Australian Privacy Foundation

p o s t: GPO Box 1196
Sydney NSW 2001

e m a i l: enquiries@privacy.org.au

w e b : www.privacy.org.au

20 May 2005

Re: Review of the Regulation of Access to Communications under the *Telecommunications (Interception) Act 1979*

Submission by the Australian Privacy Foundation

Introduction

The Australian Privacy Foundation

1. The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For information about the Foundation and the Charter, see www.privacy.org.au

2. We note that the Foundation has made a significant contribution over a sustained period to inquiries and reviews on the subject of telecommunications interception (see Attachment), including giving evidence to several Senate Committee inquiries.

Inadequate consultation period

3. Without labouring the points made in our letter of 19 April, we re-iterate our concern about the limited consultation period and lack of transparency of information relevant to the review. Despite the terms of reference being dated July 2004, the review was only announced, and invitations made to interested parties, in March 2005. We contrast the limited opportunity for public input with the more than 9 months that have been available to government agencies, who have no doubt been aware of the terms of reference, at least in general terms, since last year and have had the opportunity to prepare detailed submissions and supporting cases.

Policy Objectives on Interception

4. We are pleased to see that the Terms of Reference for this Inquiry do not set up privacy and other public interests as necessarily in opposition. We strongly believe that it should be possible *both* to maintain strong privacy protection *and* to meet the legitimate needs of security and law enforcement agencies. We also support the objective of legislation that, as far as possible, is technology neutral.

Relevant Legislation and Guidelines - commentary

Telecommunications (Interception) Act 1979

5. The *Telecommunications (Interception) Act 1979* (TIA) is obviously the primary legislation dealing with interception of personal communication when it is passing over the telecommunications system. We argue that the underlying intention of this legislation is not simply to regulate the conduct of interception, but also to protect the privacy of personal communications. Exceptions are permitted only in the case of need in relation to serious matters of law enforcement and national security, demonstrated to the satisfaction of an ndependent decisison maker. In such cases, the Act provides significant protections for the privacy of the communication through high thresholds of need (investigation of major offences), the requirement for

warrants issued by an independent quasi judicial decision maker[1], and transparent reporting requirements.

ACIF Guidelines on the interception legislation

6. The Australian Communications Industry Forum (ACIF) has issued two Industry Guidelines *Participant Monitoring of Voice Communications* (ACIF G516:2004) and *Monitoring of Voice Communications for Network Operation and Maintenance* (ACIF G517:2004). Both were revised in 2004 to reflect significantly revised interpretation by the Attorney-General's Department about the meaning of two exceptions to the prohibition on interception in the TIA.

7. Guideline 516 deals with the monitoring of voice (but not data) communications by one of the parties to that communication, while Guideline 517 sets out processes for the monitoring of communications, by carriers or carriage service providers (CSPs)[2] only, for the purposes of installation, operation or maintenance of a network. These Guidelines provide important context for discussion of interception policy.

Telecommunications Act 1997

8. The *Telecommunications Act 1997* (TA) also provides protection for communications, but in a different and broader context. The protection applies not only to the content or substance of communications, but also to other personal information such as a subscriber's name, addresses, telephone numbers, billing information and call charge records, i.e.details of the time, date, parties to and duration of each communication.. The use and disclosure restrictions in the TA (Part 13) do however apply only to the service provider (carrier or CSP), their employees and contractors, rather than the far broader general prohibition against *any person* intercepting communications under the TIA.

9. Privacy protection under the TA is significantly weaker than under the TIA. The situations in which information other than 'content or substance' can be revealed are not restricted to situations of serious crime or national security, but extend for instance to assistance with any law enforcement matter; the arrangements for directories; emergency services; complaint handling by the Telecommunications Industry Ombudsman (TIO) and Privacy Commissioner, etc.

10. Disclosure is only protected by requirements of a warrant in limited circumstances and the only accountability is through requirements under Pt 13 Divison 5 of the TA for some limited record keeping and reporting by carriers and CSPs and monitoring by the Privacy Commissioner (but see below for evidence of how these latter supposed safeguards have been rendered ineffective).

[1] The Act has already been weakened by the amendments which allowed for warrants to be issued by senior members of the AAT, rather than only, as previously, by tenured judges.

[2] Note that Internet Service and Access Providers (ISPs and IAPs) are subsets of the wider class of carriage service providers under the TA.

Privacy Act 1988

11. The *Privacy Act 1988* (PA) has applied since 1988 to most Commonwealth agencies and, since 2001, to most larger private sector organisations, including telecommunications carriers and CSPs. The PA requires holders of personal information to comply with a set of Principles (IPPs or NPPs). which are however relatively permissive in relation to use and disclosure, allowing for instance any use and disclosure authorised or required by or under law, and for more or less anything the holder chooses to do provided they have been open about it.

12. Because of the permissive nature of the use and disclosure principles, the PA adds little to the TIA and TA constraints, and cannot be accurately portrayed in any sense as an adequate alternative. It is more effective in requiring complementary safeguards in relation to data quality, security, notice to individuals and access and correction rights.

13. There have been two recent reviews of the PA. The Privacy Commissioner's review of certain aspects of the PA has now concluded and her report to the Minister was published on 18 May. The broader Senate Legal and Constitutional Committee Inquiry into the PA is still under way. While the findings and recommendations of the Senate Review are not yet available, it seems clear from submissions, that the need for continued and in some cases wider privacy protection is not seriously questioned. A very preliminary reading of the Privacy Commissioner's Report suggests widespread support for a strengthening of privacy protection, and certainly no serious case for weakening.

14. It is important to recognise that in the last fifteen years, privacy protection has been progressively extended to more and more areas of activity, by both federal and state legislation, and that trend seems set to continue, with a steady stream of new laws dealing with specific issues such as health privacy and surveillance, as well as the progressive adoption by the remaining States of general information privacy laws.

Overall balance between privacy protection and other public interests

15. We submit that the trend towards greater privacy protection oultined above is an important context for this review. In light of recent concerns about crime including terrorism, governments have given significantly greater powers to law enforcement, intelligence and national security agencies. While we do not oppose narrowly targeted and temporary increases in powers where they can be justified, we submit that there is growing sense that there may have been an overreaction and we are in danger of undermining the very freedoms and rights which we seek to protect, and which are under threat from terrorists and other criminals. We commend to you a recent speech[3] by High Court Justice Michael Kirby in which he made the following observation:

> "We should never forget that, to the extent that we exaggerate the risks to national security, we fall into the hands of those who threaten our constitutionalism. To the extent that their threats propel us into demolishing the fundamentals of our liberal democracy, we reward the enemies of our form of government with success. To the extent that we over-react, we proffer the terrorists the greatest tribute."

[3] *National security: proportionality, restraint & commonsense*, a paper delivered at an Australian Law Reform Commission National Security Law Conference in Sydney on 12 March 2005

16. In the same speech he referred to several recent examples in overseas jurisdictions, including the UK and USA, where excessive and disproportionate law enforcement and national security legislation has been successfully challenged in the courts.

17. In Australia, almost uniquely amongst countries with which we normally compare ourselves, we do not have the same protection of a Constitutional or legislative Bill or Charter of Rights on the basis of which laws can be challenged. This makes it all the more important that Reviews such as this are balanced and take into account these wider issues, to fully inform the Parliament which is our only guarantor of rights and freedoms.

Stored communications focus

18. We note that the immediate stimulus for this review was the passage of the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004.* This and previous Bills were the subjects of Senate Committee Inquiries that expressed serious concerns about the amendments (see below). As a consequence, the amendments were accompanied by a sunset clause, such that the exemption of stored communication from the interception prohibition in s. 7 of the TIA applies for only 12 months from the commencement of that subsection. The exception will therefore lapse in December 2005 unless successor amendments are passed.

19. We also note however that the terms of reference for this Review are broader than just a review of the stored communications provisions. We welcome this as we have long called for a more fundamental review of the basis of the TIA, which has been damaged in our view by a series of ad-hoc amendments. However, because of the limited time available, we have reluctantly focussed our submission on the stored communications issue, although we have tried to set it in a wider context. We also attach the comprehensive submission made by our then sister organisation, the Australian Privacy Charter Council, to the two reviews of Telecommunication Interception in 1999. This submission covered wider ground and many of the points made are still valid and relevant to this review.

20. Specifically, we have not had time to review the potential overlap between the TIA and Computer Crime legislation (regulating unlawful access to computer data & unauthorised impairment of computer functions); DOCITA/ACA proposals for spyware legislation (and the recently introduced Cth private member's Spyware bill) and surveillance legislation (which applies to information held that is no longer travelling over a telco system). We assume that you will have had the time and resources to take these into account.

Issues Raised by the 2004 Senate Inquiry

21. In June 2004, the Senate referred provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill to the Senate Legal and Constitutional Committee for inquiry. The Committee, chaired by Senator Payne, issued the Committee's report (Senate Report 2004) in July 2004.

22. The Report raised a number of serious issues with the Bill and, while ultimately recommending the passage of the Bill, said its operation should last only 12 months, after which time a full review should be undertaken into the TIA, particularly in relation to the exclusion of stored communications from the prohibitions on interception.

23. The issues raised by the 2004 Senate Inquiry, which remain 'live' include:

- The application of the TIA to stored communications, including Practical difficulties in ISPs determining whether a message has been accessed
- Access to stored communications, including potentially by private parties
- Implications for IT security and integrity
- The Privacy Commissioner's monitoring function

24. Below, we discuss each of these issues in turn.

The application of the TIA to stored communications

Constitutional basis

25. The 2004 Senate Inquiry heard evidence that there has been uncertainty as to the constitutional limits of of the TIA[4]. The prohibition is from intercepting communications 'in their passage over a telecommunications network', and the issue is whether a communication that has been stored (e.g. an email sitting in a server awaiting access by the intended recipient) can still be seen as 'passing over a telecommunications network'. A subsidiary issue would be whether Federal power extends to stored communications once it has ceased passage over the network and is stored and awaiting access.

26. Because both sending and receiving messages necessarily involves communications passing over a network, inclusion of stored communications in the prohibition on interception should be within Federal power. The TIA already applies to any communications (voice AND/OR data) passing over a telecommunications network, so coverage of communications, in what ever form, is already included in current provisions of the TIA. In any case, even if the communications fall outside the scope of 'telephony', they would still be within the broader reach of s.51(v) of the Constitution.

Policy basis

27. We argue that the intention of the TIA is to protect the privacy of personal communications – even if the means of communication involves a disjuncture between the time of sending and the time of receipt. The fact that an Email or SMS message has not been read by the other party to the communication means that protection should be applied to the communication throughout its delivery (whether interrupted or not).

28. The critical distinction is whether the recipient has had an opportunity to receive (hear or read) the communication and to make a decision about its future. Once the recipient of a communication has had this opportunity, the privacy of its content is in their hands – they can either delete it, or choose to store it in a variety of formats and locations, the security of which will vary but can be assessed.

[4] Given its basis in the postal … telephonic.. etc power of the Parliament conferred by s.51(v) of the Constitution.

29. Until the recipient has had that opportunity, the communication should be regarded as still 'in the course of transmission', and subject to the 'higher level' protection of the TIA.

30. One decision a recipient might make would be to leave the communication in the same storage device (e.g. E-mail or SMS inbox or Voice messagebank), but at this point the message should become subject to the same privacy and confidentiality regime as applies to communications stored elsewhere. The protection of the Interception regime should only apply up to the decision point.

31. The definition of when a recipient is considered to have had the critical opportunity for a decision should allow for a 'considered' decision, i.e. it should not be simply a 'technical' opportunity such as arrival in a recipient's mailbox or messagebank, with or without a real time 'warning' to the recipient. Recipients of communications are entitled to choose the time and place of hearing or reading, and this may involve considerable delay – such as when the recipient is out of contact with the storage device for whatever reason.

32. It also needs to be borne in mind that the privacy of the sender is also at issue. The reasonable expectation of a sender is that their communication will be protected to the same extent until the recipient has had an opportunity to decide what to do with it. Applying lesser protection at some completely arbitrary and unpredictable point of 'deposit' into a holding bay (inbox or messagebank) leaves the sender in a position of ignorance.

33. The overall effect of the current (i.e. under the stored communication amendments) arbitrary and unpredictable point of application of the TIA is that neither the sender not the recipient of many communications can know the true extent to which their communication is protected. This could have a very important chilling effect on free speech and free communication, not least political free speech.

Practical difficulties in ISPs determining whether a message has been accessed

34. The 2004 Senate Inquiry heard evidence about, but did not finally decide on, the feasibility of ISPs being able to determine whether emails had been accessed by the intended recipient, and recommended that the issue be further examined in the context of a review of the amendments on stored communications (paras 3.12-3.19). In our view, this is a matter which could be addressed by the law – carriers and CSPs could be required to devise a method of determining whether any stored communication had been accessed, and the onus should lie with the law enforcement agency interested in accessing a particular communication to ascertain whether it had not, thereby triggering the requirement for an interception warrant.

35. To the extent that it was not possible to conclusively establish whether a stored communication had been accessed by the recipient, the default position should be that the TIA applies.

Access to stored communications

36. Under the amendments relating to stored communication, because accessing stored communications is not considered an interception, the protection of stored communications then falls under Part 13 of the TA, subject also to the PA.

37. The government made great play, in its submissions to the Senate inquiries and public statements, of the protections that would still apply. In our view these submissions bordered on misleading as they implied that warrants (or at least equivalent levels of authorization) would apply to access to stored communications.

38. This is far from the case. The TA and PA both allow for any other disclosure 'required or authorised by law', so that any power of compulsion would allow access to stored communications. Only disclosures in connection with the operation of 'enforcement agencies' require a warrant (TA s.280(1)). Other powers possessed by a wide range of other Commonwealth agencies, (arguably some state agencies?) and both Commonwealth and State Courts and Tribunals could allow access without a warrant, and 'authorised by law' also allows for an unpredictable range of additional disclosures.

39. A more significant exception that undermines the assurances is provided directly by the TA s.282, which allows carriers and CSPs to disclose information (other than the 'contents or substance' protected by the TIA) to federal state or territory 'enforcement agencies' solely on the basis that the carrier or CSP decides that the disclosure is reasonably necessary for enforcement of the criminal law, the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue.

40. The Act then provides a mechanism for certificates from an enforcement agency to provide a carrier or CSP with a basis for relying on their s.282 discretion. The only safeguards in relation to these certificates are that the Privacy Commissioner is involved in determining the form of the certificate and in theory audits the records of certificates (but has no oversight of the content of the certificates (see also under Privacy Commissioner resources).

41. We also note that the Senate Report 2004 points out that there was disagreement between the AFP and AGs about whether section 3L of the Crimes Act 1914 permitted the AFP to remotely access stored communications without a TI warrant (para 3.9). We are not aware of any public announcement about the resolution of this matter.

42. All of the above points to the need for clarification of the circumstances and conditions in which access to stored communications can be obtained and by whom in the current legislative environment. We urge you to do this in your report, pursuant to the term of reference about 'providing certainty … to agencies …and for users'. Such clarification is also essential to inform a decision about the balance of public interests and whether to renew the stored communication amendments.

Access by private parties?

43. The 2004 Senate Inquiry heard arguments that private parties would be able to use Part 13 of the TA to obtain access to stored communications through court orders made during the discovery process, summons for witnesses to attend and produce records and subpoenas for documents. (Report para 3.40).

44. Whatever the arguments for access by other government agencies, it is surely not an intended or desirable consequence of the stored communication amendments to allow private parties to access the content or substance of communications without consent? We urge you to recommend that such access be expressly prohibited.

Implications for IT security and integrity

45. The 2004 Senate Inquiry heard evidence that the application of the TIA to stored communications might inadvertently prevent organisations from undertaking normal and necessary information technology security and integrity measures (Report paras 3.12-3.14).

46. The Privacy Commissioner acknowledged this and made the sensible suggestion, which we support, that a specific tailored exemption could deal with this potential difficulty (Report para 3.15). The AFP acknowledged that this would address their concerns (3.16), and the Committee expressly suggested that [the current] Review should consider this option (3.21).

Privacy Commissioner's inability to perform a monitoring function

47. The Privacy Commissioner is given a function by s.309 of the TA to monitor the records of disclosures under Pt 13 Division 3.

48. It is now even clearer than during the Senate Inquiry that this supposed safeguard has been rendered totally ineffective by the lack of resources available to the Privacy Commissioner. We refer you to the transcript of the Senate Estimates Committee on 11 November 2003 which recounts the parlous state of the Commissioner's audit capability, including the following from the Deputy Commissioner:

> " Mr Pilgrim —…. We will be undertaking three audits in the next financial year,
> and those audits will be undertaken in accordance with some memorandums of understanding
> we have with a couple of agencies to specifically undertake audits. They will be the only
> audits we will undertake."

49. The Commissioner's latest Annual Report (for 2003-04) confirms (Figure 5.3, page 65) that no TA s.309 audits were actually performed. Only one such audit was commenced in each of the two previous years. This effective cessation of auditing under s.309 is particularly disturbing in light of the findings of previous audits reported in the 2001-02 AR, which included

- Disclosures made which were not reasonably necessary
- Information disclosed to unauthorised agencies and persons
- Information disclosed to unauthorised officers
- Failure to report to the ACA
  (page 81)

50. This evidence seriously undermines the assurances given about the safeguards that will apply to access to stored communications under the current regime.

Other issues

51. There are a number of other relevant issues, not directly canvassed in the more recent Senate Committee inquiries, on which we have comments.

Notice of interception to parties

52. We have generally taken the position that the warrants that are required for some disclosures under the TA (those under s.280(1)) provide a lesser safeguard than do TIA warrants. This is partly because the warrants for TA purposes can be issued by a wide range of magistrates and judges rather than by the senior AAT members or federal court judges required to issue a TIA warrant. It is also partly because of the less rigorous reporting and auditing requirements.

53. There is however one respect in which some warrants for TA purposes may be superior to TIA warrants. This is relation to the transparency of the process to the parties to the communication. We understand that a condition of the issue of some of the search warrants that would be used under the TA could be notification of one or both parties to the communication. This could give them an opportunity to check that the authority was properly issued and to challenge it. At the very least it would make them aware of the disclosure such that they could take whatever action they thought appropiate.

54. We acknowledge of course that there will be circumstances in which notification of the parties would prejudice the purpose of the disclosure, and in such cases it would not be appropriate. But even in these cases, there is often no compelling reason why the parties could not be informed some time after the event. US Wiretap laws contain a requirement for such notification wherever possible.

55. The Barrett review recommended either notification of persons whose calls have been intercepted (if they have not been subsequently charged) or a special register, to be monitored by the Privacy Commissioner. The draft AGs 1999 report stated that this second alternative was implemented in 1994 amendments, but in fact these amendments only provided for register to be provided to the Attorney-General. This provides an inadequate level of accountability in that there is no independent public scrutiny, and the Attorney-General, as the Minister responsible for the AFP and ACC and for law enforcement policy, has a clear conflict of interest.

56. The APF supports the first alternative recommended by Barrett - of notification. This could be subject to a 'no prejudice to ongoing investigations' test which should meet any legitimate objection from law enforcement agencies. Any suggestion that notification is undesirable because it would draw attention to the scale and incidence of interception activity should be rejected - that is a good reason for notification - having to publicly justify intrusions which have proved ineffective would be a much better deterrent against abuse than any amount of closed monitoring.

Mandatory minimum data retention periods

57. Consideration of law enforcement and national security powers to access information inevitably leads on to discussion of the availability of information – specifically the question of how long organizations keep information and how well current practices serve the needs of government agencies. There has been considerable debate about mandatory minimum retention periods – both internationally – e.g. in the context of the Council of Europe *Cybercrime Convention*, and domestically, in the context of the proposed Internet Industry Association Cybercrime Code of Practice (see http://www.iia.net.au/cybercrimecode.html).

58. We do not know if this Review intends to canvass this issue. If it does we have very strong views. National Privacy Principle 4.2 of the Privacy Act, applying to

telcos and ISPs, requires 'reasonable steps to destroy … information if it is no longer needed for any purpose for which the information maybe used or disclosed under NPP2'. But since NPP2 allows for disclosure 'required or authorized by or under law' (2.1g) and 'where reasonably necessary … for law enforcement [etc]' 2.1(h) this offers little protection.

59. If you do decide to canvass the retention issue we request an opportunity to make a further submission.

The contact-person for this submission is Nigel Waters
Phone: 02 4981 0828 and 0407 230342
E-mail: nigelwaters@iprimus.com.au

Contact Details for the Australian Privacy Foundation and its Board Members are at:
http://www.privacy.org.au/About/Contacts.html

Attachment: Telecommunications Interception: Submissions by Australian Privacy Charter Council, March 1999

See separate document