TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL 2006

Inquiry by the Senate Legal & Constitutional Committee

Submission by the Australian Privacy Foundation

CONTENTS

The Australian Privacy Foundation

1. The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. Relying entirely on volunteer effort, 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

Interception of Stored Communications (Schedule 1)

General comments

2. We note that the Telecommunications (Interception) Act (TI Act) is to be restructured to deal separately with interception of real time and stored communications respectively. We welcome the restatement of the primary focus of the Act as being to protect the privacy of communications, and the adoption of many of the recommendations of the 2005 Blunn Report.

3. We are very disappointed, however, that these amendments are being rushed through with very limited time for consideration and debate, and without the accompanying amendments to the Telecommunications Act recommended by Blunn. It makes a mockery of the thorough and considered review by Blunn, and of the thorough review of previous changes to the Telecommunications Interception regime by Senate Committees and others, to proceed with such unseemly haste. The government's timetable also displays contempt for genuine consultation on vitally important issues of rights and liberties.

4. Note that in some parts of the submission, we have abbreviated Stored Communication Interception to SCI.

Definitions – Items 2 & 3

5. We cannot see the justification for the offence thresholds for *use* of information obtained by means of a warrant to be lower than those for the initial warrant (offences carrying a penalty of one year's imprisonment/60 penalty units as opposed to 3 years imprisonment/180 penalty units). This difference is also reflected in the provisions relating to permitted dealings in accessed information (new s.139). The fact that this appears to replicate existing differences in the real-time interception regime does not in itself justify it – the case needs to be made again.

6. The penalty unit thresholds seem very low relative to the matched periods of imprisonment – 180 units is equivalent to only $19,800, which hardly seems proportionate to the concept of a 'serious contravention', whereas three years imprisonment does.

7. There is a significant 'truth in legislation' problem with the use of the new concept of 'serious contravention' (item 57 and new s.5E). We suspect that this definition will include many relatively trivial offences and breaches of civil penalty provisions, which it would be inaccurate to describe as 'serious'.

8. In order to fully assess the appropriateness of the thresholds, the Committee should require the government to provide examples of the sorts of offences that would be able to trigger a stored communications interception (SCI) warrant.

9. Is the application of the law to 'carriers' consistent with the meaning of that term under the Telecommunications Act? We understood that many ISPs, who will be the holders of many stored communications, are 'carriage service providers' rather than 'carriers' under the TA. It would be undesirable to have two different definitions of 'carrier'.

10. The requirement for a warrant will apply to communications that are 'passing over' a telecommunications system (see also Item 52). The Bill provides that a communication that is passing over a telecommunications system continues to do so until it *can be* accessed by the intended recipient of the communication (our emphasis). New section 5H makes it clear that it is the government's intention that this excludes messages that are technically accessible but not yet read (or even of which the intended recipient is unaware) from the protection of the stored communication warrant scheme

11. We have consistently argued throughout the long history of these provisions that the warrant regime protection should apply until a communication *has been* accessed by the intended recipient. There are many reasons why someone to whom an email or pager message has been sent may not access it immediately it becomes technically possible – it is one of the main attractions of stored communications that they do not require real-time presence or action. Making the threshold 'can be accessed' rather than 'has been accessed' is not a sensible distinction consistent with the intention to protect substance and content of communications with a warrant based access scheme.

12. The definition of intended recipient in new section 5G (see also Item 38) employs the concept of a communication 'addressed to a person who is an individual' It is not clear whether this means that an individual's name has to form part of the address? Many individuals use email addresses that do not contain their real name, even though it is clear to all parties that the user is an individual not a legal entity. The Bill must ensure that protection is afforded to all individuals whatever form their email address takes. The appropriate distinction is between addresses which are either obviously generic (e.g. widget@widget.com) or advertised or promoted as 'generic' (e.g. mail@widget.com or enquiries@widget.com) and all others which should be assumed to 'belong' to individuals.

13. The government needs to explain how it expects the distinction between 'individual' and 'organisational' recipients to apply to telephone numbers (used for SMS/MMS/pager messages), since there may not be any other indication of the recipient type in the communication itself. Is it intended that the distinction should relate in some way to the identity of the customer (subscriber) of the telephone service? If so this will cause difficulties where numbers/lines clearly intended for use by an individual happen to be paid for by an organisation.

14. The new section 6AA introduces the concept of 'accessing' a communication, defined in part as being 'without the knowledge' of the intended recipient (see also Item 30). This would seem to be an example of 'counter-intuitive' use of ordinary language. Most people would expect 'accessing' to include access with or without knowledge. It would be better to use clearer terminology – in this case 'covert access' would seem to accurately describe what is being regulated. (Similar comments apply to the new definition of 'access' in Item 29)

Issuing Authorities - Item 4

15. The new section 6DB allows the Minister to appoint a range of people as issuing authorities for stored communications warrants. We suggest that the threshold is far too low – part time members of the AAT and ordinary State and Territory magistrates should not carry this responsibility, even if they are legal practitioners. Restricting warrant issuing authority to judges, full time federal magistrates and full-time senior AAT members would be an important safeguard against it becoming too easy to for enforcement agencies to obtain a warrant.

16. However, we also have a generic problem with the government's ever expanding use 'volunteer' members of courts and tribunals for executive functions. The following extract from our recent submission to the Security Legislation Review Committee summarises our view.

> "The role of judges and magistrates in some of the provisions amounts to an executive role in fundamental conflict with their judicial functions. The community was told by this government in the 1990s that this conflict prevented federal court judges from issuing warrants for telecommunications interception – to justify moving that function to AAT members without the same independence (even though issuing warrants does not amount to punishment). Now it suits the government to co-opt the judiciary into an even more clearly executive role. We note that this issue has now been raised as a more general criticism of the more recent Ant-Terrorism legislation.
>
> It is misleading to describe the involvement of judges as 'judicial' since it is in many cases to be performed in their 'personal' capacity. Also, to the extent that individual judges may decline to take on this role, this further erodes the purported assurance of independence – by definition those involved will be 'volunteers' who presumably agree with the legislation, while the sceptics who might bring a more rigorous standard to bear on applications will have excluded themselves."

17. We assume that the government's intention under this Bill is to appoint federal judges and magistrates as issuing authorities in their 'personal capacity', and the Explanatory Memorandum (EM) clearly states that their agreement will be required, so our generic criticisms apply here as well.

Non-disclosure - Item 5

18. The proposed prohibition on disclosure of stored communication warrant information (new section 133) is too broad. We have also consistently argued in previous submissions on the TI regime for a requirement to notify the subjects of warrants 'after the event' when there ceases to be any immediate prospect of action or continued investigation. This notification regime applies to wiretaps in the US and is an important safeguard against abuse as well as affording individuals 'natural justice'.

New Chapter - Stored Communications interception regime - Item 9

Prohibition on access

19. New section 108 provides for imprisonment of up to two years and or a fine of up to 120 penalty units (less than $15,000). As with the offence thresholds for interception already mentioned above, we do not see these as 'equivalent' – surely a much larger maximum fine would be justified and commensurate both with the term of imprisonment and the seriousness of the offence? Given the reluctance of courts to sentence 'white collar' criminals to prison, it will be the fines that are seen as the most likely penalty, and the prospect of a fine of less than $15,000 is a grossly inadequate deterrent against actions which may well often be motivated by the prospect of significant commercial gain.

20. We note that the provision simply replicates the existing interception offence, but we have the same criticism of that. This amendment Bill provides an opportunity to remedy rather than replicate the existing defect.

Access by enforcement agencies

21. The new Part 3-3 of the Act expressly allows for a much wider range of agencies to obtain covert access to stored communications, for a much wider range of offences, and through warrants issued by a much wider range of issuing authorities. We have already criticised the latter extension under Item 4 above.

22. We are also critical of the other two extensions. Our preferred position has consistently been that there should be no difference in the regimes that apply to real time and stored communications. While we maintain this view, we accept that Parliament is likely to approve lesser protection, in the form of lower thresholds and wider access, for stored communications.

23. However, this acceptance does not extend to the breadth of access provided for in this Bill. In our view it strikes the wrong balance between protection of privacy – the acknowledged focus of the legislation, and the exceptions for other public interests.

24. The range of agencies to which, and the range of offences for which, stored communication warrants can be granted should be much more limited. Under the provisions of Part 3-3, a huge number of relatively minor agencies with criminal and even civil penalty enforcement functions will be able to apply directly for warrants.

25. The principle that invasion of privacy through covert interception should only be allowed in relation to genuinely serious offences is clearly established in the existing interception regime. In our view, no convincing case has been mounted for why a lower threshold should apply to stored communications, which can contain information just as private, sensitive and even intimate. In the absence of any such case, it is difficult to have a rational discussion about where the threshold should be set, but we strongly urge the Committee to recommend higher thresholds than those proposed.

26. As already noted above, we are concerned that the offence threshold is far too low (and misleadingly labelled as serious contravention), potentially leading to the widespread use of SCI warrants for everyday enforcement activity.

27. Even where a case can be made for a particular type of agency to have access in relation to particular classes of offence, it does not follow that direct access is appropriate. The AFP used to perform a centralised role in interception on behalf of other agencies. This has been abandoned for real-time interception (although the AFP retains a role in relation to record keeping), but we believe a partially centralised approach would be appropriate at least access for by agencies outside the group authorised to intercept real-time communications.

28. Under this model, those agencies which have established processes for obtaining authorisation and intercepting real-time communications could use these processes for stored communications interception as well, but any other agencies authorised to obtain SC interception warrants ('SCI-only' agencies) would have the warrants executed through a central agency with appropriate expertise and resources.

29. The prospect of hundreds of agencies having relatively infrequent contact with hundreds of carriers and ISPs over something as sensitive as communications interception is a recipe for disaster. It is difficult enough to ensure appropriate security, discretion, and competence in the existing regime – the 'free for all' likely under the legislation as drafted will inevitably lead to lapses, with potentially serious consequences not only for individuals but for the security of law enforcement investigations.

30. New section 110 allows for Chief Executives of 'SCI-only' agencies to nominate anyone to apply for warrants. In our view this power of delegation must at least be restricted to an employee of sufficient seniority to be held properly accountable.

31. Otherwise the procedural provisions seem appropriate. We particularly welcome the duty of the issuing authority to satisfy itself that the information to be obtained would be likely to assist in the investigation of a serious contravention, and the express inclusion of privacy impact as a consideration for the issuing authority alongside the gravity of the serious contravention, the likely value of the information that could be obtained and a comparison of other methods of investigation (all in nw s.116).

32. We note that new s.117 provides for SCI warrants to have retrospective effect i.e. to authorise access to communications sent before the warrant was issued but still held by the (carrier).

33. The provisions in new s.119 for time limits seem appropriate – we particularly welcome the limitation that a warrant expires once it has been executed i.e. the regime only permits a 'snapshot' of information held at a particular moment in time, and not continuing surveillance, which would undermine the separate and more restricted real-time interception regime.

34. We also welcome the provision in new s.122(1) of the ability for an enforcement agency to revoke a warrant with which it has been issued – this provides enforcement

agencies with the means to prevent access to stored communications where they become aware that such access would not assist the investigation.

35. We note that new s.124 ensures that a stored communications warrant may be authority to access all of the stored communications pertaining to a person and held by a particular carrier, even where the communications are in relation to a telecommunications service which the enforcement agency was unaware of the person's use at the time the warrant was executed. This appears to give all stored communications warrants the same effect as a 'named person' warrant under the real-time interception regime. We suggest that the same distinction between 'service' and 'named person' communications should be made for stored communications as for real-time communications, with stricter conditions applying to the latter, which are inherently more intrusive.

Destruction of records

36. We welcome the provision for destruction of records in new s.150. This brings Commonwealth agencies, otherwise subject to the Privacy Act IPPs (which are silent on retention) in line with the more recent private sector NPPs, and the requirement will also apply to state and territory agencies, whether or not they are subject to any equivalent principle in their own privacy laws. The requirement for an annual report on destruction (new s.150(2)) is valuable but would more effectively serve an accountability function if the reports are made public.

Records and monitoring

37. We are concerned that the record keeping and reporting requirements are expressly less detailed than the equivalent requirements in relation to real-time communication interception. For the reasons already set out, we believe that the large number of less regular users of the SCI regime justifies at least as rigorous if not greater accountability mechanisms.

38. The monitoring and inspection regime proposed appears to mirror that under the existing Act, with roles for both the Commonwealth and State and Territory Ombudsmen. We note that their functions are limited to review of procedural compliance and do not extend to the merits of the applications for interception (which are left to the issuing authorities).

39. We suggest that, without setting up merits review of the applications for warrants, the Commonwealth Ombudsman's functions could be extended to enquire, at his or her discretion, into the overall operation of the interception regime.

40. We note that the Privacy Commissioner, as well as her jurisdiction over compliance by all Commonwealth agencies with the Privacy Act IPPs, remains responsible for auditing the records kept under the access to call record provisions of the Telecommunications Act. There would seem to be some merit in integrating these parallel and related functions. Consideration was given in a previous round of reviews to transferring the Interception Act monitoring functions to the Privacy Commissioner. A sensible and considered response to the Blunn report could have invited submissions on the pros and cons of this suggestion. But there should at least be some attention to the relationship between these two sets of related functions.

41. The requirements in new ss.161-164 for a detailed annual report by the Attorney-General on the operation of the SCI regime are welcome.

Secrecy and access - Item 20

42. We note the exemption for SCI warrant information from access under the FOI Act, which is obviously appropriate while investigations are still in progress, but re-iterate our suggestion of a post-facto notification requirement (see under item 5 above).

Interception of 'B-party' communications (Schedule 2)

43. These proposed amendments appear to have come 'out of the blue', without any previous evidence of need having been adduced even in the many Interception reviews, including last year's Blunn report.

44. We think it is inapppopriate for these amendments to be rushed through as part of this package and we urge the Committee to recommend that they be deferred pending more detailed justification and a longer period of consultation.

45. Our provisional concerns about these provisions are as follows.

46. The concept of interception of the communications of persons not suspected of any wrongdoing is radical and poses a significant threat to the presumption of innocence. The EM admits that

> "B-Party interception inherently involves a potential for greater privacy intrusion of persons who may not be involved in the commission of an offence."

47. We suggest that the arguments in favour of this radical departure, and the balance of interests, may be more convincing in relation to national security activities of ASIO (using Part III warrants) than in relation to the wide range of other offences for which Part VI interception warrants can be sought by other enforcement agencies.

48. We suggest that the Committee consider the desirability of severing the provisions relating to B-party interception under Part III and Part VI respectively, and considering separately the merits of each.

49. We note that the considerations for issuing authorities are different (more stringent) and the period of validity of warrants are shorter, for proposed B-party interception. While these are desirable safeguards if B-party interception is eventually accepted, but we do not see them as replacing the need for a much deeper debate about this radical departure from the basis of the existing regime.

Equipment-Based interception (Schedule 3)

50. It is not clear to us, even with the help of the EM, how the provision for named person warrants in respect of 'telecommunications devices' would work, or assist enforcement agencies. Interception is by definition of the use of a 'service', and we are not aware that the carrier or carriage service provider would necessarily have any information that identified the particular device being used by an individual to access a service, even if the enforcement agency did.

51. If this is not the case, the Committee should require a much clearer explanation as to how equipment-based interception would operate, particularly in view of the likelihood that particular devices may well be used by third parties other than persons of interest, including those about whom there are no grounds for suspicion.

52. Equipment-based interception would appear to open up the prospect of considerable 'collateral' intrusion into the privacy of innocent third parties, and the Committee should consider very seriously whether the alleged benefits outweigh this privacy intrusion, again by reference to the agreed primary objective of the Interception legislation.

53. Item 20 of this Schedule amends the Act to requires the issuing authority to have regard to the interference with the privacy of the person that will be caused by authorising the interception of the person of interest's telecommunications services or telecommunications devices. We suggest that *if* equipment-based interception was allowed, then the issuing authority must also be required to have regard to the privacy of *third parties* likely to use the device. This would be consistent with the considerations for issuing telephone service interception and stored communication interception warrants, which refer to the "privacy of any person or persons" (e.g. new section 116(2)). This wording could be used to ensure consistency and equivalent protection.

Class 1 & Class 2 Offences (Schedule 4)

54. We have no objection in principle to these changes, and welcome the effect that the issuing authorities for *all* interception warrants will need to have regard to privacy considerations – an advance on the present position.

Transfer of functions (Schedule 5)

55. We support the removal of the TIRAC function and transfer of the registration and record keeping functions previously carried out by the AFP to the Attorney-General's Department.

56. We do however suggest that the General and Special Registers of Warrants be reviewed quarterly not just by the Attorney-General, who has a conflict of interest, but also by an independent body such as the Ombudsman or Privacy Commissioner (see above for discussion of this generic issue). The proposed amendments would remove the current role of the Ombudsman in inspecting the AFP registers, thereby reducing accountability.

Other amendments (Schedule 6)

Participant Monitoring - repeal of s.6(2) - Items 5 & 6

57. We strongly support the repeal of this section, which has been interpreted by some businesses in a way that subverts the Act's requirements, when a call is being monitored or recorded by one party, for notification of the other party.

58. We have recently been campaigning for clarification of the legal position in relation to 'participant monitoring'. The government's view about the intention of the legislation was clearly set out in the revised Guideline issued by the Australian Communications Industry Forum (ACIF) in 2005, but some businesses are known to have received legal advice that s.6(2) allows for monitoring without notice.

59. Repeal of s.6(2), which is no longer needed for its original purpose of allowing monitoring by employees of telecommunications carriers, will remove the uncertainty and allow the ACIF Guidelines to be promoted more vigorously.

Contact for this submission

Nigel Waters, Policy Coordinator
E-mail: enquiries@privacy.org.au
APF Web site: http://www.privacy.org.au