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 commend the Chair and the Secretariat for their efforts.

1.3 The Democrats recognise the importance of the review of the regulation of access to communications carried out by Mr Anthony Blunn AO and agree that it is necessary that amendments be made to the current outdated *Telecommunications (Interception) Act 1979* in order to maintain its technological relevance.

1.4 We note with dismay the lack of time that the committee has been allocated to report on this bill. The ability of members of the general public to make submissions and Senators to report to the Parliament is constrained when there is inadequate amount of time to consider a Bill.

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

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

1.7 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:

Stored Communications Warrants – Schedule 1

1.8 The Democrats recognise the necessity for a stored communications warrant regime to be introduced in order to maintain the ability of enforcement agencies to efficiently combat crime.

1.9 We believe that the balance between the privacy rights of Australians and the need for enforcement agencies to carry out their duties efficiently is disproportionate in the current format of the bill to the detriment of privacy rights.

1.10 A matter of concern for the Democrats is the differing thresholds for interception warrants and stored communications warrants.

1.11 During the inquiry, I asked the Attorney-General's Department about the rationale for the differing thresholds for stored communications and interception warrants. The notion that e-mails and SMS' are more considered than a live communication was stated by the Department;

> "It is something that is in writing – something that definitely involves more consideration of the expression – although there is the speed issue."[1]

This rationale is unconvincing. In response to this claim, Professor Williams argued;

> "It strikes me as nonsensical that a differentiation would be drawn between speaking to somebody on a mobile phone and sending them an SMS message. Many of the students who I teach today see them as equivalent forms of communications. It makes no sense as a matter of law or public policy why, indeed, it is easier to gain one type of information than the other … I think the proper focus for assessing this legislation is: what is the appropriate limitation upon the privacy of Australian people? For them there is no rational distinction, so I cannot see how you could justify one from the government's end."[2]

1.12 I note statements made earlier in the year by NSW Council of Civil Liberties Chair Mr Cameron Murphy regarding comparisons of Telecommunication Intercepts between Australia and the United States where he highlighted the councils concerns:

> "Recently released figures show that telephone wiretapping by government agencies in Australia (including the police) continues to grow. Not only does Australia issue 75% more telecommunications interception warrants than the US, but per capita Australia issues 26 times more warrants than the US. In Australia non-judges issue 76% of all warrants, whereas in the US only judges can issue warrants.
>
> In the twelve months 2003/2004 there were 3028 warrants issued in Australia. In the twelve months of 2004, US courts issued 1710 warrants. Adjusting for population, Australia intercepts telephone communications 26 times more per capita than the United States.
>
> Worryingly, the numbers are way up on figures only two years ago. In 2001 there were more than 2150 warrants issued in Australia, compared with only 1490 warrants issued in the United States of America. Australia intercepted telephone communications 20 times more per capita than the United States."[3]

1.13 The Democrats see these overwhelming numbers as an indication that the current methods of oversight are not functioning properly.

1.14 The Democrats support the recommendation made by the Chair to review the suitability and effectiveness of the AAT in warrant issuing regime.

1.15 In order to address these deficiencies we make the following recommendations;

Recommendation 1

1.16 That the threshold for stored communications warrants, that being for investigations into offences with penalties of at least a maximum of three years,

---

[1] *Committee Hansard*, Wednesday, 15 March 2006, p. 39.

[2] *Committee Hansard*, Wednesday, 15 March 2006, pp. 28 and 31.

[3] NSW Council for Civil Liberties, 'Australia phones 26-times more likely to be bugged than an American phone', *media release*, 13 January 2006.

be replaced by the same threshold as that for telecommunication interception warrants.

Recommendation 2

1.17 That more information be required of agencies requesting a stored communication warrant. This information should include the number of previous applications the agency has made with respect to the person or the service the person has used, the number of warrants previously issued and the date on which the most recent was issued and particulars of the use made by the agency of information obtained by access under such warrants.

Recommendation 3

1.18 That the individuals on whom a stored communications warrant has been exercised be notified of the existence of the warrant where that disclosure will not materially affect the investigation. Where it is considered that such disclosure will materially affect the investigation, there exists an obligation on the Chief Officer of the agency to inform the person on whom the warrant was exercised as soon as that disclosure is considered to no longer materially affect the investigation.

B-Party Warrants – Schedule 2

1.19 The operation of B-party warrants represents a serious breach of privacy as they are targeted at non-suspected persons. We believe that the operation of B-Party warrants as they are contained in the Bill can not be justified.

1.20 As the Victorian Privacy Commissioner stated;

> "Telecommunications is one of the common means by which many individuals discuss their most private and intimate thoughts, as well as the ordinary daily details of their lives. They may also engage in political discourse, discuss business ventures, seek legal and other professional advice. People have a legitimate and reasonable expectation that the State will not listen surreptitiously to these conversations. Accordingly, any such interception has been subject to strict regulation under law, with oversight."[4]

1.21 The Democrats welcome the recommendations made in the Chair's report, however, we believe that the recommendations are not sufficient to ensure the privacy rights of Australian citizens.

1.22 During the inquiry, I asked a number of the witnesses for their opinion on how this Bill may operate in conjunction with other legislation to affect the civil liberties of Australian Citizens. Dr Bibby of the New South Wales Council for Civil Liberties stated;

---

[4] Office of the Victorian Privacy Commissioner, *Submission to the Commonwealth Parliament's Senate Legal and Constitutional Committee on its inquiry into the Provision of the Telecommunication (Interception) Bill 2004*, 12 March 2004.

> "As soon as you give powers to organisations to take away liberty in the way that the two antiterrorism laws and the powers that were given to ASIO a few years ago have done, you open up the possibility of it being done for totally spurious reasons. The more you allow privacy to be invaded, and the more you allow the stuff to be kept secret, the greater the chances are that these powers will be misused – and misused in ways which it is impossible for people to correct."[5]

1.23 The President of the New South Wales Council for Civil Liberties Mr Cameron Murphy remarked that;

> "We are seeing both the public and the parliament becoming desensitised to the nature of the extraordinary powers that are being sought. Instead of just being used to get us over a period in which there might be a drastic and imminent threat, it is becoming the norm, and those powers are being extended to many other agencies."[6]

1.24 The Democrats note this statement with alarm.

1.25 We believe that the Bill does not adequately consider the importance of professional privilege and note that where this privilege is abrogated it erodes the ability of lawyers, medical officers, parliamentarians and religious leaders to offer their services in confidence.

1.26 Despite arguments submitted by the Attorney-General's Department that there has been precedent established in *Carmody v MacKellar& Orrs* [1996] 791 FCA 1, which allows for the abrogation of legal professional privilege, we are not convinced that this should be applied by analogy to justify the interception of telecommunications to non-suspected third persons.

1.27 We believe that professional privilege should be protected from interception not only for the reason that non-suspected persons should not have their privacy infringed upon but also for reasons of public policy. It is crucial that Australian citizens can be assured that whatever information is given in confidence to a lawyer, religious leader or medical officer remains in confidence.

1.28 Evidence has been produced to persuade the Parliament that B-Party warrants are necessary in the prevention of crime and terrorism as criminals are evolving with technology and continuing to use it to their advantage to avoid detection and prosecution.

1.29 ASIO's ability to use B-party warrants is of concern to the Democrats as the criteria to obtain a warrant for the organisation operates at a very low threshold. Professor George Williams in his submission to the inquiry stated;

> "B-party warrants may be issued even if there is no evidence that the warrant will assist in obtaining information relevant to the activities which triggered the warrant. It is enough to show that intercepting B-party communications to or from *anyone* may assist in obtaining *any* intelligence related to security.

---

[5] *Committee Hansard*, Wednesday, 15 March 2006, p. 57.

[6] *Committee Hansard*, Wednesday, 15 March 2006, p. 57.

> Once it is shown that the person involved in activities prejudicial to security communicates with the B-party, the Director General must only discharge the very low burden that the interception will be likely to assist in obtaining intelligence related to security. 'Likely to assist' is a very broad standard. Further, the concept of 'relating to security' is both wide and vague, particularly since 'security' has the same wide meaning as that given in section 4 of the *Australian Security Intelligence Organisation Act 1979* (Cth)."[7]

1.30 The Democrats are of the belief that it is in only very remote circumstances where the use of a B-Party warrant may assist intelligence and enforcement agencies in a manner which would be otherwise unavailable to them.

1.31 For this reason, it is crucial that a high threshold be required in the issuing of a B-Party warrant. Any warrant issued should meet the following list of recommendations at a minimum.

Recommendation 4

1.32 The same requirements that apply to the AFP for a B-party warrant should also apply to ASIO.

Recommendation 5

1.33 The use of such warrants should only be authorised by a Judge on the Federal Court of Australia, the Family Court of Australia or on the Federal Magistrates Court.

Recommendation 6

1.34 Warrants should be limited to fourteen days duration and should not be renewable unless during that fourteen days information material to the investigation had been obtained and suggested that continued interception would likely result in further material information. The duration of a renewed warrant should not exceed 30 days.

Recommendation 7

1.35 An issuing authority must under no circumstances grant a B-Party warrant where the warrant is likely to breach professional privilege. Any agency applying for a B-Party warrant must state in an affidavit that they are of the belief that the B-party is not privy to professional privilege.

Recommendation 8

1.36 The B-Party must be informed about the operation of the warrant after it has been exercised. The Chief Officer of the authorised agency may use their discretion to delay the disclosure where such disclosure may materially affect the success of the investigation. Where disclosure will not materially affect the success of the case the Chief Officer is required to inform the B-Party of the existence of the warrant as soon as possible.

---

[7] *Submission 2*, p. 2.

Recommendation 9

1.37 No copies of recordings should be made before the review of the original recording. Where it is apparent that the interception does not involve the suspected person the recording should be immediately destroyed.

Recommendation 10

1.38 The destruction provisions of the act should be amended to mirror those contained in the *Surveillance Devices Act 2005.*

Equipment Based Warrants – Schedule 3

1.39 The section of the Bill that relates to equipment based warrants has led to much confusion as to the scope of its operation.

1.40 During the inquiry, I asked the Office of the Privacy Commissioner about their submission which stated;

> "The office has not yet been able to fully determine the limits to the scope of the operation of schedule 3."[8]

In response Mr Timothy Pilgrim, Deputy Privacy Commissioner stated

> "…it is an issue that we have been grappling with and, given our time to be able to devote to issues such as this, have not been able to fully explore…What we are not able to grapple with – or have not had time to grapple with – is how that might be broadly applied in various scenarios."[9]

1.41 Electronic Frontiers Australia in its submission stated that;

> "This proposal appears to have an inappropriately and unjustifiably high potential to result in interception of communications of persons who are not suspects (i.e. are not named in the warrant) because, among other things, the types of device numbers proposed to be used do not necessarily uniquely identify a particular device.[10]

1.42 The Democrats note that the Blunn report did not recommend the introduction of equipment based warrants. Rather the report recommended that "priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access."[11] Discussion in the report highlights the difficulties of accurately identifying a person through the use of International Mobile Service Identifiers (IMSI) or similar identification numbers.

---

[8] *Submission 6,* p. 3.

[9] *Committee Hansard,* Wednesday, 15 March 2006, p. 25.

[10] *Submission 3,* p. 29.

[11] Anthony Blunn AO 'Report of the Review of the Regulation of Access to Communications' August 2005

1.43 The Democrats believe that the operation of schedule 3 of the Bill in its current form is untenable and needs to be referred for further consideration.

Recommendation 11

1.44 Schedule 3 of the bill should be removed from the Bill and referred back to the committee until such time as it is possible to determine the full scope of its operation.

Senator Stott Despoja
Australian Democrats