Working Groups when developing Codes and Standards and assist those entities to understand the industry's obligations under the Privacy Act.

Michael Pickering
Chairman
CCRP/WG1 – ***Privacy Advisory Working Group***

INDUSTRY GUIDELINE

TABLE OF CONTENTS

1. SCOPE

1.1.1 The objective of this Guideline is to provide guidance to ACIF Reference Panels, Working Committees and Working Groups on privacy implications which may arise when developing ACIF documents (for example, a Code, Guideline, Standard or other document). It is intended that this Guideline will assist in ensuring that ACIF documents meet privacy requirements.

1.1.2 Section 5 of this Guideline provides specific questions which ACIF Reference Panels, Working Committees and Working Groups should consider in assessing whether their document may have privacy implications.

1.1.3 If, after reading the Guideline, a Reference Panel, Working Committee or Working Group considers that privacy implications will arise, further advice can be obtained from the Privacy Advisory Group (PAG). The issue should first be raised to the CCRP who will refer the matter to the PAG if appropriate. The PAG may:

(a) Consider the issue;

(b) Confirm that a privacy issue(s) does or does not exist; and,

(c) Suggest a course of action to address the issue(s).

1.1.4 This course of action may include, but is not limited to:

(a) Drafting by a legal representative; or

(b) Consultation with the OFPC.

2. PARTICIPANTS

The group that developed this Industry Guideline consisted of the following organisations and their representatives:

Representative	Organisation
Michael Pickering (Chairman)	Telstra
Rosie Rowe	Optus
Robyn Ziino	AAPT
Julian Gorman	Vodafone
Trent Czinner	Hutchison Telecoms

Holly Raiche of ACIF supplied project management support.

3. DEFINITIONS AND ABBREVIATIONS

For the purposes of this Guideline, the following definitions and abbreviations apply:

3.1 Abbreviations

ACA means the Australian Communications Authority.

ACCC means the Australian Competition and Consumer Commission.

ACIF means the Australian Communications Industry Forum.

Act means the *Telecommunications Act 1997* (Cth).

CLI means Calling Line Identification.

CND means Calling Number Display and has the same meaning as contained in the ACIF C522:2001 ***Calling Number Display*** Industry Code.

CSP means Carriage Service Provider.

GCSP means Gaining Carriage Service Provider and is used in the context of the Mobile Number Portability Code.

IPND means Integrated Public Number Database.

LCSP means Losing Carriage Service Provider and is used in the context of the Mobile Number Portability Code.

NPPs means the National Privacy Principles.

OFPC means Office of the Federal Privacy Commissioner.

SFOA means Standard Form of Agreement.

TAF means Transfer Acknowledgement Form and is used in the context of the Commercial Churn Code.

TFN means Tax File Number.

TIO means Telecommunications Industry Ombudsman.

3.2 Definitions

Act means the *Telecommunications Act 1997* (Cth).

Billing Code means ACIF C542:2001 ***Billing*** Industry Code.

Carriage Service Provider has the meaning given by Section 87 of the Act**.**

Carrier has the meaning given by Section 7 of the Act.

CND Code means ACIF C522:2001 ***Calling Number Display*** Industry Code.

Commercial Churn Code means ACIF C531:2002 ***Commercial Churn*** Industry Code.

Credit Management Code means ACIF C541:2001 ***Credit Management*** Industry Code.

Complaint Handling Code means ACIF C547:2001 ***Complaint Handling*** Industry Code.

Customer Transfer Code means ACIF C547:2001 ***Customer Transfer*** Industry Code.

IPND Code means ACIF C555:2002 ***Integrated Public Number Database*** Industry Code.

Mobile Number Portability Code means ACIF C570:2002 ***Mobile Number Portability*** Industry Code.

National Privacy Principles means the principles contained in Schedule 3 of the Privacy Act.

Privacy Act means the *Privacy Act 1988* (Cth**).**

Privacy Code means ACIF C523:2001 ***Protection of Personal Information of Customers of Telecommunications Providers*** Industry Code**.**

Privacy Commissioner means the Federal Privacy Commissioner as established under the Privacy Act**.**

Standard Form of Agreement means a standard agreement for the supply of carriage services under section 479 of the Act**.**

TIO Scheme refers to the obligations on carriers and CSPs under part 6 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999.*

Trade Practices Act means the *Trade Practices Act 1974* (Cth).

Transfer Acknowledgement Form means as defined in ACIF C531:1999 ***Commercial Churn*** Industry Code, and is used to mean a form completed by the authorised customer in order to authorise a churn by that customer to another CSP.

4. LEGISLATIVE FRAMEWORK

The following is a summary of some applicable legislation that has privacy implications and information on relevant telecommunications regulators and their relevance to privacy in the telecommunications industry

The Privacy Commissioner has the primary responsibility for privacy protection in the telecommunications industry. The TIO also has general jurisdiction in handling privacy complaints. Carriers and CSPs should provide customers with the option to escalate a privacy complaint to either the Privacy Commissioner or the TIO.

Note: It is recognised within the telecommunications industry that this may lead to a small amount of 'forum shopping' by customers when escalating their privacy complaint and carriers and CSPs need to be prepared for this.

4.1 Telecommunications Act 1997

4.1.1 Part 13 of the Act contains provisions imposing privacy obligations on carriers, CSPs and their employees (amongst others) to protect the confidentiality of information relating to:
(a) the contents of communications that have been, or are being carried by carriers or CSPs;
(b) carriage services supplied by carriers or CPS; and,
(c) the affairs or personal particulars of another person.

4.1.2 Protected information may be used or disclosed in limited circumstances specified in the Act.

4.1.3 The Act also restricts the secondary use or disclosure of information and imposes record keeping requirements.

4.1.4 Carrier and CSP's disclosure practices can be audited by the Privacy Commissioner and an annual report of disclosures must be provided to the ACA.

4.2 Privacy Act 1988

From 21 December 2001, the Privacy Act created a separate privacy scheme for the private sector. This is in addition to the provisions already contained in the Privacy Act relating to the Commonwealth public sector, credit reporting and TFNs.

4.2.1 The Privacy Act requires carriers and CSPs to comply with the National Privacy Principles in the collection, storage, use, correction, disclosure or transfer of personal and sensitive information.

4.2.2 Personal and sensitive information may only be collected if necessary for one or more of the functions or activities of carriers and CSPs and must be collected only by lawful and fair means.

4.2.3 Personal and sensitive information may only be used or disclosed in limited circumstances specified in the Privacy Act.

4.2.4 Secondary use and disclosure is also restricted by the Privacy Act and specific access and correction requirements are imposed.

4.3 ACIF C523:2001 *Protection of Personal Information of Customers of Telecommunications providers* Industry Code

4.3.1 The Act also provides for the development and registration by the ACA of industry codes and standards. The Privacy Code has been developed but is not currently registered with the ACA. All telecommunications providers are required to comply with a registered Code but compliance with the Privacy Code is voluntary.

4.3.2 There is a high level of consistency between the NPPs and the Privacy Code.

4.4 Privacy Commissioner

4.4.1 The Privacy Commissioner administers the Privacy Act and oversees regulation of privacy in the private sector.

4.4.2 It is highly desirable for the industry to consult with OFPC on issues with significant privacy implications.

4.4.3 The Privacy Commissioner is responsible for monitoring compliance with the record keeping requirements imposed under the Act.

4.4.4 Privacy complaints arising from telecommunication breaches can be made to the OFPC.

4.5 Telecommunications Industry Ombudsman (TIO) Scheme

The TIO, under its general jurisdiction, can handle complaints about alleged breaches of privacy by carriers and CSPs.

4.5.1 All carriers and CSPs are required to be participants in the TIO scheme, which operates independently of government, Carriers, CSPs and other interested bodies.

4.5.2 Privacy complaints from customers need to first be addressed via the Carrier or CSP's internal complaint handling procedures. If the matter cannot be satisfactorily resolved within a reasonable period of time, the customer can escalate their complaint to the TIO. Carriers and CSPs should ensure that customers are aware of their right to escalate their complaint.

4.5.3 Under section 114 of the Act, industry codes and standards may confer powers on the TIO. The TIO may have regard to those codes and standards when determining a customer's complaint.

4.6 ACA

The ACA has specific roles under the Act in relation to privacy in the following areas:

4.6.1 The ACA administers the Act, including Part 13 of the Act.

4.6.2 The ACA and ACIF must consult the Privacy Commissioner on industry codes intended for registration which address matters dealt with by the Privacy Act;

4.6.3 If a Carrier or CSP implements new technology or modifies existing technology in a manner that impacts upon its ability to meet its interception obligations under Part 15 of the Act, it must notify the ACA. The ACA is required to consult with agencies regarding a carrier or CSP's intention to implement a new technology or change an existing technology.

4.6.4 Under Part 15 all carriage services are to have interception capability unless an exemption is granted by the Agency Coordinator (Attorney General's Department) or the ACA. Carriers are also obligated to submit an annual Interception Capability Plan (ICP) to the Agency Coordinator and the ACA.

4.6.5 The ACA is responsible for monitoring industry compliance with registered codes. Under the Act, it has the power to direct compliance with registered codes. If the ACA determines that industry cannot agree on the content of an industry code or that an industry code is failing to meet its objectives, the ACA may determine an industry standard. Compliance with an ACA industry standard is mandatory.

4.6.6 The ACA cannot determine a standard if the standard relates to privacy and compliance with the standard would be likely to have the effect of requiring customer equipment, customer cabling, a telecommunications network or a

facility to have particular design features or to meet particular performance measures. The ACA can however determine a standard relating to privacy if the benefits to the community outweigh the costs of compliance with the standard.

4.7 ACCC

4.7.1 The OFPC and the ACCC have signed a memorandum of understanding (MoU), enabling them to establish joint taskforces to assist each other with enforcement, investigations, litigation and training.

4.7.2 Organisations not acting in accordance with the NPPs, for example NPP 2 on Use and Disclosure, could be considered to be engaging in misleading and deceptive conduct which is prohibited under section 52 of the TPA.

5. KEY CONCEPTS IN THE NATIONAL PRIVACY PRINCIPLES

This section describes some of the key concepts are used in the NPPs and their use in this Guideline

5.1 Access

5.1.1 Access refers to a person's right to see or know about the personal information an organisation holds on them.

5.2 Collection

5.2.1 An organisation collects personal information if it gathers, acquires or obtains information from any source or by any means, in circumstances where the individual is identified or is identifiable. It includes information that:

(a) an organisation comes across by accident or has not asked for but nevertheless keeps;

(b) information the organisation receives directly from the individual; and,

(c) information about an individual an organisation receives from somebody else.

5.3 Consent

5.3.1 Consent means voluntary agreement to some act, practice or purpose. It has two elements: knowledge of the matter agreed to, and voluntary agreement. Consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation. Consent is invalid if there is extreme pressure or coercion.

5.4 Disclosure

5.4.1 An organisation discloses information when it releases information outside the organisation. Examples of disclosures include:

(a) when an organisation gives another organisation information under contract to carry out an "outsourced" function;

(b) when an organisation sells information to another organisation; or

(c) when an organisation discloses information about one individual to another individual or makes the information publicly available

5.5 Personal Information

5.5.1 Personal information means information or an opinion (including information or an 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.

5.5.2 Personal information must relate to a natural person. A natural person is a human being rather thana company.

5.5.3 Personal information can range from the very sensitive (for example, political beliefs, medical history, sexual preference or medical records) to the everyday (for example, hair colour, address, phone number). The information need not be accurate, it may include opinion and speculation

and it may simply be false information. It doesn't matter whether the information is held in a computer database, or in paper records, or in any other medium. If the information itself makes it clear which individual it is about then the person is identifiable. Whether a person's identity is reasonably ascertainable will depend on the context and on who holds the information.

5.5.4 For the telecommunications industry this will include, but is not limited to,:

(a) Narrations on customer service systems; and,

(b) Billing information, including A party and B party numbers;

5.6 Primary Purpose

5.6.1 The primary purpose is the dominant or fundamental reason for information being collected in a particular transaction.

5.7 Secondary and Related Purposes

5.7.1 Secondary purposes are purposes other than the primary purpose that an organisation has in mind for the information it collects. For a secondary purpose to be related to the primary purpose, the secondary purpose must be something that arises in the context of the primary purpose. The Privacy Act permits personal information being used for secondary purposes that are within the reasonable expectations of individuals (as well as in some other specific situations).

5.8 Sensitive Information

5.8.1 Sensitive information is information or an opinion about an individual's:

(a) racial or ethnic origin;

(b) political opinion;

(c) membership of a political association or religious beliefs, affiliations or philosophical beliefs;

(d) membership of a professional or trade association or membership of a trade union;

(e) sexual preferences or practices;

(f) criminal record;

(g) health information about an individual; or,

(h) disability.

5.9 Use

5.9.1 Use of personal information relates to the handling of the personal information within the organisation. Examples of uses of information include, but are not limited to:

(a) matching of data from a company's data bases; and

(b) forming an opinion based on information collected and noting it on a file.

6. GUIDELINES

This section provides guidance on potential privacy issues that may arise in the course of Reference Panel, Working Committee and Working Group work and provides examples of potential privacy issues for the telecommunications industry.

6.1 Collection (NPP 1):

6.1.1 Requirement

(a) Personal Information should only be collected:

(i) if it is necessary for one or more of the functions or activities of the organisation; and.

(ii) only by lawful and fair means and not in an unreasonably intrusive way.

(b) NPP 1 requires organisations to make it clear to individuals, at or before the time of collection (or, if that is not practicable, as soon as practicable after),who is collecting their information why it is being collected, how the individual can gain access to the information held about them and the consequences for the individual if they do not provide the information.

(c) Personal Information should generally be collected directly from the individual. If the individual's personal information is indirectly collected, that is from another person or organisation, then the individual should be informed of this as soon as possible after the indirect collection.

NOTE: Organisations would, in most cases, be responsible for the acts of its contractors.

6.1.2 Relevance

(a) Does the ACIF work refer to the collection of personal information, including:

- Collection either directly from the customer or indirectly from a third party?
- Collection via the interception of communications or surveillance?
- Collection via CLI or other means?
- Collection of sensitive information?

6.1.3 Examples

(a) Billing Code

In the Billing Code, one of the Code Rules is that carriers and CSPs must include certain information on a customer's bills. The majority of this information may not fall under the Privacy Act, however there is a requirement to collect the customer's billing name and address. This involves a collection of personal information from the customer and would fall within NPP 1 (Collection).

(b) Commercial Churn Code

In the Commercial Churn Code, carriers and CSPs must obtain, amongst other things, the consent of a customer via a TAF. This is a collection of personal information and would fall within NPP 1

(Collection).

(c) Customer Transfer Code

The Customer Transfer Code is concerned with selling practices such as door to door selling or outbound telemarketing. Carriers and CSPs may use independent sales organisations to sell their product on their behalf. The collection of personal information by sales agents is still a collection under the Privacy Act and the carrier, CSP and the independent sales organisation needs to be aware of NPP 1 (Collection).

6.2 Use and Disclosure (NPP 2)

6.2.1 Requirement:

(a) NPP 2 requires that Personal Information must generally only used for the purpose that it was collected, that is the primary purpose of collection. This means that organisations should not use or disclose an individual's personal information for any reason other than to provide the individual with service , subject to the secondary purpose uses that are permitted, In addition to the primary purpose, personal information may be used for other purposes (a secondary purpose):

(i) if the secondary purpose is related to the primary purpose and would be within the reasonable expectations of the individual; or

(ii) where the individual has consented; or

(iii) for direct marketing if certain strict criteria are met; or,

(iv) for law enforcement reasons.

6.2.2 Relevance

(a) Does the ACIF work refer to the use of personal information? For example, for marketing, activation, fault rectification, etc.

(b) Does the ACIF work involve the disclosure of personal information:

- to a third party; or,
- as a result of network or operational requirements?

6.2.3 Examples:

(a) Credit Management Code

The Credit Management Code outlines a process that must be followed when assessing a customer for credit. This includes obtaining the customer's consent when seeking a credit report from external sources and informing the customer that their personal information and their application for credit may be disclosed to external sources.

In the telecommunications industry, generally, but not always, the primary purpose for collecting customer information is for the provision of a service to the customer. This information can then be used or disclosed for this primary purpose or related secondary purposes. In relation to related secondary purposes, the customer must either consent or would reasonably expect the carrier or CSP to use the information for that secondary purpose.

In the case of using and disclosing the customer's information for the purposes of credit management, this would be defined as a related secondary purpose that the individual would reasonably expect. To be absolutely certain, the requirement to use and disclose the

customer's information for credit management purposes should be included in the SFOA or other customer terms and conditions.

(b) Commercial Churn Code

In a commercial churn, the customer's personal information may be passed to other telecommunications providers to effect the churn. This is a use and disclosure of customer's personal information. Although it would generally fall within the related secondary purpose, it would be wise to include information regarding transfer of customer's information to other telecommunications providers in the SFOA or other customer terms and conditions.

(c) IPND

Carriers and CSPs have an obligation to disclose information to the IPND. This is a use and disclosure of customer's personal information. Although it would generally fall within the related secondary purpose, it would be wise to include information regarding transfer of customer's information to other telecommunications providers in the SFOA or other customer terms and conditions.

6.3 Data Quality (NPP 3)

6.3.1 Requirement

(a) 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.

6.3.2 Relevance

(b) Does the ACIF work impact on an organisation's data quality, for example, require specific accuracy verification?

6.3.3 Examples

(a) Commercial Churn Code

The Commercial Churn code discusses the concept of invalid churns. A churn may be invalid because the information held by the losing party is inaccurate or out of date or invalid. A carrier and CSP has an obligation to hold information that is accurate, complete and up to date.

(b) Mobile Number Portability Code

Ports can be rejected by the LCSP for a limited number of reasons. One of these may be where the account number does not match the mobile number. It is possible that this port could be rejected as the LCSP has not kept their systems up to date. Carriers and CSPs have an obligation to keep customer's personal information accurate, complete and up to date.

(c) Credit Management Code

The Credit Management Code details Carriers and CSP's obligations to ensure that customer information in the credit reporting databases is kept up to date. For example Carriers and CSPs must ensure that credit information about customers is updated with credit reporting agencies when a customer's default is remedied. Carriers and CSPs have an obligation to keep customer's personal information accurate, complete and up to date.

6.4 Data Security (NPP 4)

6.4.1 Requirement

(a) NPP 4 requires an organisation to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.

(b) An organisation must destroy or permanently de-identify personal information it no longer requires.

6.4.2 Relevance

(a) Does the ACIF work refer to the retention, storage, archiving and disposal of personal information (including paper based and electronic records)?

(b) Does the ACIF work refer to the transmission of personal information across networks or in paper form?

(c) Does the ACIF work refer to practices that create a heightened risk concerning the security of personal information (such as those practices which may involve a greater level of disclosure of personal information)?

6.4.3 Examples:

(a) Commercial Churn Code

Carriers and CSPs have an obligation to retain TAFs for a period of two years. Carriers and CSPs must take reasonable steps to protect this personal information from unauthorised access, modification or disclosure. The personal information should be destroyed or de-identified when is it no longer required for any purpose.

(b) Complaint Handling Code

A customer's complaint needs to be recorded and maintained for two years. Carriers and CSPs must take reasonable steps to protect this personal information from unauthorised access, modification or disclosure. The Personal Information should be destroyed or de-identified when is it no longer required for any purpose.

Calling Number Display

Carriers and CSPs must ensure that customers who have an unlisted number carry a permanent line block unless the customer has requested permanent CND. Carriers and CSPs must take reasonable steps to protect this type of personal information from unauthorised access, modification or disclosure.

6.5 Openness (NPP 5)

6.5.1 Requirement

(a) NPP 5 requires an organisation to document and make available a policy about how it manages personal information.

(b) Organisations must tell an individual, if they ask, what personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6.5.2 Relevance

(a) Does the ACIF work impact on organisations having a Privacy

Policy? or

(b) Does the ACIF work impact on an organisations responsibility to advise individuals of their Privacy Policy?

Note: It would be reasonable to refer to your Privacy Policy when addressing a customer's privacy complaint.

6.6 Access and Correction (NPP 6)

6.6.1 Requirement

(a) NPP 6 requires an organisation to give an individual access to their Personal Information, except to the extent that:

(i) it would be unlawful to disclose the information or would prejudice a criminal investigation;

(ii) would mean disclosing information about another person;

(iii) the person is seeking the information for the purposes of legal proceedings and certain conditions prevail; or

(iv) providing access would reveal the intention of commercial negotiations and prejudice those negotiations.

(b) An organisation may charge for providing access to Personal Information, but the charges must not be excessive and must not apply to lodging a request for access.

(c) Any Personal Information that is inaccurate or out of date should be corrected at the request of the individual.

6.6.2 Relevance

(a) Does the ACIF work impact on an organisation providing individuals with the ability to access and correct their personal information?

6.6.3 Examples

(a) Credit Management

In the Credit Management code, carriers and CSPs have an obligation to provide customers with access to information concerning their credit history or credit standing. Customers must be able to access and correct such personal information as appropriate.

(b) Billing Code

The Billing Code says that carriers and CSPs must ensure that customers are able to obtain information relevant to their current bill. Customers must be able to access and correct such personal information as appropriate.

6.7 Identifiers (NPP 7)

6.7.1 Requirement

(a) An organisation must not adopt as its own identifier an identifier of the individual that has been assigned by a third party agency, including a contracted service provider for a Commonwealth contract (for example TFN or other assigned identifiers, such as a Medicare number).

(b) An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in unless necessary for the organisation to fulfil its obligations to the agency or is required.

6.7.2 Relevance

(a) Does the ACIF work refer to the use of identifiers to identify customers? or

(b) Does the ACIF work require organisations to use unique identifiers?

6.7.3 Example

(a) Mobile Number Portability Code

When porting customers, account numbers, mobile numbers and in the case of pre-paid customers, date of birth, are sent by the GCSP to the LCSP to identify and verify the customer wishing to port. Account numbers, mobile numbers and date of birth are not identifiers assigned by a third party agency. The telecommunications industry is allowed to use and disclose these identifiers when identifying and verifying our customers.

Note: Some organisations may use a verification process to identify customers when selling a service to them. This may involve the customer showing identification to the seller and may include, for example, a requirement to show identification such a Medicare card. This NPP still allows for a customer's identity to be verified by using , for example, their Medicare card. This NPP does not allow for the customer to be uniquely identified in customer service systems by that number.

6.8 Anonymity (NPP 8)

6.8.1 Requirement

(a) Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

6.8.2 Relevance

(a) Does the ACIF work require individuals to identify themselves?

6.8.3 Examples

(a) Public payphone users should have the option of not identifying themselves when they use the payphone. This may include providing a payment mechanism that does not require the disclosure of personal information (for example, allowing the user to pay by cash).

(b) Allowing individuals to make calls and enquiries to service providers (for example to obtain a quote or information about the price of services) without being required to provide their name and contact details.

6.9 Transborder data flows (NPP 9)

6.9.1 Requirement

(a) An organisation in Australia or an external Territory may only transfer Personal Information about an individual to a third party who is in a foreign country if:

(i) the recipient of the information is subject to similar privacy laws;

(ii) the individual consents to the transfer;

(iii) the transfer is necessary in respect of the contract with the individual; or

(iv) the recipient will securely hold the information in line with the NPPs.

6.9.2 Relevance

(a) Does the ACIF work refer to the transfer of personal information to a foreign country?

6.9.3 Examples

Transferring customer personal information to a related overseas company.

Note: the use and disclosure of personal information by related bodies corporate is acceptable where the use and disclosure is for the same purpose as the collection of the information. For example, if Company A collects a customer's personal information for the purpose of providing them with a telecommunications service, this information can be transferred to Company B if the transfer is required to provide the customer with the telecommunications service (perhaps in a bundled situation).

However if Company A collects a customer's personal information for the purpose of providing them with a telecommunications service, and Company A transfers this information to Company B for the purpose of direct marketing the customer, this transfer of information may require the advice of your company's Privacy Officer, Compliance Manager or Legal Counsel.

6.10 Sensitive information (NPP 10)

6.10.1 Requirement

(a) An organisation must not collect sensitive information about an individual unless:

(i) the individual has consented;

(ii) the collection is required by law; or

(iii) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, who is incapable of giving consent.

6.10.2 Relevance

(a) Does the ACIF work refer to or necessarily involve the collection of sensitive information. This can include information revealing a person's race, religion, ethnicity, trade union membership, health, disability or sexual orientation.

6.10.3 Example

(a) Information on customers who receive priority services; or

(b) Information provided by a customer for the provision of services and/or equipment to people with disabilities.

7. FURTHER INFORMATION

Privacy Act 1988 Cth, as amended by the *Privacy Amendment (Privacy Sector) Act 2000*

Telecommunications Act 1997, especially Part 13

Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles*, September 2001 (available at www.privacy.gov.au)

Organisation for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

Directive 97/66/ EC of the European Parliament and of the Council of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector

The United Kingdom *Telecommunications (Data Protection and Privacy) Regulations 1999/2093*

US-EU Agreement on Safe Harbor Privacy Principles for the Protection of Personal Data Transferred from the EU

New Zealand Privacy Commissioner*, Privacy on the Line: a Resource Document in relation to Privacy in Telecommunications, 10 July 2000*

8. REVIEW

8.1.1 Review of this Guideline will be conducted in line with any reviews of Federal privacy legislation.and consistent with the ACIF policy on review of its documents

ACIF is an industry owned, resourced and operated company established by the telecommunications industry in 1997 to implement and manage communication self-regulation within Australia.

ACIF's role is to develop and administer technical and operating arrangements to foster a thriving, effective communications industry serving the Australian community through

- the timely delivery of Standards, Codes and other documents to support competition and protect consumers;
- driving widespread compliance; and
- the provision of facilitation, coordination and implementation services to enable the cooperative resolution of strategic and operational industry issues.

ACIF comprises a Board, an Advisory Assembly, four standing Reference Panels, various task specific Working Committees, a number Industry Facilitation/Coordination Groups and a small Executive.

The ACIF Standards and Codes development process involves the ACIF Board, Reference Panels, Working Committees and the ACIF Executive. The roles and responsibilities of all these parties and the required operating processes and procedures are specified in the ACIF Operating Manual.

ACIF Standards, Codes and other documents are prepared by Working Committees made up of experts from industry, consumer, government and other bodies. The requirements or recommendations contained in ACIF published documents are a consensus of views of representative interests and also take into account comments received from other stakeholders.

Care should be taken to ensure that material used is from the current version of the Standard or Industry Code and that it is updated whenever the Standard or Code is amended or revised. The number and date of the Standard or Code should therefore be clearly identified. If in doubt please contact ACIF.

Published by:

THE AUSTRALIAN COMMUNICATIONS INDUSTRY FORUM LTD

Level 9, 32 Walker Street
North Sydney NSW 2060

Correspondence: PO Box 444
Milsons Point NSW 1565

Telephone: (02) 9959 9111
Facsimile: (02) 9954 6136

E-mail: acif@acif.org.au

Web Site: http://www.acif.org.au/