Interception Law Under Scrutiny

On the anniversary of September 11, Ben Kuffer reviews the rise and fall of a key plank in the government's post September 11 2001 reforms.

INTRODUCTION

The Federal Government's widely criticised hardline response to the September 11 2001 terrorist attacks has been dealt a blow, with the Senate rejecting certain controversial proposed amendments to the *Telecommunications (Interception) Act 1979* ("**TIA**"). The impact of the aboutface means, at least for now, a victory for privacy in the telecommunications sector and a continuing level of confusion for certain telecommunications sector participants such as internet service providers.

This article reviews the key components of the TIA and the proposed amendments, considers whether the TIA remains effective in light of dramatic changes in technology and policy since its inception, and considers whether Australian's have missed yet another opportunity for debate. The article does not consider the more specific procedural amendments proposed by the Bill such as the proposed amendments to the TIA relating to the Western Australian Anti-Corruption Commission, the Royal Commission into Police Corruption or the NSW Independent Commission Against Corruption[1].

HISTORY OF THE *TELECOMMUNICATIONS (INTERCEPTION) ACT 1979*

The TIA details the rights and responsibilities of Australian's in relation to the interception of communications. On its introduction, the TIA significantly expanded the grounds for which telephone interception may be authorised. Due to the increasing use of computers and electronic technology, the TIA extended the scope of protection from interception to include other telecommunications services such as data transfer systems[2].

The TIA is a tool used to regulate the access of law enforcement agencies to private communications. The TIA became the secure legal basis for the use of telephone intercepts for general law enforcement purposes[3] but this was coupled with an "objective to protect the privacy of telecommunications passing between users of telecommunications systems"[4]. The tension in the TIA is that it is per se an offence to intercept telecommunications but this is balanced with Parliament's and the broader community's law enforcement and national security interests.

Commentators have noted that "in Australia the legislation governing the interception of communications is not entirely satisfactory"[5] and the TIA has been described as "a model of legislative obscurity, being confusing, circular and verbose"[6].

CASE LAW - WORKINGS OF THE TIA

It is useful to drill-down into the workings of the TIA and, by reference to case law, to determine exactly what is permitted and prohibited in relation to intercepting communications in the Australian telecommunications system.

Interception is defined in section 6(1) of the TIA as:

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

(a) Telecommunications System

The TIA only applies to communication passing over a "telecommunications system", and as such the definition of telecommunications system is critical. The definition of "telecommunications system" and "telecommunications network" contained in section 5 of the TIA have the effect of limiting the application of the TIA to communications which pass over a system or series of systems for carrying communications by means of guided or unguided electromagnetic energy or both, and includes equipment, a line or other facility that is within Australia, but does not include a system or series of systems for carrying communications solely by means of radiocommunications[7]. If a communication is made solely by means of radiocommunication it may be intercepted without infringing the TIA.

The distinction between radio communications (a form of unguided electromagnetic energy) and the definition of "telecommunications network" contained at section 5 of the TIA is unclear. However, the TIA has been amended so that the definition of telecommunications system now more clearly includes mobile telephony.

The current definition of telecommunications system is broad enough to cover technological advancements that we know about at present, such as optic fibre and other opto-electronic developments, because these new developments are guided or unguided[8]. The problem, however, is whether there is sufficient flexibility in the legislation to cover what has not yet been invented and to distinguish any 'new' telecommunications network (as defined) from a radiocommunications network.

(b) Passing Over

As described above, another component of interception under the TIA is the fact that the communication must be "passing over" the telecommunications system. Numerous cases have considered what is meant by the term passing over and the Courts have applied a technical test to determine same[9]. The Criminal Court of Appeal in *Edelsten* upheld Lee J.'s decision in the original *Edelsten* trial[10] to reject an argument put forward by the plaintiff that electromagnetic waves picked up by a scanner were free in the air and not passing over a telecommunications system. The judge held that the mobile phone's electromagnetic waves were in fact part of a system controlled by the then Telecom which had control of the transmitting and receiving unit. The means used to listen to or record the signal in the course of the passage over the telecommunications system was held by the court to be irrelevant[11].

Passage over a telecommunications system was also considered by the judiciary in *Miller v Miller (1978)*[12] ("***Miller***"). Here the High Court applied an earlier 1960 Act and, among other things, concluded that the 1960 Act was inconsistent with the State listening devices legislation[13] and to the extent of the inconsistency, the 1960 Act applied. In essence the High Court, by accepting that the Commonwealth Act applies, concluded that the recording of a

conversation by a party lawfully on a premises but eavesdropping on another extension did not constitute interception of a communication passing over a telecommunications system and was therefore admissible in the original Family Court proceedings because the listener was lawfully on the premises and the communication at a second extension was passing over the telecommunications system. The judgment in *Miller* allowing the admission of the recorded phone call between the mother and child at the centre of a custody dispute goes against Sackville J.'s comments in *Taciak* which suggest a "restrictive approach to the construction of the statutory exceptions to the prohibitions on the interception of telecommunications and on the use of lawfully obtained intercept information"[14].

In *Harvey v Baumgart (1965)*[15], Gowans J held that "passing over" required an element of "automatic simultaneousness"[16]. In *R v Curran*[17] McGarvie J held that a portable tape recorder held to the earpiece of a telephone which was being used by another person illegally (ie a wire had been run so that a legitimate service was being charged for another person's calls) was not an interception because the recording of the communication passing over the telecommunications system was done by equipment not part of the service[18]. See further *R v Luciano Giaccio* SASC 6103 (1997)[19].

McGarvie J distinguished the decision of Cosgrove J in *R v Migliorini*[20] because the tape recorder in that instance was attached directly to the wire and made its recording "directly by the electromagnetic energy passing through the service"[21]. Cosgrove noted that the legislation would not capture an external recording device but McGarvie disagreed with this limited construction[22] of interception and, following the decision in *Miller* held that an external tape recorder held up to an earpiece recording the sounds being emitted was in fact recording of a communication passing over the telecommunications system. This interpretation was confirmed by the minority in *T v The Medical Board of South Australia (1992)*[23] (***"T v Medical Board SA"***) and the decision in *Miller* by the majority is inconsistent with *T v Medical Board SA*.

(c) Without the Knowledge

The third element of the definition of interception of a communication is that the interception must be made "without the knowledge" of the person making the communication. In *T v Medical Board SA*[24] interception was held to occur if a third party intrusion into a communication was made without the knowledge of the caller or the recipient[25]. The TIA offers no protection as between the caller and the intended recipient, but only against an invading third party[26].

PROHIBITION ON INTERCEPTION – SECTION 7 OF THE TIA

Section 7(1) of the TIA prohibits the interception (as defined above) of communications passing over the telecommunications system in the following circumstances;

> *"A person shall not:*
>
> *(a) intercept;*
>
> *(b) authorize, suffer or permit another person to intercept; or*
>
> *(c) do any act or thing that will enable him or her or another person to intercept;*
>
> *a communication passing over a telecommunications system"*

EXCEPTIONS TO THE PROHIBITION

These prohibitions are subject to certain exceptions which allow for interceptions to be made in connection with certain activities including, without limitation, interception of a communication by a person;

- who is an employee of a carrier in the course of his or her duties for or in connection with, among other things the installation of any line or equipment used or intended for use in connection with a telecommunications service[27], the operation or maintenance of a telecommunications system[28] or the identifying or tracing of any person who has, is suspected of or is likely to contravene a provision of Part VIIB of the *Crimes Act 1914*[29] where it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively;
- who is another person lawfully engaged in duties relating to the installation or maintenance of equipment or a line[30];
- who is lawfully engaged in duties relating to the installation, connection or maintenance of equipment used, or to be used, for the interception of communication under warrants[31];
- which is incidental to, or results from action taken by an officer of the Australian Security Intelligence Organisation in discovering where a listening device is being used at or is located[32];
- under a warrant[33]; or
- in an emergency (as defined in section 30 of the TIA)[34].

It is important to note that the stipulation that communications may not be intercepted is also waived (i.e. in addition to those exemptions listed above) if an officer of an agency[35] is a party to the conversation and there are reasonable grounds for suspecting that another party to the communication has, among other things, caused or threatened to cause serious injury, killed or threatened to kill another person, seriously damaged property or threatened to take his own life. The provisions of s. 7(6) of the TIA give broad powers to certain officers to retrospectively apply for Class One and Class Two warrants in an 'emergency' situation.

TELECOMMUNICATION INTERCEPTION WARRANTS

The issuing of interception warrants by the Attorney-General to ASIO and other law enforcement agencies is subject to specific and detailed regulations. In the case of law enforcement agencies, warrants may be issued to assist in the investigation of certain serious offences as defined in sections 5 and 5D of the TIA[36]. Warrants can be obtained in relation to particular identified telecommunications services or any telecommunication service that is used or is likely to be used by a named individual.

WHAT IF THE TIA DOES NOT APPLY?

The above cases and the development of judicial opinion has shown that as a general rule listening in to or recording communications using equipment which is "electronically connected into or which intercepts radio signals transmitted by a telecommunications system"[37] is covered by the TIA. If the equipment is external to the telecommunications system then the State based listening devices legislation applies[38]. This is reinforced by Barwick

CJ in *Miller* who states, "the TIA does evince a clear intention to be the whole law on the matter of telephonic interception"[39] and, as a result, holds that the TIA prevails over the State based legislation. This is consistent with the provisions of s. 109 of the *Constitution*[40]. If the State based legislation does not apply then the standard search warrant provisions apply.

Telecommunications interception is also dealt with under the *Telecommunications Act 1997* (**"TA"**). This article does not attempt to deal with the provisions of the TA, suffice to note that the essential difference between the TIA and the TA in respect of telecommunications interception is that the TIA "makes it an offence for anyone, subject to certain exemptions to intercept telecommunications"[41] whereas Part 13 of the TA makes it an offence for people in the business of telecommunications to disclose or use confidential communications that come into their knowledge or possession through their legitimate business.

TELECOMMUNICATIONS INTERCEPTION LEGISLATION AMENDMENT BILL

On 27 September 2001, the *Telecommunications Interception Legislation Amendment Bill (2001)* (**"2001 Bill"**) was introduced before the House of Representatives. The 2001 Bill had not passed either Chamber before the Parliament was prorogued for the 2001 Federal Election and consequently it lapsed.

On 12 March 2002, after the federal election had been held and importantly the world had experienced the dramatic events of September 11 2001, the now amended *Telecommunications Interception Legislation Amendment Bill (2002)* (**"2002 Bill"**) was re-introduced into the House of Representatives by the Attorney General. The 2002 Bill expanded on the 2001 Bill by including a new offence (act of terrorism) for which a telecommunications interception warrant may be sought. The 2002 Bill was introduced by the Federal Government as one component of a suite of some five anti-terrorism bills[42]. Amid a storm of controversy the 2002 Bill was passed the next day by the House of Representatives and introduced into the Senate on 14 March 2002.

The Senate refused to pass the suite of bills and demanded an enquiry be conducted by the Senate Legal and Constitutional

Legislation Committee (**"SLCLC"**). This report has been tabled and contains significant recommended amendments to the 2002 Bill and the other 5 anti-terrorism bills. There has been an outcry, indicated by the a total of 431 submissions to the SLCLC, in relation to the legislation and the unwillingness of bi-partisan members of the Senate to rush to pass the bills notwithstanding the panic that followed 11 September 2001. The Committee's report (**"SLCLC Report"**) was released in early May 2002 and it contained some key recommendations in relation to both suite of anti-terrorism bills and specifically the 2002 Bill[43].

Although some amendments to the TIA did carry, the Senate rejected amendments that would have allowed law enforcement agencies to access, without a warrant, the content of messages such as email, voicemail and SMS, while such communications were delayed or temporarily stored on a telecommunications service providers' equipment during transit.

The purpose of the 2002 Bill was to amend the TIA[44] to, among other things;

- expand Class 1 and Class 2 offences to include offences constituted by conduct involving acts of terrorism, child pornography and serious arson[45]; and
- legislatively clarify the application of the TIA to telecommunications services involving a delay between the initiation of the communication and its access by the recipient, such as email and short messaging services[46].

(a) New Offences

As stated above, the 2002 Bill expanded the Class 1 and Class 2 offences in relation to which a telecommunications interception warrant may be sought.

The Federal Attorney-General, in the Second Reading Speech for the 2002 Bill stated, in relation to the proposed amendments dealing with "terrorism" as an offence, that "these provisions and other measures taken" (that is the suite of bills introduced as part of the terrorism legislation), "are designed to bolster our armoury in the war against terrorism and deliver on our commitment to enhance our ability to meet the challenges of the new terrorist environment"[47].

The proposed amendments do not define what is meant by an offence being that

'constituted by conduct involving an act or acts of terrorism'. The Explanatory Memorandum to the 2002 Bill states that the reason for this is so that intercepting agencies are able to seek interception warrants in connection with terrorism offences howsoever they are defined in relevant legislation[48]. It is unclear as to what these offences are. This is a significant risk to the privacy of users of the telecommunications system.

The Senate passed the proposed new Class 1 and Class 2 offences, with the exception of 'terrorism'. However, the Government stated that it intended to reintroduce this provision in the spring sitting of parliament. If terrorism is included as a Class 1 offenee it will be less well defined than the other Class 1 offences of the TIA. Also, due to its classification as a Class 1 offence it will be subject to significantly less preconditions for the issuance of a warrant than the stringent conditions used to determine the result of an application for a Class 2 warrant[49]. This amendment is clearly a reaction to 11 September. The underlying theme of the SLCLC Report and submissions relating to it suggests that the amendments have been rushed and ill-planned.

(b) Delayed Access Message Services

The other controversial amendment to the TIA is the proposed new sections 6(3)-(5) which deal unsatisfactorily with the concept of delayed access message service[50]. Of the 400 plus submissions to the SLCLC, only a select few mentioned these amendments which attempt to indicate when delayed access message services, such as emails and voicemail, will be regarded as communications passing over a telecommunications system and thus subject to the TIA and the requirements surrounding interception warrants.

These provisions were also rejected by the Senate. As with the terrorism provision, the Government has also stated its intention to reintroduce the delayed access message service amendments into parliament later in the year. For this reason, analysis of these proposed amendments is relevant.

The Attorney-General in his second reading speech stated:

> *"The amendments make it clear that a communication will fall outside the definition of interception where it is stored on equipment and can be accessed using that equipment but without reference to the telecommunications network"*

In that event, agencies will be able to access the communication using a search warrant or other means with a less stringent test for issuance. It is not clear if, as indicated in submissions, the 2002 Bill intended to protect emails from the time they are sent to the point at which they have been downloaded to a recipient's computer[51]. They in fact may not be protected for anywhere near as long as that indicated under the amendments depending on the technology used by the recipients email provider and his method of accessing same[52].

Problems also arise with messages stored on an ISP's server as such messages can be accessed by the equipment on which it is stored without using a telecommunications line. Access to these communications is available to anyone with access to the ISP's premises and computer passwords. The key risk is that an agency possessing only a search warrant, or merely a certificate issued under Part 13 of the TA, may access such communications in this way rather than acquiring an interception warrant[53].

The relevant section of the 2002 Bill sought to insert at the end of the TIA section 6, (from above the clause dealing with what constitutes an interception for the purposes of the TIA), certain provisions which indicate when delayed access message services such as email and voicemails will be regarded as passing over a telecommunications system and thus subject to the protection of the TIA.

The essential problem with the proposed amendments is the arbitrary distinction drawn in relation to the form of access. If, for example, a person needs to access a telecommunications service in order to access an email or voicemail message then an interception warrant is required. If however, the same voicemail or email can be accessed from a company's premises without the use of the telecommunications system, for example potentially if the voicemail is digitised and stored on a computer hard-drive or an email is stored on a server, then the provisions of the TIA will not apply[54]. In that event some other lawful authority will be required before a third party could access the message or email[55]. The probable reason for this is that, if a message isn't passing over a communications system, it may be beyond the scope of section 51 of the Australian Constitution.

The proposed amendments may lead to the situation where voicemail and email at the service provider's location are not protected by the TIA and may be accessed with a search warrant, however a telecommunications interception warrant will be required at the time that the intended recipient accesses the messages.

The proposed definition of delayed access message service is also problematic in relation to the GSM mobile phone short message service ("SMS"). Under the proposed amendments an SMS message in its passage to a handset would be protected by the TIA but once it is opened or stored on the phone's SIM card it would no longer be covered by the TIA. Likewise, as with an email message, once it has been downloaded or replicated to a computer hard drive whether or not at the point of downloading the message has been opened.

IMPACT OF PROPOSED AMENDMENTS

The focus of Australia's telecommunications regulatory framework is that of a light touch self-regulation based model with significant consumer protections[56]. A key aspect of the consumer protection provisions is for codes of conduct to be developed consultatively by all stakeholders in the industry. The Australian Communications Industry Forum ("**ACIF**"), an industry body established to manage the telecommunications industry's response to self-regulation through a system of committees and working groups made up of representatives from the industry, consumer groups and the various regulators, has facilitated the development of a voluntary guidelines entitled "Participant Monitoring of Communications"[57]. The guidelines are intended to provide guidance to call centres, carriage service providers and carriers who have need to monitor communications by other people within the relevant organisation (eg supervisor).

The ACIF guideline is a valuable resource for participants in the telecommunications industry and provides a good summary of the Act from a practical perspective. The guideline must be updated to include the significant recent amendments when and if they are passed through parliament. There may be particular difficulty for ACIF in interpreting the amendments. To be relevant to an ISP for example, any new ACIF code or guideline would need to clarify whether an agency is entitled, without an interception warrant, to access communications stored on an ISP's server[58].

Currently, some ISP's are refusing access to data without a telecommunications interception warrant[50]. The proposed amendments, as currently drafted, may permit the agencies to access the communication without an interception warrant.

In its submission to the Senate Enquiry, the Office of the Federal Privacy Commissioner questioned why the 2002 Bill sought to remove the privacy protection via the requirement of an interception warrant in relation to a voicemail or SMS merely because they transmission is delayed[60]. With the December 2001 amendments to the Commonwealth *Privacy Act*, and a heightened public and political awareness of the issue, it remains to be seen whether the government will risk removing an important privacy protection mechanism from the playing field.

CONCLUSION

The rejection of the proposed amendments is an initial victory for common sense and privacy in Australia. However, it remains to be seen if the legislative clarification required to establish a logical and consistent system of interception, which is able to deal with new technology such as SMS, actually eventuates.

The views expressed in this article are those of the author and not necessarily those of the firm or its clients.

Ben Kuffer is an Associate in the Information, Communications and Technology Group at PricewaterhouseCoopers Legal, Sydney.

1 Other amendments proposed include, without limitation, those relating to the removal of references to defunct State bodies and the substitution of replacements.

2 See TIA at s.5 "Communication" which is defined to mean "conversation and a message... in the form of *(among other things)* speech, data, text and visual images". The definition of "Telecommunications Network" is also instructive in that it is so broad as to include both guided and unguided electromagnetic energy.

3 *"Electronic surveillance, human rights and criminal justice"*, Simon Bronitt, Australian Journal of Human Rights, 3(2), 1997, at p.188, as referred to in Dept of Parliamentary Library

4 *Alan Taciak v Commissioner of Australian Federal Police ("**Taciak**") (1995)* NG 476, Unreported, at 24.

5 *"Controlling the Interception of Communications: Law or Technology?"*, RG Smith, Australian Institute of Criminology, 1997, at p.1.

6 *"Aspects of Criminal Investigation: Arrest, Search and Seizure, Listening Devices and Telephone Taps"*, D.Re, paper presented at Young Lawyers, Continuing Legal Education Seminar, 16 August 1995, as cited in Smith.

7 s.5 TIA, see further *"Controlling the Interception of Communications: Law or Technology?"*, RG Smith, Australian Institute of Criminology, 1997, at p.3.

8 *Personal conversation with D.J.Bowman*, UNSW Physics and Bio-medical Engineering.

9 *"Participant Monitoring of Communications"*, Australian Communications Industry Forum G:516, July 1998 at 4.3.

10 *R v Edelsten* (1990) 21 NSWLR 542 at 548.

11 Ibid at 549.

12 *Miller v Miller (1978)* 141 CLR 269.

13 Barwick CJ in *Miller* states that, "The 1960 Act *(sic)*does evince a clear intention to be the whole law on the matter of telephonic interception: nor should such a conclusion be surprising for the telephone system is provided and administered by an Australian instrumentality under Australian law".

14 Op cit note 4 at 27.

15 *Harvey v Baumgart (1965)* 7 FLR 389.

16 ibid at 393 and 395.

17 *R v Curran (1982)* 50 ALR 745 per McGarvie J.

18 Note that passing over was accepted by the Court and as it was an interception not permitted by the TIA, the court used its discretion to admit the recording on public interest grounds.

19 In this case Cox J states that In my opinion the taping of these telephone conversations by means of a micro-cassette recorder, held close to the telephone hand-piece by one of the persons having the conversation, did not amount to an interception of a communication passing over a telecommunications system within the meaning of sections 6 and 7 of the Interception Act

20 *R v Migliorini (1982)* 38 ALR 356.

21 Ibid at 360.

22 *R v Curran* (1982) 50 ALR 745 at 767

23 See further Olsson J's judgment in *T v The Medical Board of South Australia* (1992), 58 SASR 382

24 Ibid per Matheson J at 397.

25 This decision was followed in *Carbone and Another v National Crime Authority and Others (1994)*.

26 *Green v R* (1995) 135 ALR 81.

27 TIA, s. 7(2)(a)(i)

28 TIA s. 7(2)(a)(ii)

29 TIA s. 7(2)(a)(iii)

30 TIA s. 7(2)(aa)

31 TIA s. 7(2)(ab)

32 TIA s. 7(2)(ac)

33 TIA s. 7(2)(b)

34 TIA s. 7(2)(c)

35 Agency for the purposes of this part of the TIA means the Australian Federal Police, ASIO and eligible State agencies as declared by the Minister pursuant to s. 34 of the TIA. These agencies must also be listed in the corresponding year's Annual Report.

36 Op cit note 5, at p. 4.

37 *"Participant Monitoring of Communications"*, ACIF G516:1998, July 1998, at 4.4.

38 Op cit note 12

39 Op cit note 12 per Barwick CJ at 13.

40 The relevant constitutional law is not the topic of this paper other than to note that s.109 of the Constitution states that to the extent of any inconsistency between Commonwealth (i.e. TIA) and State (i.e. Listening Devices Act) laws, Commonwealth legislation shall apply. In *Miller*, Barwick CJ held that the was an inconsistency between the legislation brought about by a "manifestation of intention" by the Commonwealth Act that it be the whole with respect to telecommunications interception (Op cit note 12 per Barwick CJ at 12).

41 *"Australian Telecommunications Regulation"*, edited by Jock Given and Alasdair Grant, 2nd edition 2001, at p.229.

42 The five bills are: *Security Legislation Amendment (Terrorism) Bill 2002, Suppression of the Financing of Terrorism Bill 2002, Criminal Code Amendment (Suppression of Terrorist Bombing) Bill 2002, Border Security Legislation Amendment Bill 2002* and the 2002 Bill.

43 SLCLC Report, May 2002.

44 *"Telecommunications Interception Legislation Amendment Bill 2002"*, Department of Parliamentary Library Information and Research Service, Bills Digest No. 121 2001-2002 at p. 6..

45 *"Explanatory Memorandum - Telecommunications Interception Legislation Amendment Bill 2002"*, circulated by the Attorney-General, the Honourable Daryl Williams, at p. 2. As interception warrants can only be issued for Class 1 and Class 2 offences new offences are proposed in these classes to include terrorism, arson and child pornography.

46 ibid

47 *Hansard*, House of Representatives, 12 March 2002, p 977.

48 Op cit note 44 at p. 14.

49 Compare TIA s. 45 (e) re. Class 1 offence with 46(2) Class 2 offence.

50 This amendment only appeared in the 2002 Bill and not in the TIA amendments as originally tabled in the *Telecommunications Interception Legislation Amendment Bill 2001*.

51 Electronic Frontiers Australia, submission to the Senate and Constitutional Legislation Committee, 5 April 2002, Submission Number 134, at p 4.

52 An example may be the situation where an email is sent to a recipient who downloads the email by way of replication onto his hard drive and does not look at the email until some time later. The email would no longer be protected once off line unless the recipient logs in remotely to a server and downloads this mail over the telecommunications system.

53 Oz Net Law submission to the Senate Legal and Constitutional Committee

54 These are but some eventualities. It is highly probable that the interception provisions will only cover a small portion of delayed access message situations.

55 Explanatory Memorandum to the 2002 Bill, at p. 4.

56 *"Telecommunications and new technologies"*, Office of the Privacy Commissioner, www.privacy.gov.au, at p. 34.

57 Op cit note 33.

58 From above this is relevant because emails stored on the ISP's server are stored communications as they can be accessed by the equipment on which they are stored without using a telecommunications line.

59 *Hansard*, Legal and Constitutional Committee, 19 April 2002, p. 211.

60 Federal Privacy Commissioner Submission to the Senate Legal and Constitutional Legislation Committee, 15 April 2002, at p. 14.