



ACIF G516:2004

AUSTRALIAN COMMUNICATIONS INDUSTRY FORUM

INDUSTRY GUIDELINE

**PARTICIPANT MONITORING OF VOICE
COMMUNICATIONS**

Industry Guideline– *Participant Monitoring of Voice Communications*

First published as ACIF G516:1998

ISBN: 1 74000 264 4

©Copyright Australian Communications Industry Forum
PO Box 444, Milsons Point NSW 1565

Disclaimers

1. Notwithstanding anything contained in this Industry 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 Industry Guideline;
 - (ii) inaccuracy or inappropriateness of this Industry Guideline; or
 - (iii) inconsistency of this Industry 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 Industry Guideline.
2. The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

© Australian Communications Industry Forum Limited 2004

This document is copyright and must not be used except as permitted below or under the *Copyright Act 1968*. You may reproduce and publish this document in whole or in part for your or your organisation's own personal or internal compliance, educational or non-commercial purposes. You must not alter or amend this document in any way. You must not reproduce or publish this document for commercial gain without the prior written consent of ACIF. Organisations wishing to reproduce or publish this document for commercial gain (i.e. for distribution to subscribers to an information service) may apply to subscribe to the *ACIF Publications Subscription Service* by contacting the ACIF Business Manager at acif@acif.org.au. If you publish any part of this document for any purpose, you must also publish this copyright notice as part of that publication.

PARTICIPANTS

The Working Committee responsible for the revisions made to this Industry Guideline consisted of the following organisations and their representatives:

Organisation	Membership	Representative
Attorney-General's Department	Non-Voting	Catherine Smith
Australian Communications Authority (ACA)	Non-Voting	Matthew O'Rourke
Australian Privacy Foundation	Voting	Nigel Waters
Australian Telecommunications Users Group (ATUG)	Voting	John Pack
Consumers' Telecommunications Network (CTN)	Voting	Teresa Corbin
Hutchison Telecommunications	Voting	Lindsay Alexander
MCI	Voting	Mary-Jane Salier
SingTel Optus	Voting	Rosie Rowe/Andrew Osborne
Telstra	Voting	Michael Pickering
Telstra	Non-Voting	Lydia Jones
Vodafone	Voting	Brian McDonnell

This Working Committee was chaired by Rosie Rowe for most of the life of the Committee and on an ad hoc basis thereafter. Holly Raiche of ACIF provided project management support.

**INDUSTRY
GUIDELINE**

TABLE OF CONTENTS

1	INTRODUCTION	1
2	SCOPE	3
3	ACRONYMS, DEFINITIONS AND INTERPRETATIONS	5
	3.1 Acronyms	5
	3.2 Definitions	5
4	REFERENCES	7
5	GENERAL PRINCIPLES	9
6	NOTIFICATION	11
	6.1 Notification Requirements	11
	6.2 Notification Methods	12
7	USE AND DISCLOSURE OF INFORMATION OBTAINED FROM PARTICIPANT MONITORING	15
8	DATA QUALITY, SECURITY AND ACCESS TO RECORDINGS	17
9	Employment issues	19
10	RELEVANT LEGISLATION	21
	10.1 Telecommunications Act 1997	21
	10.2 Privacy Act 1988	21
	10.3 Telecommunications (Interception) Act 1979	23
	Exceptions to the Interception Prohibition	23
	10.4 State and Territory Listening Devices legislation	24
	APPENDIX A: USEFUL CONTACTS	27
	APPENDIX B: PARTICIPANT MONITORING GUIDELINES FLOWCHART	31
	APPENDIX C: STATE AND TERRITORY LISTENING DEVICES LEGISLATION: USE OF LISTENING DEVICE BY PARTY TO COMMUNICATION	33
	APPENDIX D: STATE AND TERRITORY LISTENING DEVICES LEGISLATION: COMMUNICATION OR PUBLICATION OF INFORMATION OBTAINED BY USE OF A LISTENING DEVICE BY A PARTY TO THE COMMUNICATION	35

**INDUSTRY
GUIDELINE**

1 INTRODUCTION

- 1.1.1 The revision of this Guideline has been facilitated by the Australian Communications Industry Forum (ACIF) through a Working Committee comprised of representatives from the telecommunications industry, Government, regulatory agencies, privacy advocates and consumer groups.
- 1.1.2 This Guideline should be read together with ACIF G517:1998 *Monitoring of Communications for Network Operation and Maintenance* Industry Guideline.
- 1.1.3 This Guideline should be read in conjunction with related legislation, including:
- (a) the *Telecommunications (Interception) Act 1979*
 - (b) the *Telecommunications Act 1997*;
 - (c) the *Telecommunications (Consumer Protection and Service Standards) Act 1999*;
 - (d) the *Privacy Act 1988*; and
 - (e) State and Territory legislation on listening devices/surveillance.
- 1.1.4 This Guideline was first published in July 1998 by ACIF in response to requests by various user/customer groups to provide industry guidance in relation to listening and recording of communications under the interception legislation.
- 1.1.5 The Guideline has been reviewed following the amendments to the *Privacy Act 1988* and seeks to provide guidance on the practical application of interception and privacy legislation to the listening to and recording of Voice Communications. The Commonwealth Attorney-General's Department has provided input on the application of interception legislation.
- 1.1.6 The Guideline has been written in a form which can be utilised by both Carriers and Carriage Service Providers in the telecommunications industry and companies in other industries which may widely use telecommunications services and systems in their businesses, or which engage in telecommunications related activities (e.g. call centres).
- 1.1.7 It is intended that this Guideline assist both industry and consumers in their understanding of the application of relevant legislation.
- 1.1.8 In the future, ACIF intends to further review the Guideline to consider how relevant legislation applies to electronic non-Voice Communications as compared with Voice Communications. This will potentially result either in a revised version of this guideline or a separate document.

**INDUSTRY
GUIDELINE**

2 SCOPE

2.1.1 This Guideline covers both Monitoring of internal communications within organisations and Monitoring of external communications with customers or the general public. Monitoring includes listening to and/or recording a communication.

2.1.2 This Guideline only deals with Voice Communications.

Note: The TIA applies to all forms of telecommunications, not just Voice Communications.

2.1.3 This Guideline sets out:

- (a) general principles applicable to Participant Monitoring;
- (b) a discussion of the prohibition on intercepting Voice Communications passing over a Telecommunications System;
- (c) guidance on notification requirements and methods if Participant Monitoring takes place;
- (d) guidance on the use and storage of information obtained as a result of Participant Monitoring;
- (e) employment issues arising from Participant Monitoring; and
- (f) the application of relevant legislation.

2.1.4 This Guideline does not deal with:

- (a) Monitoring of electronic non-Voice Communications;
- (b) Monitoring by an employee of a telecommunications Carrier of a communication during the installation, operation or maintenance of a telecommunications network (which is addressed in a separate guideline, ACIF G517:1998 *Monitoring of Communications for Network Maintenance* Industry Guideline);
- (c) the interception of communications under telecommunications interception warrants;
- (d) the interception of communications by police in emergency circumstances;
- (e) the recording of emergency calls or maritime emergency frequencies;
- (f) interception undertaken for the detection and/or prevention of fraudulent use of a Carrier's or Carriage Service Provider's Telecommunications Network;
- (g) interception for the identification or tracing of any person who has contravened or is suspected of having contravened or being likely to contravene, the computer crimes provisions in Part VIIIB of the *Crimes Act 1914 (Cth)*;
- (h) AS/ACIF S002:2001 *Analogue interworking and non-interference requirements for Customer Equipment for connection to the Public Switched Telephone Network* Industry Standard which provides guidance for equipment used for listening to or recording Communications.

**INDUSTRY
GUIDELINE**

3 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

3.1 Acronyms

For the purposes of this Industry Code, the following acronyms apply:

ACA	Australian Communications Authority
ACCC	Australian Competition and Consumer Commission
ACIF	Australian Communications Industry Forum
NPPs	National Privacy Principles
TA	<i>Telecommunications Act 1997</i> (Cth)
TIA	<i>Telecommunications (Interception) Act 1979</i> (Cth)
TIO	Telecommunications Industry Ombudsman
PA	<i>Privacy Act 1988</i> (Cth)

3.2 Definitions

For the purposes of this Industry Code, the following definitions apply:

Carriage Service Provider

has the meaning given by section 87 of the TA.

Carrier

has the meaning given by section 7 of the TA.

Monitoring

means listening to and/ or recording communications

National Privacy Principles

means the Privacy Principles contained in Schedule 3 of the PA.

Participant Monitoring

means the Monitoring by one party to the Voice Communication of a person or organisation related to a party to the Voice Communication.

Personal Information

means information or an opinion that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

For the purposes of this Guideline, recordings of Voice Communications should be assumed to be Personal Information even in cases where no names are mentioned, as it will generally be possible to attribute a voice to at least one party from call charge and other records.

Premises

has the meaning given by section 5 of the TIA.

Telecommunications Network

has the meaning given by section 5 of the TIA.

Telecommunications Service

has the meaning given by section 5 of the TIA

Telecommunication System

has the meaning given by section 5 of the TIA.

Voice Communications

includes conversation and a message, and any part of a communication or message in the form of speech, music or other sounds.

4 REFERENCES

Relevant Commonwealth Legislation

Telecommunications Act 1997

Telecommunications (Consumer Protection and Service Standards) Act 1999

Telecommunications (Interception) Act 1979

Privacy Act 1988

Relevant State and Territory Legislation

Invasion of Privacy Act 1971 (Qld)

Listening Devices Act 1992 (ACT)

Listening Devices Act 1984 (NSW)

Listening Devices Act 1991 (Tas)

Listening and Surveillance Devices Act 1972 (SA)

Surveillance Devices Act 2000 (NT)

Surveillance Devices Act 1999 (Vic)

Surveillance Devices Act 1998 (WA)

**INDUSTRY
GUIDELINE**

5 GENERAL PRINCIPLES

- 5.1.1 The TIA prohibits listening to or recording a communication in its passage over a Telecommunications System without the knowledge of the parties to the communication.
- 5.1.2 The general rule under State and Territory legislation is that listening to or recording a 'private conversation' that is not being carried over a Telecommunications System without the consent of the parties is prohibited.
- 5.1.3 Privacy laws may also apply to Participant Monitoring. Many private sector organisations are required to comply with the NPPs in the PA, with Commonwealth and ACT public sector agencies having to comply with the Information Privacy Principles in that legislation. State and other Territory government agencies must comply with the information privacy principles in their relevant legislation, where this exists. These include principles requiring collection of Personal Information to be necessary for a legitimate purpose, notification when Personal Information is being collected, and principles limiting the use and disclosure of Personal Information.
- 5.1.4 In order to avoid contravening the prohibition against interception set out in the TIA, all parties to a telephone conversation must have actual knowledge that the conversation is being Monitored. The TIA does not require parties to a telephone conversation to consent to Monitoring activities.

See, however, Clause 10.2.3 for the collection of sensitive information

- 5.1.5 The TIA and State or Territory listening device legislation set out limited exceptions permitting Monitoring of Voice Communications without informing the parties to the Communication. Under the TIA, this can only occur with the authority of a warrant issued to assist in the investigation of serious criminal activities or matters of national security, and in certain other, strictly limited situations.
- 5.1.6 Recognising these general principles, the ACIF has developed this voluntary guideline for consideration.

6 NOTIFICATION

6.1 Notification Requirements

- 6.1.1 Except for the extremely limited exceptions referred to in Clause 6.1.4 below, all parties to a telephone conversation must have actual knowledge that the conversation will be Monitored in order to avoid contravening the prohibition against interception set out in the TIA.
- 6.1.2 Parties seeking to Monitor Voice Communications must inform the parties to the Voice Communication of these activities prior to them being undertaken. This requirement applies to third parties and employees where they are participants in a Voice Communication that is being Monitored. This requirement applies equally to inbound and outbound calling.
- 6.1.3 It should also be noted that the following do not affect whether the Monitoring is lawful:
- (a) whether or not a permanent record of the Voice Communication is made or stored;
 - (b) whether or not all parties to the Voice Communications actually speak;
 - (c) whether or not the parties to the Voice Communication are identified in the process of Monitoring;
 - (d) the use to which Voice Communications that have been listened to or recorded are put (including whether there is a perceived overall benefit to a party as a result of the use).

For example, the mere fact that listening is limited to the purpose of quality assurance will not remove the need for knowledge of the listening on the part of all parties to the Voice Communication.

- 6.1.4 The TIA provides for an exception to the prohibition against interception for Monitoring calls made to designated emergency services numbers (currently 000, 106 and 112). Monitoring calls from any other numbers, whether used for seeking assistance or raising an alarm or otherwise, are subject to this Guideline.
- 6.1.5 "Piptones" or "beeps" will not be a sufficient measure to convey to the individual the knowledge that the conversation is being Monitored.
- 6.1.6 It is recognised that there may be situations where actual knowledge may be imparted by methods other than an oral notification that attaches to a specific Voice Communication.
- 6.1.7 Where a genuine choice is offered, Monitoring should be discontinued as soon as the other party objects. However, where it is intended that Monitoring will take place whether or not the other party consents (and this satisfies National Privacy Principles 1.1 and 1.2) then Monitoring may only continue where the fact of Monitoring is expressly made clear. It will then be the other party's choice to continue with the Voice Communication.
- 6.1.8 NPP 10 provides for greater protection when an organisation collects sensitive information (including health information) about an individual. Generally, an organisation will require consent to collect such information, unless one of a limited set of circumstances apply. In most circumstances where sensitive information is collected in the course of monitoring, an organisation would need the consent of the individual before proceeding; it would not be sufficient to advise the individual that the call is to be recorded.

6.2 Notification Methods

Some examples of methods of imparting knowledge to the parties to Voice Communication of the fact that the Communication is being Monitored are set out below. All notification methods must be implemented prior to the Monitoring commencing. Where appropriate, suggested text is included after the scenarios. The notification methods are followed by scenarios in which those methods may apply.

6.2.1 Pre-recorded messages:

It would be appropriate to use pre-recorded messages in the following situations to alert callers to an organisation that the calls may be Monitored. In these scenarios, callers must be expressly advised that calls may or will be Monitored, as the case may be, in order to avoid contravening the prohibition against interception set out in the TIA.

Scenario 1: ABC Pty Ltd wishing to assess the performance of staff handling telephone calls from members of the public or to listen into calls for staff training and coaching purposes.

Scenario 2: XYZ Pty Ltd records a conversation between a customer service representative and a customer and then uses this as part of a training exercise to identify how company policy works in a particular situation or to identify areas of improvement for particular operators.

Suggested text: "Your call may be listened to and recorded for quality and coaching purposes. Please tell the consultant if you don't want this to happen."

Scenario 3: QRS Pty Ltd routinely records telephone calls with customers as part of their general business practice.

Suggested Text: "For security and quality purposes your call will be recorded."

6.2.2 Verbal Notification

Verbal notification of a caller or called party by an employee or other person using a standard script could be used as an alternative to a pre-recorded message (in scenarios 1 and 2 above). Such notification may also be an appropriate method in the following scenarios:

Scenario 4: ABC Pty Ltd phones customers asking them to take part in a survey and records the conversation to enable verification of the results of the survey.

Scenario 5: when medical, legal or financial advice is given to a particular caller, the call is Monitored and the caller has not otherwise been informed (through prior written notification or a pre-recorded message) that such calls are Monitored.

6.2.3 Written Notification

Written notification could include:

- a notice accompanying an advertised telephone number, advising that calls to the number will or may be Monitored;
- a prominent clause in a contract or notice in employee or customer collateral; or
- prominent signage in close proximity to a phone used to dial a specific number which is Monitored.

(a) Written notification to customers

NOTE: This is only appropriate for customers with an established and continuing relationship with the organisation and will only be sufficient

to impart knowledge in limited and very clear circumstances. To rely on written notification, organisations must ensure that the notification reaches all parties who may be Monitored.

Scenario 6: written notice is provided by a prominent clause in a contract or collateral of, for example, a stockbroker or financial advisor, advising that telephone Voice Communications to the company will or may be Monitored.

- (b) Written notification to employees

NOTE: This applies to employees. Where other non-employees are also parties to the Voice Communication, separate notification must be provided by one of the other methods to ensure that all parties are aware of the recording.

All employees must be expressly advised that calls may be Monitored in order to avoid contravening the prohibition on interception set out in the TIA through, for example, individual messages to employees, posters or prominent educational/reminder signage in the workplace, material provided during induction, as well as regular material at appropriate times. Written notification to employees may be an appropriate notification method in the following scenarios:

Scenario 7: notifying employees in call centres that they may be Monitored for training or quality assurance purposes.

Note: advice to such employees as to which specific calls will be Monitored is not ordinarily required.

Scenario 8: notifying employees in organisations such as financial or stock broking firms that calls are routinely Monitored for the protection of the organisation and could possibly be used in evidence of advice provided and/or received.

- (c) Written notice advising that calls to and from a phone which is used for a particular purpose will be Monitored.

Scenario 9: a prominent notice, stating that all calls on that particular telephone will be recorded, is located in near proximity to the telephone used for a particular purpose, eg, emergency calls

Note: It will still be necessary to ensure that the receiving party also has knowledge of the recording.

7 USE AND DISCLOSURE OF INFORMATION OBTAINED FROM PARTICIPANT MONITORING

- 7.1.1 The TIA prohibits, other than in strictly limited circumstances, the use of any information gained by way of intercepting communications passing over a Telecommunications Network. This prohibition does not apply if the communication has been Monitored with each party's knowledge as Monitoring in these circumstances will not amount to interception.
- 7.1.2 The TIA also regulates the use of lawfully intercepted material (eg under warrant or another exception to the prohibition). For further information on the TIA, see subsection 10.3.
- 7.1.3 The use and disclosure of any information obtained through Participant Monitoring activities may also be regulated under the TA. For further information on the TA, see subsection 10.1.
- 7.1.4 The PA also needs to be considered in relation to use and disclosure of information obtained from Participant Monitoring. Under NPP 2, organisations must not use or disclose Personal Information about an individual for a purpose other than the primary purpose of collection except in limited circumstances, including where the organisation has gained the consent of the individual. Where Participant Monitoring is undertaken, tapes and permanent records should only be used for the purpose for which they are recorded in the first place, or as otherwise authorized or required by law. For further information on the PA, see subsection 10.2.
- 7.1.5 Organisations should also ensure that individuals are not called back or otherwise intruded upon further unless such further contact is necessary on a case by case basis (e.g. if the party has been given the wrong information and it is important enough to warrant calling the individual back). Additional use of information recorded through Monitoring in this manner, may go beyond the purpose for which the information may properly be used.

8 DATA QUALITY, SECURITY AND ACCESS TO RECORDINGS

For more detailed description of relevant legislation, see section 10. That legislation generally provides as follows:

- 8.1.1 Organisations should take reasonable steps to ensure that recordings containing Personal Information are accurate, complete and up-to-date.
- 8.1.2 Records of Voice Communications should be stored in a secure place accessible only by authorised employees.
- 8.1.3 Instances of access to and use of recordings of Voice Communications or other recordings should be logged.
- 8.1.4 Records should be erased or destroyed once they are no longer required for any legitimate purpose or as authorized or required by law.
- 8.1.5 Organisations should provide access to those recordings that contain Personal Information about an individual, at that individual's request, subject to any relevant grounds for withholding such access, as specified in privacy laws. Organisations should develop their own policy guidelines on how they will provide such access.

9 EMPLOYMENT ISSUES

- 9.1.1 A number of employment issues may also arise in relation to the use of Participant Monitoring. Often these will occur where Participant Monitoring, which was not primarily intended to be used for the purpose of assessing employee's conduct, may in fact be put to this purpose. For example, where listening into a Voice Communication might reveal that an employee's skills are inadequate or that they have engaged in conduct outside the scope of their employment contract (e.g. undisclosed conflict of interest).
- 9.1.2 Problems that may arise in relation to the Monitoring include that recordings may be compiled in such a way as to give a distorted image of an employee's conduct. (see, by analogy, The Privacy Committee of New South Wales, *Invisible Eyes: Report on Video Surveillance in the Workplace*. (No 67 August 1995). Industrial relations law in relation to surveillance emphasises that detrimental action taken against employees on the basis of surveillance still needs to be fair and should not be based on irrelevant, inaccurate or incomplete facts. Courts will expect to see reasonable procedures: openness, and fair and timely action, and for employers to exercise caution in drawing conclusions about employees based on the content of Participant Monitoring (see *Byrne v Australian Airlines Limited* [1995] 185 CLR 410)
- 9.1.3 These guidelines are not intended to be a substitute for legal advice in relation to employment issues. However there are some key principles that should be followed in relation to the conduct of Participant Monitoring or use of Participant Monitoring records for employment related purposes. As outlined in section 6, there are some notification steps that organisations should take in relation to the Monitoring of employee Voice Communications, depending upon the purpose of the Monitoring. These are based on the following general principles:
- (a) employees should be informed that their conversation is or may be Monitored and of the purpose for which this is being carried out (e.g. training, or protection of lawful interests of the company). Advice as to which specific calls are being Monitored is not ordinarily required.
- Example: Disclosure in an employee training manual and company policy documents that listening to or recording of communications is performed routinely by the employer.*
- (b) employees should be fully informed of the processes adopted in the organisation for storage of and access to records obtained through Participant Monitoring.
- 9.1.4 Companies might also consider consulting with employees and developing a policy that deals with questions that employees might have about the possibility of Participant Monitoring being used for employment related purposes. Such a policy should be developed with both industrial relations and privacy considerations in mind.

Examples of the type of principle that might be included in such a policy include that if employment decisions such as a warning, or any form of disciplinary proceedings (including legal action), are to be made on the basis of a recorded Voice Communication, the recordings should be made available to the employee.

10 RELEVANT LEGISLATION

10.1 Telecommunications Act 1997

- 10.1.1 Participants in organisations that are a section of the telecommunications industry under section 110 of the TA (Carriers, Carriage Service Providers, telecommunications contractors and each of their employees) are regulated under the TA in relation to any information obtained through Participant Monitoring.
- 10.1.2 Part 13 of the TA provides general prohibitions on the use of telecommunications related information.
- 10.1.3 This legislation prohibits the use or disclosure of information that relates to the contents or substance of a communication or the affairs or personal particulars of another person and which comes to that person's knowledge in the course of their business and employment, apart from for authorised purposes. These authorised purposes include where the disclosure or use:
- (a) is in the course of the person's duties as an employee;
 - (b) is authorised under a warrant or by law;
 - (c) is made to ASIO, the ACA, the ACCC or the TIO;
 - (d) is as a witness summonsed to give evidence or produce documents;
 - (e) is reasonably necessary for the enforcement of the criminal law, the protection of public revenue or a law imposing a pecuniary penalty;
 - (f) has been consented to (either explicitly or implicitly) by the party it concerns;
 - (g) is believed by the person making it to be reasonably necessary to prevent or lessen a serious and immediate threat to the life or health of a person; or
 - (h) is provided to another Carrier or Carriage Service Provider in connection with the business of that Carrier or Carriage Service Provider.
- 10.1.4 The legislation also provides that records must be kept of disclosures and the purpose for which the information was disclosed, except in limited circumstances.

10.2 Privacy Act 1988

- 10.2.1 The PA applies to private sector organisations with an annual turnover of at least \$3 million, health service providers, organisations which trade in personal information and contractors to the Commonwealth. The PA contains 10 National Privacy Principles (NPPs) setting out how personal information is to be collected, used, disclosed and stored. Full information on the PA and NPPs can be found at <www.privacy.gov.au>. The following are the NPPs most relevant to Participant Monitoring.
- 10.2.2 NPP 1 – Collection, aims to limit the personal information that an organisation collects that is necessary for its functions and activities. This Principle states that collection must be fair and lawful and the organisation must take reasonable steps to inform individuals about the purposes of collection.
- 10.2.3 NPP 10 – (Collection and) Sensitive Information. Generally, when an organisation collects sensitive information (including health information) about an individual, it must have their consent to do so. There are some limited circumstances where consent is not required, including where the collection itself

is required by law, or where the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any person, and the individual (to whom the information relates) is physically or legally incapable of giving consent or physically cannot communicate their consent.

10.2.4 NPP 2 – Use and Disclosure, sets out the general rule that an organisation must only use or disclose Personal Information for the primary purpose of collection. Use and disclosure for a secondary purpose is not allowed except where it falls within one of the exceptions listed in NPP 2. These exceptions or permitted uses and disclosures include where:

- (a) the secondary purpose relates to the primary purpose of collection and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;
- (b) the individual has consented to the use or disclosure;
- (c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing and where, among other things, it is impracticable to seek the individual's consent and where the individual is told that they can opt out of receiving any more marketing from the organisation;
- (d) the information is health information and the use or disclosure is necessary for research or statistics relevant to public health or public safety and among other things, it is impracticable to seek the individual's consent;
- (e) there is a serious and imminent threat to an individual's life, health or safety; or public health/safety and is believed that the use or disclosure would reduce the threat;
- (f) there is a suspected unlawful activity and the use or disclosure is seen as a necessary part of an investigation or in reporting the matter;
- (g) the use or disclosure is required or authorised by or under law;
- (h) it is reasonably believed that the use or disclosure is reasonably necessary for a range of activities carried out by or on behalf of an enforcement body.

Note: For organisations which are subject to both the TA and the PA generally, the specific use and disclosure rules in Part 13 of the TA prevail over NPP 2, although they are mostly consistent and supportive.

10.2.5 Other NPPs, in particular NPP 4 and NPP 8, may need to be considered by organisations collecting Personal Information through Participant Monitoring. NPP 4 Security, requires an organisation to secure information against misuse, loss, unauthorised use, modification or disclosure and to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2.

10.2.6 NPP 8, Anonymity, provides that wherever lawful and practical, individuals must have the option of not identifying themselves when entering transactions with an organisation. This supports the general principle in these Guidelines that collection of Personal Information through Participant Monitoring must be necessary (see subsection 5.1.3)

10.2.7 Individuals who believe their privacy rights under the NPPs have been breached and the matter has not been adequately resolved, may complain to the Federal Privacy Commissioner.

10.3 Telecommunications (Interception) Act 1979

- 10.3.1 Monitoring a communication in its passage over a Telecommunications System by anyone without the knowledge of the parties to the communication is prohibited under the TIA, subject to limited exceptions.
- 10.3.2 It is critical to determine whether a communication is in its passage over a Telecommunications System for the purposes of this prohibition. Only in these circumstances will the TIA apply. In cases where a communications has ceased its passage over the Telecommunications System, State or Territory Listening Devices legislation may apply. The Courts have applied a technical test as to whether a communication is in its passage over a Telecommunications System or not for the purposes of assessing whether the TIA applies or not.
- 10.3.3 As a general principle, the Courts have drawn a distinction between the following situations:
- (a) listening to or recording using equipment which is electronically connected into or which intercepts signals transmitted by a Telecommunications System - TIA applies and State or Territory Listening Devices legislation does not. For this purpose, the Telecommunications System includes customer equipment attached to a Telecommunications Network; and
 - (b) the communication is listened to or recorded by equipment external to the Telecommunications System (such as a tape recorder) after the sounds have ceased passing over a Telecommunications System – State or Territory Listening Devices legislation applies.
- 10.3.4 By way of example, in the following cases the TIA applies and the State or Territory Listening Devices legislation has no application (see section 10.5 for further information. See also *Miller v Miller* (1978) 41CLR 269):
- (a) recording communications using a device connected to the Telecommunications System;
 - (b) intercepting radio signals from the mobile telephone network (see *Edelstein v Investigating Committee of NSW* (1986) 7 NSWLR 222);
 - (c) “double jacking” which is used widely in call centre and training centres. Double jacking is performed using equipment which enables a third party to Monitor a conversation by plugging in a headset which permits the conversation to be heard by the customer service representative and the trainer.
- 10.3.5 On the other hand, putting a person on speaker phone and then taping their communication by use of a tape recorder would fall outside the scope of the TIA and may be regulated by State or Territory Listening Devices legislation.

Exceptions to the Interception Prohibition

- 10.3.6 The TIA contains a limited number of exceptions to the general prohibition against interception. Most of these exceptions relate to law enforcement activities and emergency circumstances and are not the subject of these guidelines.
- 10.3.7 There are however two circumstances where Participant Monitoring does not amount to interception. The first is where the persons between whom communications are passing over a Telecommunications System have knowledge that the communication is being Monitored. If this knowledge exists, the TIA does not prohibit Monitoring the communication (as it is not an

interception under the TIA). It is this exception that underpins the notification requirements in section 6 above.

- 10.3.8 Secondly, subsection 6(2) of the TIA provides that Monitoring of a communication passing over a Telecommunications System is not prohibited where the person carrying out the Monitoring activity is lawfully on premises to which a Telecommunications Service is provided by a Carrier or a Carriage Service Provider using apparatus or equipment that is part of that Service.
- 10.3.9 The exception in subsection 6(2) of the TIA applies only rarely in the current, deregulated telecommunications market. The market currently consists of a large number of Carriers providing a variety of services to end-users who, in order to access those services, use a multiplicity of handsets and other “apparatus”. This end-user equipment is commonly not supplied by the Carrier in connection with the service, nor integral to the functioning of the service.
- 10.3.10 It should be noted that Courts have generally taken a narrow approach to the interpretation of statutes concerning individuals’ privacy and may adopt a narrow interpretation of subsection 6(2).
- 10.3.11 If reliance is to be placed on the provisions of subsection 6(2), organisations should obtain their own legal advice as to whether the activities proposed to be undertaken fall within the provision.

10.4 State and Territory Listening Devices legislation

- 10.4.1 Each of the States and Territories has its own listening devices legislation (see References section for list of relevant state and territory legislation). As discussed above, the listening devices legislation regulates Monitoring a private communication using a listening device.

Examples:

- (a) *where a listening device is placed in a room to listen to a private conversation between parties; or*
- (b) *where a recording device is placed against a speaker phone and which records the contents of a private communication.*

- 10.4.2 A private conversation for the purposes of the State and Territory legislation is a conversation that occurs in circumstances that indicate that a party or parties to the conversation desired it to be confined to the parties to the conversation (see *Miller v TCN Channel Nine* (1998) 36 A Crim R 92 (an open door does not cause a conversation to cease to be private))
- 10.4.3 Each State and Territory prohibits the use of a listening device to record a private conversation to which you are not a party. In some States and Territories, a party to the conversation who uses a listening device to record that conversation is not committing an offence. However, in all States and Territories, a party to the conversation is prohibited from communicating or publishing that record or a report of that conversation except in certain circumstances.
- 10.4.4 Appendices C and D set out:
- (a) the general prohibitions and exceptions applicable to a party to a conversation using a listening device to record that conversation; and
- (b) the prohibition and exceptions applicable to a party to a conversation communicating or publishing a record or report of that information.

10.4.5 Generally organisations that engage in Participant Monitoring within the constraints imposed by the prohibition in the TIA as set out earlier in these guidelines (eg Monitoring a communications in its passage over the Telecommunications System with the knowledge of all parties to the communication), do not need to consider the State and Territories Listening Devices legislation. However this information is provided so as to assist in the identification of when a matter will fall within the listening devices legislation.

APPENDIX A: USEFUL CONTACTS**State and Territory Government Departments responsible for listening devices laws****New South Wales**

Attorney-General's Department
GPO Box 6
SYDNEY NSW 2001
Ph: (02) 9228 7777

Victoria

Department of Justice
55 St Andrew's Place
MELBOURNE VIC 3000
Ph: (03) 9651 0728

Queensland

Attorney-General's Office
GPO Box 149
BRISBANE QLD 4001
Ph: (07) 3239 3478

South Australia

Attorney-General's Department
ING Building
GPO Box 464
ADELAIDE SA 5001
Ph: (08) 8207 1555

Western Australia

Department of Justice
141 Georges Terrace
PERTH WA 6000

Tasmania

Department of Justice and Industrial Relations
Level 14,
Trafalgar Building
110 Collins Street, HOBART TAS 7000
Ph: 1300 135 513

ACT

Department of Justice and Community Safety
Policy and Regulatory Division
GPO Box 158
CANBERRA ACT 2601
Ph: (02) 6207 0581

Northern Territory

Policy Division, Department of Justice
GPO Box 1722
DARWIN NT 0801
Ph: (08) 8999 7466

Federal Bodies

Federal agency responsible for the Telecommunications (Interception) Act 1979:

Attorney-General's Department
Robert Garran Offices
National Circuit
BARTON ACT 2600
Ph: (02) 6250 6666

Federal agencies responsible for the Privacy Act 1988

Attorney-General's Department	Office of the Federal Privacy Commissioner
Robert Garran Offices	GPO Box 5218
National Circuit	SYDNEY NSW 2001
BARTON ACT 2600	Ph 1300 363 992
Ph: (02) 6250 6666	

Australian Telecommunications Regulator (administers telecommunications regulatory arrangements under the Telecommunications Act 1997):

Australian Communications Authority

PO Box 13112 Law Courts

MELBOURNE VIC 8010

(Attn: Manager, Codes and Consumer Safeguards)

Ph: (03) 9963 6800

Telecommunications Industry Ombudsman

PO Box 276

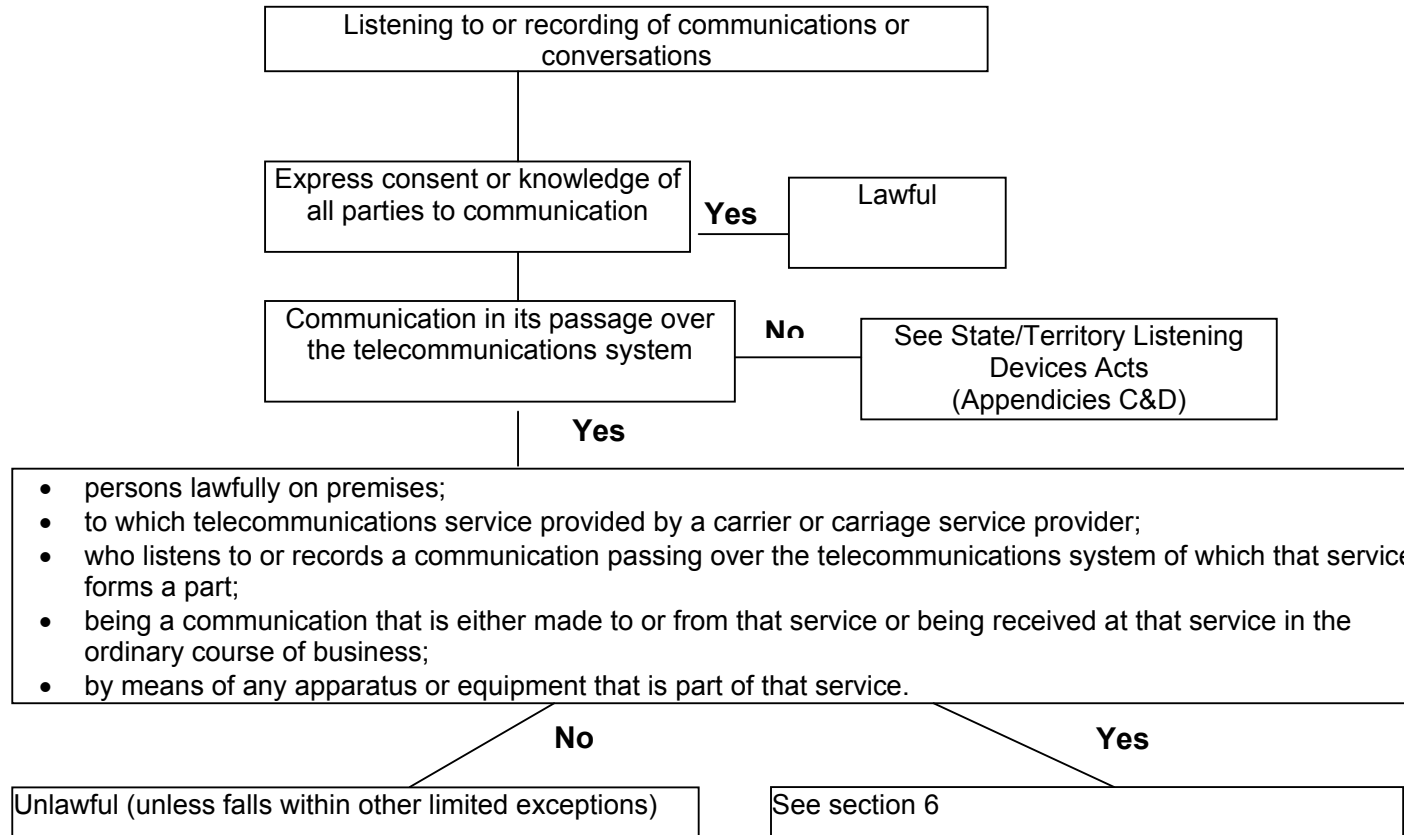
Collins Street West

MELBOURNE VIC 8007

Freecall: 1800 062 058

(The TIO scheme is established under the Telecommunications (Consumer protection and Service Standards) Act 1999 but the TIO is independent and industry funded.)

APPENDIX B: PARTICIPANT MONITORING GUIDELINES FLOWCHART



The information in this table is for guidance only and should not be regarded as a substitute for independent legal advice.

APPENDIX C: STATE AND TERRITORY LISTENING DEVICES LEGISLATION: USE OF LISTENING DEVICE BY PARTY TO COMMUNICATION

State/Territory	Prohibition on Party to Conversation using Device	Exception: Consent of all Parties	Exception: Do not intend to Communicate conversation to Non-Parties	Exception: To protect your lawful Interests	Exception: Course of Duty	Exception: Public Interest:
ACT	X	X	X	X		
VIC						
NSW	X	X	X	X		
QLD						
SA	X	X		X	X	X
WA						
TAS	X	X	X	X		
NT						

X = Prohibition or exception applies in that jurisdiction

The information in this table is for guidance only and should not be regarded as a substitute for independent legal advice.

**INDUSTRY
GUIDELINE**

APPENDIX D: STATE AND TERRITORY LISTENING DEVICES LEGISLATION: COMMUNICATION OR PUBLICATION OF INFORMATION OBTAINED BY USE OF A LISTENING DEVICE BY A PARTY TO THE COMMUNICATION

State/Territory	Prohibition on Party to Conversation Publishing Record/Report	Exception: To protect your lawful Interests	Exception: Course of Duty	Exception: Public Interest	Exception: In the course of Legal Proceedings	Exception: Disclosure to a party with interest in Conversation	Exception: All Other Parties' Consent	Exception: Disclosure to Other Party to Conversation
ACT	X	X			X	X	X	X
VIC	X	X	X	X	X		X	
NSW	X	X			X	X	X	X
QLD	X	X	X	X	X		X	X
SA	X	X	X	X				
WA	X	X	X	X	X		X	
TAS	X	X			X	X	X	X
NT	X	X	X	X	X			

X = Prohibition or exception applies

The information in this table is for guidance only and should not be regarded as a substitute for independent legal advice.

**INDUSTRY
GUIDELINE**

ACIF is an industry owned, resourced and operated company established to implement and manage communications 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;
- 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, standing Reference Panels, task specific Working Committees, Industry Facilitation/Coordination Groups, Consumer Advisory Bodies and a small Executive. Its members include carriers, carriage/content service providers, business and residential consumer groups, industry associations and individual companies.

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 applicable operating procedures are specified in the ACIF Operating Manual.

These procedures are based upon ACIF's openness, consensus, representation and consultation imperatives and have been designed to ensure that all sectors of Australian society are reasonably able to influence the development of Standards and Codes. Reference Panels and Working Committees must be representative of parties interested in the subject matter of the body of work being undertaken. All draft Codes/Standards are also released for public comment prior to publication to ensure outputs reflect the needs and concerns of all 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
TTY: (02) 9923 1911

E-mail: acif@acif.org.au

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