SUPPLEMENTARY REPORT WITH ADDITIONAL COMMENTS OF DISSENT BY THE AUSTRALIAN DEMOCRATS

1.1 The Democrats agree with a majority of the recommendations presented in the Chair's report.

1.2 We note the majority of submissions desire a single comprehensive legislative regime dealing with access to telecommunications information.

1.3 The Democrats note this Bill amends the *Telecommunications (Interception) Act 1979* to implement further recommendations from the August 2005 *Review of the Regulation of Access to Communications* by Anthony Blunn AO (the Blunn Review).

1.4 We believe the Bill, as introduced, does not adequately account for privacy considerations.

1.5 The operation of the Bill is in conjunction with other legislation which further reduces fundamental civil liberties of Australian citizens.

1.6 We believe a majority of the recommendations contained in the Chair's report will improve the Bill and lessen the potential for abuses of privacy but provide the following additions:

Definition of enforcement agency

1.7 The legislation gives enormous powers to law enforcement agencies to listen to the private conversations of Australians.

1.8 The Democrats believe that the definition of 'law enforcement agency' is too broad.

1.9 In particular we share the concerns raised in the inquiry that the Bill will grant new powers to the CrimTrac Agency to apply for stored communications warrants and to issue authorisations for access to historical 'telecommunications data'.

1.10 As Electronic Frontiers Australia state in their submission, CrimTrac is not a law enforcement agency authorised to conduct investigations into suspected offences except in limited circumstances related to spent conviction legislation.[1]

1.11 While we note the Department has stated that CrimTrac's functions do not include the investigation of any offences and therefore they will be ineligible to be issued with a stored communications warrant,[2] CrimTrac's functions could just as easily be expanded. We note that, in addition to providing criminal history checks, CrimTrac's functions have already been expanded into the area of DNA samples.

---

[1] Electronic Frontiers Australia, *Submission 6*, pp 4-5.

[2] *Committee Hansard*, 16 July, p. 10.

1.12 The Democrats do not consider, at this time, it is appropriate for CrimTrac to be included in the definition of a law enforcement agency.

Recommendation 1

1.13 The Democrats support the removal of CrimTrac from the definition of 'enforcement agency'.

Convergent technologies

1.14 There is a need to consider how best to respond to the fact that current and emerging communications technologies have resulted in a convergence of areas that have traditionally been separately regulated by federal or state government laws.

1.15 During the course of this inquiry various examples of converging technologies were discussed including, web browsing, downloading from the internet, entering chat rooms, sharing emails, taking digital photographs and video footage and playing MP3 files all from a mobile telephone. Questions were raised as to what information captured can properly be considered telecommunications data.

1.16 The best way to deal with these new technologies is to give certainty as to whether or not the information they produce can be categorised as telecommunications data. This is something which the Attorney-General's Department appears reluctant to do.

1.17 The Attorney-General's Department has stated that they are 'concerned about defining technology and call associated data now because the definition might be redundant in 12 months time'.[3] The Democrats are dissatisfied with this reason.

1.18 As a matter of public policy, it is desirable to clarify what is meant by telecommunications data now. If in a certain time period, albeit 6 or 18 months, that definition needs amending then this can occur. The absence of a clear definition should not be justified by an assertion that this will allow the law to remain current with technology.

1.19 With advances in technology it is important to clarify the scope of telecommunications data to reassure current and future users of new technologies that such communications may or may not be intercepted.

Recommendation 2

1.20 The Democrats will be amending any future Bill to define telecommunication data. The definition of telecommunications data will balance a desire to be technology neutral with a desire to protect certain citizen's lawful activities from disclosure to enforcement agencies

[3] *Committee Hansard*, 16 July 2007, p. 22.

Location Information

1.21 Location and identity are fundamental characteristics of telecommunications data. Location requires measurement. Identity requires classification and definition.

1.22 A by-product of locating a mobile telephone is the ability to locate with precision people. The Democrats acknowledge that this is a by-product, not an aim, of most telecommunications data collection. But it is a by-product that as the Law Council has noted in its submission which requires greater controls.[4]

1.23 Tom Wright, Information and Privacy Commissioner for Ontario, Canada, considered that location can:

> in essence become a personal identifier because geographical information systems technology enables the synthesis and analysis of information not possible with other information management systems. It can construct a very detailed picture of an individual's life, even without the use of their name, just by collecting and analysing data related to a specific location.[5]

1.24 The Democrats recommend that a person's mobile telephone phone should not be used as a surrogate tracking and tracing technology for people in the absence of any countervailing public interest, significant independent oversight and public reporting.

1.25 We favour access to location information only through a warrant.

Recommendation 3

1.26 The Democrats will be amending the Bill to ensure that real time data, in other words location information, can only be accessed by enforcement agencies with a warrant.

Time periods

1.27 As noted above, the Democrats believe in a requirement to allow mobile telephone location information to be disclosed under a warrant.

1.28 However, if this is not accepted by the government, then the Bill will allow mobile telephone location information to be disclosed under a written authorisation for a period of 45 or 90 days without the need to obtain a warrant.

1.29 The Democrats consider this time frame is excessive and should be limited.

Recommendation 4

1.30 Written authorisations to access mobile telephone location information should be limited to 14 days duration and should not be renewable unless during that 14 days information material to the investigation has been obtained which

---

[4] Law Council of Australia, *Submission 20*, p. 6.

[5] Tom Wright, *Geographic Information Systems*, at http://www.ipc.on.ca/english/pubpres/papers/gis.htm (accessed 31 July 2007).

suggests that continued interception would likely result in further material information. The duration of a renewed warrant should not exceed 20 days.

Public Interest Monitor

1.31 This Bill creates a new two tier access regime. The first tier encompasses the traditional access to existing telecommunications data. The second tier allows for access to future telecommunications data. The Bill also creates new controls over the existing access framework.

1.32 The Democrats view this Bill as a widening of the Commonwealth phone-tapping powers. As such it is appropriate that there be an independent umpire to balance necessary, lawful, and proportionate access by law enforcement agencies to telecommunications data with the public's right to communicate free from surveillance.

1.33 The Democrats note that in relation to the area of listening devices, a model can be found in Queensland, where a Public Interest Monitor is authorised under the *Police Powers and Responsibilities Act 2000* (Qld) to intervene in applications for listening devices warrants, and to monitor and report on the use and effectiveness of the warrants.

1.34 Queensland Premier Peter Beattie has also prepared telephone interception legislation to include a Public Interest Monitor.

1.35 The Democrats see merit in adopting the Queensland public interest monitor model to improve accountability.

Recommendation 5

1.36 The Democrats will amend the legislation to require enforcement agencies consult with the Public Interest Monitor (PIM) before they apply for an authorisation under the TIA Act.

Collection of telecommunications data which is necessary

1.37 Proposed sections 174 and 177 concern voluntary disclosures of telecommunications data to ASIO and enforcement agencies by employees of a carrier or carriage service provider.

1.38 The Democrats are concerned that an employee of a carrier or carriage service provider may volunteer more personal information than is necessary for ASIO and enforcement agencies to perform their functions. The reality is that employees of a carrier or carriage service provider when faced with a request or warrant from ASIO or an enforcement agency will be overly cooperative.

Recommendation 6

1.39 The Democrats propose that there be a positive obligation on the part of ASIO and the enforcement agency, where they suspect or have actual knowledge

that an employee of a carrier is volunteering personal information, to warn that employee that they are not legally obliged to disclose telecommunications data.

Conclusion

1.40 This Bill confirms privacy as a valued norm but does not do enough to protect Australians' private conversations and communications.

1.41 While legitimate law enforcement activities may in exceptional circumstances override a right to privacy the increasingly complex telecommunications environment exposes individuals to arbitrary interference.

1.42 The Democrats will be moving a number of amendments to this Bill to ensure there are greater protections afforded for telecommunications data.

Senator Stott Despoja
Australian Democrats