COMMUNICATIONS ALLIANCE LTD

INDUSTRY GUIDELINE

G516:2014

PARTICIPANT MONITORING OF VOICE COMMUNICATIONS

G516:2014 Participant Monitoring of Voice Communications

First published as ACIF G516:1998
Second edition as ACIF G516:2004
This edition as G516:2014

Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

Disclaimers

1) Notwithstanding anything contained in this Industry Guideline:

   a) Communications Alliance disclaims responsibility (including where Communications Alliance 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) Communications Alliance disclaims responsibility (including where Communications Alliance 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

INTRODUCTORY STATEMENT

The ***Participant Monitoring of Voice Communications*** Guideline (G516:2014) replaces the ***Participant Monitoring of Voice Communications*** Guideline (ACIF G516:2004).

The purpose of the changes are to:

- reflect amendments to the *Telecommunications (Interception and Access) Act 1979;*
- reflect amendments to the *Privacy Act 1988; and*
- update references to State and Territory listening devices/surveillance legislation.

The ***Participant Monitoring of Voice Communications*** Guideline is designed to:

- provide guidance on the practical application of interception and privacy legislation to the listening to and Recording of Voice Communications;
- be 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); and
- assist both industry and consumers in their understanding of the application of relevant legislation.

James Duck
Chair
Participant Monitoring Revision *Working Committee*

JUNE 2014

TABLE OF CONTENTS

1 GENERAL

1.1 Introduction

1.1.1 The development of the Guideline has been facilitated by Communications Alliance through a Working Committee comprised of representatives from the telecommunications industry, Government, privacy advocates and consumer groups.

1.1.2 The Guideline should be read in the context of other relevant codes, guidelines and documents including the ***Monitoring of Communications for Network Operation and Maintenance*** Industry Guideline (G517:2014).

1.1.3 The Guideline should be read in conjunction with related legislation, including:

(a) the *Telecommunications (Interception and Access) 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 Compliance with this Guideline does not guarantee compliance with any legislation. The Guideline is not a substitute for legal advice.

1.1.5 Statements in boxed text are a guide to interpretation only.

1.2 Scope

1.2.1 This Guideline covers Monitoring of:

(a) internal communications within Organisations; and

(b) external communications with customers or the general public.

1.2.2 This Guideline only deals with Voice Communications associated with organisational networks that have an ability to listen to, monitor or record the content of a Voice Communication in 'real time'.

1.2.3 This Guideline deals with:

(a) general principles applicable to Participant Monitoring;

(b) the legal restrictions and conditions 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.

1.2.4 This Guideline does not apply to:

(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, ***Monitoring of Communications for Network Maintenance*** Industry Guideline (G517:2014));

(c) the interception of communications under telecommunications interception warrants;

(d) the recording of emergency calls or maritime emergency frequencies;

(e) interception undertaken for the detection and/or prevention of fraudulent use of a Carrier's or Carriage Service Provider's Telecommunications Network;

(f) 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 10.6 of the *Criminal Code Act 1995 (Cth)*;

(g) the ***Analogue interworking and non-interference requirements for Customer Equipment for connection to the Public Switched Telephone Network*** Industry Standard (AS/CA S002:2010) which provides guidance for equipment used for listening to or recording Communications; or

(h) the monitoring of Communications between employees, which may be subject to separate workplace surveillance legislation.

1.3 Objectives

The objectives of the Guideline are to:

(a) provide guidance on the practical application of interception and privacy legislation to the listening to and Recording of Voice Communications.

(b) be 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); and

(c) assist both industry and consumers in their understanding of the application of relevant legislation.

1.4 Guideline review

The Guideline will be reviewed every 5 years, or earlier in the event of significant developments that affect the Guideline or a chapter within the Guideline.

2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 Acronyms

For the purposes of the Guideline:

APPs

means the Australian Privacy Principles.

TA

means the *Telecommunications Act 1997 (Cth)*.

TIAA

means the *Telecommunications (Interception and Access) Act 1979 (Cth)*.

PA

means the *Privacy Act 1988 (Cth)*.

2.2 Definitions

For the purposes of the Guideline:

Australian Privacy Principle

has the meaning given by Schedule 1 of the PA.

Carriage Service Provider

has the meaning given by section 87 of the TA.

Carrier

has the meaning given by section 7 of the TA.

Equipment

means apparatus or equipment used in connection with a Telecommunications Network.

Interception

has the meaning given by section 6 of the TIAA.

NOTE: This means the Listening to or Recording of a Voice Communications, by any means, during the course of its passage over a Telecommunications System, without knowledge of the parties to the communication.

Monitoring

means listening to and/or Recording of a Voice Communication in real-time.

Organisation

means either private or public entities.

Participant Monitoring

means the Monitoring of a Voice Communication by a party to the Voice Communication.

Personal Information

has the meaning given by the PA.

> *NOTE: 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.*

Recording

means the copying of all or part of the content of a Voice Communications on any medium.

Telecommunications Industry Ombudsman

means the Telecommunications Industry Ombudsman appointed under the Telecommunications Industry Ombudsman scheme.

Telecommunications Network

has the meaning given by section 5 of the TIAA.

> *NOTE:* **"Telecommunications Network"** *means a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or series of systems, for carrying communications solely by means of radiocommunication.*

Telecommunication System

has the meaning given by section 5 of the TIAA.

> *NOTE:* **"Telecommunications System"** *means:*
>
> *a telecommunications network that is within Australia; or*
>
> *a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia;*
>
> *and includes equipment, a line or other facility that is connected to such a network and is within Australia.*

Voice Communication

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

2.3 Interpretations

In the Guideline, unless the contrary appears:

(a) headings are for convenience only and do not affect interpretation;

(b) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(c) words in the singular includes the plural and vice versa;

(d) words importing persons include a body whether corporate, politic or otherwise;

(e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(f) mentioning anything after include, includes or including does not limit what else might be included;

(g) words and expressions which are not defined have the meanings given to them in the Act; and

(h) a reference to a person includes a reference to the person's executors, administrators, successors, agents, assignees and novatees.

3 GENERAL PRINCIPLES

3.1 General Principles

3.1.1 The TIAA prohibits listening to or Recording a communication in its passage over a Telecommunications System without the knowledge of the parties to the communication.

3.1.2 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.

3.1.3 Privacy laws may also apply to Participant Monitoring. Many private sector organisations and most Commonwealth and ACT public sector agencies are required to comply with the Australian Privacy Principles (APPs) in the PA. 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.

3.1.4 In order to avoid contravening the prohibition against interception set out in the TIAA, all parties to a telephone conversation must have actual knowledge that the conversation is being Monitored. The TIAA does not require parties to a telephone conversation to consent to Monitoring activities.

3.1.5 However, in combination, several of the Privacy Act obligations require that individuals generally be offered a choice as to whether a Voice Communication to which they are a party is Monitored. There will be exceptions; e.g. where Monitoring is required by law or can otherwise be justified as necessary.

NOTE: See Clause 8.2 and Appendix D for an explanation of the effect of the collection Principles in the PA.

3.1.6 The TIAA will apply to the listening to, or Recording of, a communication passing over the telecommunications system without the knowledge of the parties to the communication. Where the TIAA does not apply, State and Territory listening device legislation may apply.

NOTE: Refer to section 9 for a list of references to, and Appendix C for a table summarising, State and Territory listening device legislation, and to Appendix B for a flowchart on participant monitoring.

4 NOTIFICATION

4.1 Notification Requirements

4.1.1 Apart from limited exceptions (for example, calls made to designated emergency services numbers – currently 000, 106 and 112), all parties to a telephone communication must have actual knowledge that the communication will be Monitored in order to avoid contravening the prohibition against interception and accessing set out in the TIAA.

4.1.2 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.

4.1.3 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; and

(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).

NOTE: 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 parties to the Voice Communication.

4.1.4 "Piptones" or "beeps" will not be a sufficient measure to convey to the individual the knowledge that the conversation is being Monitored.

4.1.5 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.

NOTE: Refer to section 4.2 for more information on notification methods.

4.1.6 Where a choice is offered, Monitoring should be discontinued as soon as the other party objects.

4.1.7 Monitoring may continue where:

(a) the intent to Monitor the Voice Communication is expressly made clear;

(b) the Monitoring will satisfy Australian Privacy Principles 3, 4 and 5;

(c) it is intended that Monitoring will take place whether or not the other party consents; and

(d) the other party chooses to continue with the Voice Communication.

4.1.8 APP 3 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.

4.2 Notification Methods

4.2.1 The level of knowledge contemplated by s 6(1) of the TIAA is 'actual knowledge'. That is, the awareness of a person, as a matter of fact, that the Voice Communications to which they are a party is being or has been Monitored. The test of actual knowledge is subjective. Some examples have been formulated to provide practical guidance as to the type of circumstances which might indicate that a person has actual, subjective knowledge that a particular Voice Communication will be, or is being, Monitored.

4.2.2 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 example scenarios in which those methods may apply.

Pre-recorded messages

4.2.3 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 TIAA.

4.2.4 Pre-recorded messages may be an appropriate notification method in the following scenarios:

(a) Scenario 1: A Government department 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.

(b) 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."

(c) 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."

Verbal notification

4.2.5 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.

4.2.6 Verbal notification may be an appropriate method in the following scenarios:

(a) Scenario 4: ABC Pty Ltd phones customers asking them to take part in a survey and, with consent, records the conversation to enable verification of the results of the survey; and

(b) 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 (e.g. through a pre-recorded message) that such calls are Monitored.

Written notification to customers

4.2.7 Written notification to customers may be an appropriate notification method for customers with an established and continuing relationship with the Organisation and will only be sufficient to impart knowledge in limited circumstances. To rely on written notification, Organisations must ensure that the notification results in parties actually being aware that their voice communication is or may be Monitored.

Written notification to employees

4.2.8 All employees must be expressly advised that calls may be Monitored in order to avoid contravening the prohibition on interception and access set out in the TIAA through, for example, some combination of 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.

NOTE: Where 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 Monitoring.

4.2.9 Written notification to employees may be an appropriate notification method in the following scenarios:

(a) Scenario 7: giving employees in call centres knowledge 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 required.

(b) Scenario 8: giving employees in Organisations such as financial or stockbroking firms knowledge that calls are routinely Monitored for the protection of the Organisation and could possibly be used as evidence of advice provided and/or received.

4.2.10 Notification for dedicated telephones

Where a phone is used for a specific purpose, written notice may be used to ensure knowledge of users of that phone that calls may be Monitored.

4.2.11 Written notification may be an appropriate notification method in the following scenario:

(a) Scenario 9: a prominent notice, giving knowledge to users that all calls on that particular telephone, such as a direct helpline, will be Monitored, is located in close proximity to the telephone used for the particular purpose.

NOTE: It will still be necessary to ensure that the other party also has knowledge of the Monitoring.

5 USE AND DISCLOSURE OF INFORMATION OBTAINED FROM PARTICIPANT MONITORING

5.1 Use and disclosure

5.1.1 The prohibitions in the TIAA on the uses of information do not apply if the communication has been Monitored with each party's knowledge as Monitoring in these circumstances will not amount to interception.

5.1.2 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 Section 8.1.

5.1.3 The PA also needs to be considered in relation to use and disclosure of information obtained from Participant Monitoring. Under APP 6, 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 Clause 8.2.

6 DATA QUALITY, SECURITY AND ACCESS TO RECORDINGS

6.1 Data quality, security and access

6.1.1 For a more detailed description of relevant legislation, see section 8, and in particular section 8.2. That legislation generally provides as follows.

6.1.2 Organisations should take reasonable steps to ensure that recordings containing Personal Information are accurate, complete and up-to-date.

6.1.3 Records of Voice Communications should be stored in a secure place accessible only by authorised employees.

6.1.4 Instances of access to and use of recordings of Voice Communications or other recordings should be logged.

6.1.5 Records should be erased or destroyed once they are no longer required for any legitimate purpose or as authorized or required by law.

6.1.6 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.

7 EMPLOYMENT ISSUES

7.1 Employment Issues

7.1.1 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).

7.1.2 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. 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.

7.1.3 Employers should also be aware that there may be State legislation that applies to surveillance in the workplace.

7.1.4 Refer to section 4 for guidance on notification to employees.

7.1.5 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.

8 RELEVANT LEGISLATION

8.1 Telecommunications Act 1997

8.1.1 Any organisation or individual who falls under section 271 of the TA (e.g. Carriers, Carriage Service Providers, telecommunications contractors and each of their employees) is regulated by the TA in relation to any information obtained through Participant Monitoring.

8.1.2 Part 13 of the TA provides general prohibitions on the use of telecommunications related information.

8.1.3 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. Information that relates to the affairs of a person includes information about the location of a telephone handset or device. 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 the Australian Communications and Media Authority, the Australian Competition and Consumer Commission or the Telecommunications Industry Ombudsman;

(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.

8.1.4 The legislation also provides that records must be kept of disclosures and the purpose for which the information was disclosed, except in limited circumstances.

8.2 Privacy Act 1988

8.2.1 The PA applies to APP entities, including Commonwealth agencies and their contractors; private sector organisations with an annual turnover of at least $3 million or which trade in Personal Information, and health service providers. The PA contains 13 Australian Privacy Principles (APPs) setting out how Personal Information is to be collected, used, disclosed and stored. Full information on the PA and APPs can be found at www.oaic.gov.au. The following paragraphs explain the APPs most relevant to Participant Monitoring.

NOTE: the Australian Government decided in the 2014 Budget to disband the Office of the Australian Information Commissioner (OAIC) by 1 January 2015. The Privacy Act will continue to be administered by the Privacy Commissioner and supporting staff.

8.2.2 APP 2 and APP 3 deal with the collection of personal information. The particular elements of these APPs that are most relevant to Participant Monitoring include:

(a) APP 2 – this provides that wherever lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an Organisation;

(b) APP 3.2 – this limits the Personal Information that an APP entity collects for inclusion in a record - the information must be reasonably necessary;

(c) APP 3.3 – this requires an APP entity that solicits Sensitive Information (including health information) about an individual, generally to have their consent to do so (as well as meeting the test in APP 3.2); and

(d) APP 3.5 – this requires an APP entity to collect personal information only by 'lawful and fair means'.

NOTE: Refer to Appendix D for more information on these APPs.

8.2.3 In combination, these APPs require that individuals generally be offered a choice as to whether a Voice Communication to which they are a party is Monitored. There will be exceptions e.g. where Monitoring is required by law or can otherwise be justified as necessary.

8.2.4 APP 5 requires APP entities to have privacy collection statements in place when collecting personal information, a part of which is to stipulate the purpose for collection. In an operational sense this means that the messaging provided to callers, either through automated or scripted means, must contain reference to all of the intended uses of the collection. This is particularly important when the use may be beyond 'quality and training' purposes. The necessity of making all of the participants to the communication

aware of the monitoring will also ensure that the TIAA interception prohibition will not apply.

8.2.5 APP 6 sets out the general rule that an APP entity must only use or disclose Personal Information for the primary purpose for which it was collected. Use and disclosure for a secondary purpose is only allowed where it falls within a prescribed exception.

8.2.6 APP 7 regulates the use and disclosure of Personal Information for direct marketing. Any Organisation which is subject to the PA, and which intends to use Personal Information obtained through Participant Monitoring for direct marketing, will need to take account of this Principle, which addresses the issue of 'opting-out' as well as with APP 6 (see clause 8.2.5 above). Offering participants a choice of whether a voice communication is monitored in the first place may in some circumstances be a way of meeting obligations under APP 7.

NOTE: For Organisations which are subject to the TA, the TIAA and the PA, the specific use and disclosure rules in Part 13 of the TA and Chapter 4 of the TIAA apply in addition to APP 6 and APP 7, although they are mostly consistent and supportive.

8.2.7 Other APPs may need to be considered by Organisations collecting Personal Information through Participant Monitoring, if they are subject to the Privacy Act. The Security Principle, APP 11, requires an APP entity to secure information against misuse, interference and loss, as well as against unauthorised access, 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 the APPs. Once again, offering participants a choice of whether a voice communication is monitored in the first place may in some circumstances be a way of meeting obligations under APP 11.

8.2.8 Individuals have rights of access to and correction of Personal Information under the PA. This may include the right to obtain a copy of any recording, where such a copy is available, made in the course of Participant Monitoring. An organisation would not generally need to make a correction of any such recording requested by an individual unless there was evidence of it not being accurate, up-to-date, complete, relevant or not misleading.

8.2.9 Individuals who believe their rights under the Privacy Act have been breached, for instance by non-compliance with an APP, and who have been unable to adequately resolve the matter with an APP entity, may complain to the Office of the Australian Information Commissioner and any external dispute resolution schemes recognised under the PA.

NOTE: For more information on external dispute resolution schemes recognised under the PA, including the TIO, refer to

http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-registers/recognised-edr-schemes.

8.3 Telecommunications (Interception and Access) Act 1979

8.3.1 Intercepting a communication in its passage over a Telecommunications System by anyone without the knowledge of the parties to the communication is prohibited under the TIAA, subject to limited exceptions.

8.3.2 In cases where a communication is not passing over a Telecommunications System, State or Territory listening devices legislation may still 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 or not the TIAA applies.

8.3.3 As a general proposition, the TIAA is likely to apply to the listening to or Recording of a Communication using a device or other equipment which is electronically connected into or which intercepts signals transmitted by a Telecommunications System. For this purpose, the Telecommunications System includes customer equipment attached to a Telecommunications Network. For example, "double jacking" which is used widely in call centres 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 between the customer service representative and the other party to be heard by the trainer.

8.3.4 Situations where State or Territory surveillance legislation may apply, to the exclusion of the TIAA, include where the communication is listened to or recorded by equipment external to the Telecommunications System after the sounds have ceased passing over a Telecommunications System. For example, putting a person on speaker phone and then Recording their communication would fall outside the scope of the TIAA and may be regulated by State or Territory listening devices legislation.

Exceptions to the Interception Prohibitions

8.3.5 The TIAA 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 the Guideline.

8.3.6 Notably Participant Monitoring does not amount to interception where the persons between whom communications are passing over a Telecommunications System have actual knowledge that the communication is being Monitored. It is this exception that underpins the notification requirements in section 4 above.

8.4 State and Territory Surveillance Devices legislation

8.4.1 Each of the States and Territories has its own listening devices legislation (see the References in section 9 for a list of relevant State and Territory legislation). As discussed above, the listening devices legislation regulates Monitoring a private communication using a listening device.

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

8.4.2 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.

8.4.3 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. This does not include a conversation made in circumstances in which the parties to it ought reasonably to expect that it might be overheard by someone else (see *Miller v TCN Channel Nine* (1988) 36 A Crim R 92 (an open door does not cause a conversation to cease to be private)).

8.4.4 Appendix C sets 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.

9 REFERENCES

Publication	Title
Industry Documents	
AS/CA S002:2010	Analogue interworking and non-interference requirements for Customer Equipment for connection to the Public Switched Telephone Network
Industry Guidelines	
G517:2014	Monitoring of Voice Communications for Network Operation And Maintenance
Commonwealth Legislation	
Criminal Code Act 1995	
http://www.comlaw.gov.au/Series/C2004A04868	
Privacy Act 1988	
http://www.comlaw.gov.au/Series/C2004A03712	
Telecommunications Act 1997	
http://www.comlaw.gov.au/Series/C2004A05145	
Telecommunications (Consumer Protection and Service Standards) Act 1999	
http://www.comlaw.gov.au/Series/C2004A00441	
Telecommunications (Interception and Access) Act 1979	
http://www.comlaw.gov.au/Series/C2004A02124	
State and Territory Legislation	
Invasion of Privacy Act 1971 (Qld)	
https://www.legislation.qld.gov.au/Acts_SLs/Acts_SL_I.htm	
Listening Devices Act 1991 (Tas)	
http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_id=21%2B%2B1991%2BAT%40EN%2B20130920130000;histon=;prompt=;rec=;term=	
Listening Devices Act 1992 (ACT)	
http://www.legislation.act.gov.au/a/1992-57/default.asp	
Listening and Surveillance Devices Act 1972 (SA)	
http://www.legislation.sa.gov.au/LZ/C/A/LISTENING%20AND%20SURVEILLANCE%20DEVICES%20ACT%201972.aspx	

Surveillance Devices Act 2007 (NSW) *http://www.legislation.nsw.gov.au/maintop/view/inforce/act+64+2007+cd+0+N*
Surveillance Devices Act 2007 (NT) *http://notes.nt.gov.au/dcm/legislat/legislat.nsf/d989974724db65b1482561cf0017cbd2/8f10699f7342fa996925784d0004c466?OpenDocument*
Surveillance Devices Act 1999 (Vic) *http://www.legislation.vic.gov.au/*
Surveillance Devices Act 1998 (WA) *http://www.slp.wa.gov.au/legislation/statutes.nsf/main_mrtitle_946_homepage.html*
Workplace Surveillance Act 1995 (NSW) *http://www.legislation.nsw.gov.au/maintop/view/inforce/act+47+2005+cd+0+N*

APPENDIX

A USEFUL CONTACTS

A1 State and Territory departments responsible for listening devices laws

TABLE 1

State and Territory departments responsible for listening devices laws

State / Territory	Department / Directorate	Website
ACT	Justice and Community Safety Directorate	http://www.justice.act.gov.au/
NSW	Department of Attorney General and Justice	http://www.lawlink.nsw.gov.au/
NT	Department of the Attorney-General and Justice	www.nt.gov.au/justice/
Qld	Department of Justice and Attorney-General	http://www.justice.qld.gov.au/
SA	Attorney-General's Department	http://www.agd.sa.gov.au/
Tas	Department of Justice	http://www.justice.tas.gov.au/
Vic	Department of Justice	http://www.justice.vic.gov.au/
WA	Department of the Attorney General	http://www.dotag.wa.gov.au/

A2 Federal Bodies

TABLE 2

Federal Organisations responsible for legislation and regulation

Responsible for	Organisation	Website
Telecommunications (Interception and Access) Act 1979	Attorney-General's Department	http://www.ag.gov.au/
Privacy Act 1988	Attorney-General's Department	http://www.ag.gov.au/
Privacy Act 1988	Office of the Australian Information Commissioner	http://oaic.gov.au/
Telecommunications regulatory arrangements under the Telecommunications Act 1997	Australian Communications and Media Authority	http://www.acma.gov.au/

NOTE: the Australian Government decided in the 2014 Budget to disband the Office of the Australian Information Commissioner (OAIC) by 1 January 2015. The Privacy Act will continue to be administered by the Privacy Commissioner and supporting staff.

A3 Other

TABLE 3

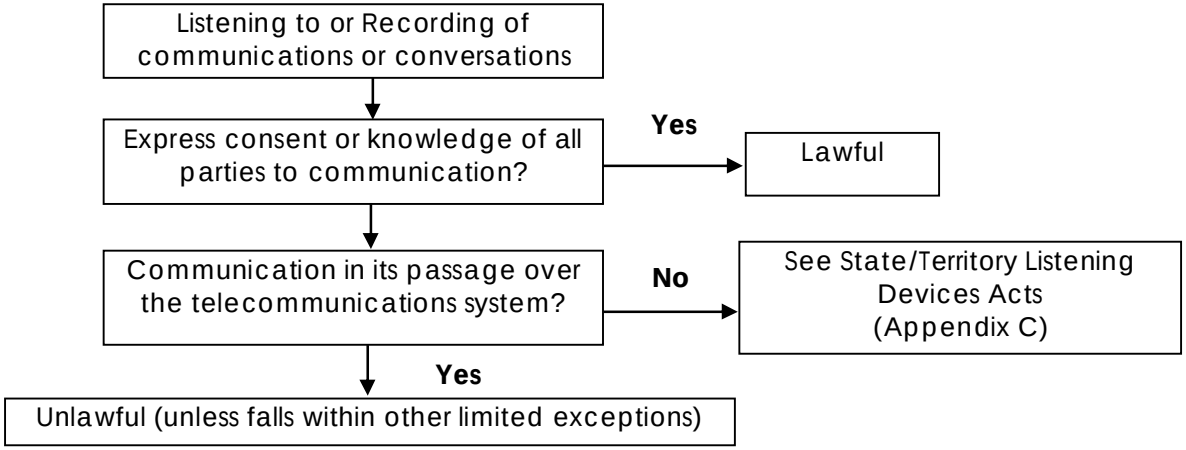
The Telecommunications Industry Ombudsman

Responsible for	Organisation	Website
TIO Scheme	Telecommunications Industry Ombudsman	http://www.tio.com.au/

NOTE: 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



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

FIGURE 1

Participant Monitoring Guidelines Flowchart

APPENDIX

C STATE AND TERRITORY LISTENING DEVICES LEGISLATION

C1 Use Of Listening Device By Party To Communication

Refer to Table 2 for a categorisation of Sate and Territory legislation on legislation on the use of listening devices.

In Table 2, X = Prohibition or exception applies in that jurisdiction

The information in Table 2 is for guidance only and should not be regarded as a substitute for independent legal advice.

TABLE 4

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	X	X	X	X	X	X
NT						

C2 Communication or Publication of Information Obtained by Use of a Listening Device by a Party to Communication

Refer to Table 3 for a categorisation of Sate and Territory legislation on communication or publication of information obtained by use of a listening device by a party to communication.

In Table 3, X = Prohibition or exception applies in that jurisdiction

The information in Table 3 is for guidance only and should not be regarded as a substitute for independent legal advice.

TABLE 5

State and Territory Listening Devices Legislation: Communication or Publication of Information Obtained by Use of a Listening Device by a Party to Communication

State / Territory	Prohibition on Party to Conversation Communicating 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
Qld	X	X	X	X	X	X	X	X
SA	X	X	X	X				
WA	X	X	X	X	X	X	X	X
Tas	X	X			X	X	X	X
NT	X	X	X	X	X		X	

APPENDIX

D AUSTRALIAN PRIVACY PRINCIPLES DEALING WITH THE COLLECTION OF PERSONAL INFORMATION RELEVANT TO MONITORING

D1 Anonymity and Pseudonymity (APP 2)

APP 2 provides that wherever lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an Organisation. This supports the obligation under APP 3 that collection of Personal Information is reasonably necessary – see below. Individuals will commonly identify themselves in voice communications – even where it is not strictly necessary for the purposes of the transaction (e.g. common courtesy in customer service). In addition to offering individuals a choice as to whether to identify themselves or not, it can be argued that offering them a choice as to whether the communication is monitored is a reasonable way of meeting the spirit, or underlying objective, of APP 2 – by at least giving them an option that their identity is not revealed to a third party (in the case of real time listening) or, more significantly, recorded.

D2 Collection of Solicited Personal Information – reasonably necessary for one or more of the entity's functions or activities (APP 3.2)

APP 3.2 limits the Personal Information that an AAP entity collects for inclusion in a record. It will therefore apply to Recording but not to real-time listening. Information solicited by an APP entity must be reasonably necessary for one or more of its functions or activities, or, where the collection is by a Commonwealth agency, directly related to one or more of its functions or activities. 'Reasonable necessity' is an objective test, and it will not be met merely because an Organisation wishes to collect information to satisfy a particular business model. In justifying collection of personal information through routine monitoring of all voice communications, without offering individuals a choice, an Organisation would have to explain why it was necessary for them if similar Organisations in similar circumstances felt able to give individuals a choice. One factor suggested as relevant in the OAIC APP Guidelines is 'whether the entity could undertake the function or activity without collecting that personal information'.

D3 Sensitive Information (APP 3.3)

Where an APP entity solicits Sensitive Information (including health information) about an individual, it must generally have their consent to do so (as well as meeting the test in APP 3.2). There are some limited circumstances where consent is not required, but these will not generally be applicable to monitoring of voice communications. Given that it will not generally be possible to know in advance if monitoring of voice communications will include sensitive information, it would be prudent for Organisations to assume that a least some Sensitive Information will be collected. In order to rely on implied consent, individuals whose communications are monitored must have been given a choice (unless one of the exceptions to consent applies, such as a legal obligation to record.

D4 Collection of Solicited Personal Information – by lawful and fair means (APP 3.5)

Under APP 3.5 an APP entity must collect personal information only by 'lawful and fair means'. The OAIC APP Guidelines suggest that 'A fair means of collection is one that is ... not unreasonably intrusive'. It may be that Recording voice communications without offering individuals a choice, where it is not 'reasonably necessary' would also be considered 'unfair'.

PARTICIPANTS

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

Organisation	Membership	Representative
AAPT	Voting	George Dionisopoulos
ACCAN	Voting	Jonathan Gadir
Attorney-General's Department	Non-voting	Catherine Smith
Attorney-General's Department	Non-voting	Kathryn Ovington
Attorney-General's Department	Non-voting	Sonia Harris
Australian Privacy Foundation	Voting	Nigel Waters
NBN Co	Voting	Peter Bull
Optus	Voting	David Bolton
Telstra	Voting	Dan Mandaru

This Working Committee was chaired by James Duck of Communications Alliance who also provided project management support.

Communications Alliance was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507