Commercial notes

Number 20 | 19 September 2006

Recent developments in telecommunications interception and access law

This note discusses the amendments to the *Telecommunications (Interception) Act 1979* (Cth) (the TI Act) introduced by the *Telecommunications (Interception) Amendment Act 2006* (Cth) (the Amending Act). It also analyses the new telecommunications interception and access regime and its implications for employers and network administrators.

Adelaide

Andrew Schatz *Senior Lawyer*
T *08 8205 4201* ***F*** *08 8205 4499*
andrew.schatz@ags.gov.au

Parliament's primary concern in passing the Amending Act was to strike the right balance between empowering law enforcement agencies and protecting the privacy of personal communications during their passage over telecommunications systems.[1] According to the Explanatory Memorandum to the Amending Act (the EM), the telecommunications interception regime is intended to protect the privacy of personal communications by generally prohibiting the interception of communications, subject to certain limited exceptions where privacy is outweighed by other considerations.[2] Australian courts have also referred to this privacy objective on a number of occasions.[3]

The Amending Act amends the TI Act to implement certain recommendations of the *Report of the Review of the Regulation of Access to Communications* prepared by Anthony Blunn AO (the Blunn Report). Mr Blunn was asked to review policy options for the regulation of access to telecommunications, with a particular emphasis on new and emerging telecommunications technologies. The resulting report, which is the fifth major report dealing with telecommunications interception legislation since 1994, was presented to Parliament on 14 September 2005.

It is also worth noting by way of introduction that the name of the TI Act changed to the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) on 13 June 2006. The new title better reflects the fact that while the TIA Act continues to govern the interception of telecommunications in Australia, it also establishes a warrant regime for enforcement agencies to access 'stored communications' held by telecommunications carriers.[4]

The telecommunications interception regime is intended to protect the privacy of personal communications by generally prohibiting the interception of communications.

The principal amendments

The principal amendments introduced by the Amending Act:

— establish a regime to govern access to 'stored communications' held by telecommunications carriers (Schedule 1) (the Stored Communications Amendments)

— enable the interception of communications of persons known to communicate with a 'person of interest' in certain limited circumstances (Schedule 2)

— enable interception of telecommunications services on the basis of the use of a telecommunications device in certain limited circumstances (Schedule 3)

— remove the distinction between class 1 and class 2 offences for which telecommunications interception powers are conferred on law enforcement agencies (Schedule 4)

— remove the Telecommunications Interception Remote Authority Connection function currently exercised by the Australian Federal Police and transfer the associated warrant register function to the Commonwealth Attorney-General's Department (Schedule 5).

This note focuses on the Stored Communications Amendments (Schedule 1), which commenced on 13 June 2006. The Stored Communications Amendments are of particular relevance to employers and network administrators who are responsible for operating and maintaining computer networks with Internet and email facilities. This is because accessing, monitoring and/or recording email and Internet communications are an essential part of many filtering, quarantining, archiving, disaster recovery and professional standards related practices.[5] Accordingly, any laws restricting the extent to which communications can be accessed or recorded are likely to have an impact on the capacity of employers and network administrators to maintain and protect their computer networks against damage or misuse.

The new meaning of the term 'stored communications'

The Stored Communications Amendments are intended to preserve the distinction between accessing stored communications and intercepting real-time communications as recommended in the Blunn Report (see the EM at p. 4). However, the previous definition of stored communications inserted at s 7(3A) of the TI Act by the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth) (the Stored Communications Act)[6] has been replaced by the following definition (at s 5(1) of the TIA Act):

> ***stored communication*** means a communication that:
>
> (a) is not passing over a telecommunications system; and
>
> (b) is held on equipment that is operated by, and is in the possession of, a carrier; and
>
> (c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

Accordingly, the term 'stored communications' no longer applies to all communications stored in any form other than on a 'highly transitory basis' and the new prohibition on 'accessing stored communications' only applies to communications that are accessed via a telecommunications carrier. According to the EM (at pp. 4–5), this limitation expressly recognises the ability of enforcement agencies to continue using lawful access arrangements to access communications stored on devices that are accessible without the assistance of a telecommunications carrier (e.g. through production by consent, a search warrant or a notice to produce).

The EM (at p. 6) and the Supplementary Explanatory Memorandum (the Supplementary EM – at p. 3) summarise the application of the new telecommunications interception and access regime as follows:

— communications that are 'passing over a telecommunications system' remain subject to the general prohibition on interception (s 7 of the TIA Act)

— communications that are 'stored communications' are subject to the new prohibition on accessing stored communications (s 108 of the TIA Act)

'Stored communications' no longer applies to all communications stored in any form other than on a 'highly transitory basis' and the new general prohibition on 'accessing stored communications' only applies to communications that are accessed via a telecommunications carrier.

— communications that are not passing over a telecommunications system and are not 'stored communications' (because they are not accessed via a telecommunications carrier) remain subject to general principles of lawful access including consent, general search warrants and notices to produce.

There is no specific reference in the EM, the Supplementary EM or the second reading speech to the ability of employers or network administrators to access communications held on equipment they possess and operate. However, by implication, the new provisions of the TIA Act permit employers and network administrators to lawfully access and record communications held on equipment they possess and operate at any time except when the communications are 'passing over a telecommunications system'.

The new 'stored communications warrant' regime

Chapter 3 of the TIA Act establishes the general prohibition on accessing 'stored communications' subject to certain limited exceptions. Section 108(1) of the TIA Act states that a person commits an offence (punishable by a penalty including imprisonment up to 2 years) if:

(a) the person:

  (i) accesses a stored communication; or

  (ii) authorises, suffers or permits another person to access a stored communication; or

  (iii) does any act or thing that will enable the person or another person to access a stored communication; and

(b) the person does so with the knowledge of neither of the following:

  (i) the intended recipient of the stored communication;

  (ii) the person who sent the stored communication.

By implication, the new provisions of the TIA Act permit employers and network administrators to lawfully access and record communications held on equipment they possess and operate at any time except when the communications are 'passing over a telecommunications system'.

However, s 108(2) of the TIA Act provides, among other things, that s 108(1) does not apply to:

(a) accessing a stored communication under a stored communications warrant; or

(b) accessing a stored communication under an interception warrant.

A number of concerns were raised about the new stored communications warrant regime during the relevant Parliamentary debates and Senate Committee consideration, including the lower threshold for, and broader access to, stored communications warrants compared to telecommunications interception warrants.[7] However, the government responded by emphasising the higher threshold for stored communications warrants compared to standard search warrants, as well as the additional record keeping and reporting requirements introduced to promote accountability.[8]

The difference between 'accessing' and 'intercepting'

Section 6AA of the TIA Act defines the term 'accessing a stored communication' to mean:

> ... listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.

By comparison, s 6(1) of the TIA Act retains the following TI Act definition of 'intercepting a communication passing over a telecommunications system':

> ... listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

While the new definition of 'accessing a stored communication' includes 'reading', the unchanged definition of 'intercepting a communication passing over a telecommunications system' does not. However, the distinction may be of little consequence given the impracticality of reading a communication passing over a telecommunications system without creating a copy.[9]

It is also worth noting that the two definitions differ in terms of whose knowledge matters for the purpose of determining whether or not the interception or accessing is unlawful. Section 108(1)(b) of the TIA Act only prohibits accessing a stored communication with '... the knowledge of neither of the following':

(i) the intended recipient of the stored communication;

(ii) the person who sent the stored communication.

Accordingly, s 108(1)(b) permits lawful access to stored communications without a warrant provided the sender, or the intended recipient, or both of those parties, know in advance that the stored communications will be accessed.[10] However, Parliament did not equally limit the general prohibition on interception of communications, and notification of the person making the communication is required to avoid unlawful interception. This may continue to prove problematic given the impracticality of notifying all potential senders of communications in advance that their communications may be intercepted while in transit.[11]

The new concept of 'passing over a telecommunications system'

The Stored Communications Amendments are intended to clarify when a communication is 'passing over a telecommunications system' principally for the purposes of the prohibition on intercepting such communications in s 7.[12] To that end, s 5F(1) of the TIA Act states that a communication:

(a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and

(b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.

The Stored Communications Amendments are intended to clarify when a communication is 'passing over a telecommunications system'.

However, s 5F(2) alters the position with respect to communications sent from addresses on computer networks operated by or on behalf of the Australian Federal Police (the AFP) for a period of two years from 13 June 2006. Such communications are not taken to start passing over a telecommunications system for the purposes of the TIA Act until they are no longer under the control of any of the following:

(a) any AFP employee responsible for operating, protecting and maintaining the network;

(b) any AFP employee responsible for enforcement of the Professional Standards of the Australian Federal Police.

The references to 'operating, protecting and maintaining the network' and 'enforcement of the Professional Standards of the Australian Federal Police' recognise the operational difficulties that could arise if the AFP and its network administrators were unable to lawfully access (or intercept) a communication sent from a telecommunications device within an AFP computer network before the relevant communication reached its network boundary (the gateway). In fact, the Supplementary EM states (at p. 3) that the insertion of s 5F(2):

> ... will enable lawful access to those communications for the AFP within the AFP network boundary.

However, while the AFP has been given the right to lawfully access and record outgoing communications at or prior to its gateway for operational, security, maintenance and professional standards purposes, a similar right has not been extended to employers and network administrators more generally. Accordingly, all organisations should review their network administration policies and practices to ensure they do not authorise or engage in behaviour that is unlawful under the new telecommunications interception and access regime.

In particular, if there is a need to access or copy outgoing communications at or prior to a gateway, then organisations should ensure their employees and other network users are adequately informed in advance. Carefully drafted and promulgated policy documents will help, but regular reinforcement through online screen prompts and user training sessions may also be required.[13]

If there is a need to access or copy outgoing communications at or prior to a gateway, then organisations should ensure their employees and other network users are adequately informed in advance.

Determining when a communication is 'accessible to its intended recipient'

It is necessary to consider when a particular communication becomes 'accessible to its intended recipient' to determine whether it is 'passing over a telecommunications system'. To that end, s 5H(1) provides that a communication is accessible to its intended recipient if it:

(a) has been received by the telecommunications service provided to the intended recipient; or

(b) is under the control of the intended recipient; or

(c) has been delivered to the telecommunications service provided to the intended recipient.

The application of s 5H(1) is fairly straightforward with respect to clearly defined telecommunications services provided by carriers such as home dial-up Internet and email services. However, the position is more complicated with respect to communications sent to intended recipients at electronic addresses on corporate computer networks (e.g. the work email address of an employee of a business or government agency).

On one view of the matter, the 'telecommunications service' provided in such a case could constitute the entire network that enables the intended recipient to access communications passing over external telecommunications systems operated by telecommunications carriers (i.e. all lines and equipment comprising the telecommunications network from the gateway to the relevant telecommunications device used by the intended recipient). On this view, all incoming communications would cease passing over the relevant telecommunications system at the gateway of the relevant destination network. Accordingly, the communications would no longer be subject to the general interception prohibition and the organisation or administrator responsible for operating the network could lawfully access and record the incoming communications at the gateway.

However, it is possible that a court may consider that allowing organisations to intercept communications at the gateway to a computer network would contravene the privacy objectives of the TIA Act,[14] particularly in view of the provisions set out in s 5G (as discussed directly below).

However, it is possible that a court may consider that allowing organisations to intercept communications at the gateway to a computer network would contravene the privacy objectives of the TIA Act.

Identifying the 'intended recipient' of a communication

Section 5G(1) of the TIA Act defines the term 'intended recipient' as follows:

(a) if the communication is addressed to an individual (either in the individual's own capacity or in the capacity of an employee or agent of another person)—the individual; or

(b) if the communication is addressed to a person who is not an individual—the person; or

(c) if the communication is not addressed to a person—the person who has, or whose employee or agent has, control over the telecommunications service to which the communication is sent.

Accordingly, in the case of a communication sent to the electronic address of an employee or other user on a corporate network, the TIA Act provides that the communication continues to pass over the telecommunications system until it becomes 'accessible to' the individual user to whom the relevant communication is addressed (see the EM at p. 6).

In addition, s 5G(2) of the TIA Act was inserted to provide a specific definition of 'intended recipient' for communications sent to an electronic address on a computer network operated by or on behalf of the AFP. The Supplementary EM (at p. 4) explains the effect of the new s 5G(2) in relation to the AFP as follows [emphasis added]:

> *The effect of the amendment will be to enable the AFP to intercept (copy) all e-mail communications received at the AFP network boundary before they are received by the individual intended recipient*. Unlike all other organisations, the AFP will therefore be able to access these communications without warrant before they are received by the intended recipient. This is to ensure the maintenance of the AFP's Professional Standards.
>
> *All other organisations will be prohibited from accessing stored communications without a warrant until such time as they are received by the intended recipient,* thereby ensuring that only communications that have been delivered to, are under the control of, or are accessible by the intended recipient may be accessed without warrant.

The extracted portion of the Supplementary EM is difficult to reconcile in some respects with the actual wording of s 5G(2) of the TIA Act.[15] However, the provisions themselves, and the EM, suggest that communications continue to 'pass over a telecommunications system' until they are able to be physically accessed by their intended individual recipient, within a corporate network. It is not necessary that the intended individual recipient actually accesses the communication for it to complete its passage. However, it appears that an incoming email sent to an individual user on a corporate network would only complete its passage over the telecommunications system when it arrives at the destination mail server and is able to be accessed by its intended recipient.

The AFP's special rights to lawfully access and record incoming communications at its gateway appear intended to complement the legislative reforms introduced by the *Law Enforcement (AFP Professional Standards and Related Measures) Act 2006* (Cth) which received Royal Assent on 30 June 2006.[16] The government is also aware of the conflict between the general prohibition against interception of communications and the need to allow other organisations and network administrators to lawfully access and record communications passing over their computer networks.[17] Accordingly, the current provisions may be an interim measure as the government works towards a long-term solution to the conflict between the general interception prohibition and the operational needs of employers and network administrators.[18]

Further amendments to the TIA Act may be made during Parliament's 2006 spring sittings.[19] However, in the meantime, it is important that all employers and network administrators understand that the amendments introduced by the Stored Communications Act on 14 December 2004 are no longer effective. As a result, all organisations should review their IT security and acceptable use policies as well as their network administration practices to ensure they do not authorise or engage in behaviour that is unlawful under the new telecommunications interception and access regime.

It is important that all employers and network administrators understand that the amendments introduced by the Stored Communications Act on 14 December 2004 are no longer effective.

Concluding remarks

Given Parliament's primary concern of striking the right balance between empowering law enforcement agencies and protecting the privacy of personal communications, it is perhaps unsurprising that the operational needs of employers and network administrators have not been specifically addressed. The government's long-term solution to the conflict between the general interception prohibition and lawful access rights for the purpose of network administration will continue to develop. Whilst it does so, organisations should continue to review their policies and practices at regular intervals to account for the ongoing changes in communications technology and the laws that govern it.

Andrew Schatz *is the national leader of AGS's Media and Communications Network. He has extensive knowledge of technology related legal issues and has advised a number of agencies regarding their IT security and acceptable use policies. Andrew has degrees in both law and computer science and has specialist expertise with commercial electronic messaging.*

Notes

1 See the Explanatory Memorandum to the Amending Act at p. 9 and the Hon. Philip Ruddock MP, Attorney-General, House of Representatives Hansard, 16 February 2006, at p. 10.

2 See the EM at p. 9.

3 *Edelsten v Investigating Committee of New South Wales* (1986) 7 NSWLR 222 at p. 229 (Lee J); *R v Edelsten* (1990) 21 NSWLR 542 at p. 548 (CCA); *T v Medical Board* (SA) (1992) 58 SASR 382 at p. 398 (Matheson J; Debelle J agreeing); *Green v The Queen* (1996) 124 FLR 423 at p. 432 (Franklyn J; Pidgeon and Rowland JJ agreeing).

4 The Hon. Philip Ruddock MP, Attorney-General, House of Representatives Hansard, 16 February 2006, at pp. 7–8.

5 See AGS *Commercial Notes* No. 13 (8 February 2005) for further examples of circumstances where network administrators may require access to email and Internet communications passing over their networks.

6 AGS *Commercial Notes* No. 13 (8 February 2005).

7 House of Representatives Hansard for: 28 February 2006 at pp. 95–96 (per Duncan Kerr MP), 1 March 2006 at p. 2 (per Peter Garrett MP) and at pp. 8–9 (per Daryl Melham MP); Senate Hansard for 28 March 2006 at pp. 85–86 (per Senator Natasha Stott Despoja).

8 See the House of Representatives Hansard for 1 March 2006 at pp. 12,14 (per the Hon. Philip Ruddock MP, Attorney-General) and the Senate Hansard for 28 March 2006 at pp. 93, 124 (per Senator the Hon. Chris Ellison, Minister for Justice and Customs).

9 The act of opening and viewing an email on a computer monitor usually involves the automatic creation of a 'pagefile' record of all or part of the email which can be subsequently retrieved and viewed until such time as it is 'written over'.

10 Senate Hansard, 29 March 2006, at pp. 131–132 and 30 March 2006, at pp. 2–4 (per Senator the Hon. Chris Ellison, Senator Joe Ludwig and Senator Natasha Stott Despoja).

11 See AGS *Commercial Notes* No. 13 (8 February 2005) at p.2 .

12 See the EM at p. 6 and the Supplementary EM at p. 3.

13 See AGS *Commercial Notes* No. 13 (8 February 2005) at p. 6 for an action checklist setting out some of the issues to be considered during any such policy review.

14 See footnote 4 above and also p. 9 of the EM.

15 The extracted text twice refers to organisations other than the AFP being unable to access communications without a warrant '... before they are received by the intended recipient'. However, an ordinary reading of the provisions suggests that a more accurate explanation would be: 'All other organisations will be prohibited from *intercepting* incoming communications before they become *accessible to* their intended recipient'.

16 Senate Hansard, 29 March 2006, at pp. 125–129 (per Senator the Hon. Chris Ellison, Senator Joe Ludwig and Senator Natasha Stott Despoja). In particular, see Senator Ellison's comments on p. 126.

17 Senate Hansard, 29 March 2006, at pp. 125–126 (per Senator the Hon. Chris Ellison).

18 See the preceding footnote and also p. 4 of the Supplementary EM.

19 Senate Hansard, 28 March 2006, at pp. 93, 117 (per Senator the Hon. Chris Ellison.)

Checklist for clients

Ensure your policies and practices:

- don't endorse unlawful practices
- keep up with changing laws and technology.

Keep staff/users informed through:

- carefully drafted policies
- training sessions and screen prompts
- alerts on access or recording practices
- watching for AGS updates.

Seek advice before accessing or recording any incoming communications before they can be accessed by their intended recipients.

Be aware that many popular spam and virus filtering software products record incoming communications as part of the filtering process.

AGS contacts

AGS has a national team of lawyers specialising in communications law. For legal advice please contact Andrew Schatz of our Adelaide office on tel: 08 8205 4201, email andrew.schatz@ags.gov.au, or Robert Orr QC of our Canberra office on tel: 02 6253 7129, email robert.orr@ags.gov.au or any of the lawyers listed below.

Canberra	Jake Blight	02 6253 7035
Sydney	John Berg	02 9581 7624
Melbourne	Jeff Cranston	03 9242 1367
Brisbane	Martin Hanson	07 3360 5643
Perth	Justin Jones	08 9268 1125
Adelaide/Darwin	Andrew Schatz	08 8205 4201
Hobart	Peter Bowen	03 6220 5474

For enquiries regarding supply of issues, change of address details etc.

T *02 6253 7052* ***F*** *02 6253 7313* ***E*** *ags@ags.gov.au*

Canberra
50 Blackall Street Barton ACT 2600

Sydney
Level 42, 19 Martin Place Sydney NSW 2000

Melbourne
Level 21, 200 Queen Street Melbourne VIC 3000

Brisbane
Level 12, 340 Adelaide Street Brisbane QLD 4000

Perth
Level 19, 2 The Esplanade Perth WA 6000

Adelaide
Level 20, 25 Grenfell Street Adelaide SA 5000

Hobart
Level 8, 188 Collins Street Hobart TAS 7000

Darwin
Level 3, 9–11 Cavenagh Street Darwin NT 0800

Web site
For a full review of AGS services, visit <www.ags.gov.au>.

Electronic versions of AGS newsletters are available for clients who prefer to receive issues in this form. Please contact 02 6253 7052 or email ags@ags.gov.au to arrange supply.

ISSN 1433-9549
Approved Postage PP 255003/05310