Law Council
OF AUSTRALIA

Telecommunications (Interception) Amendment Bill 2006

Senate Legal and Constitutional Legislation Committee

13 March 2006

GPO Box 1989, Canberra,
ACT 2601, DX 5719 Canberra

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

19 Torrens St Braddon ACT 2612
www.lawcouncil.asn.au

Table of Contents

Recommendations

1. The Law Council of Australia urges the government to abandon proposals to allow telecommunications surveillance on innocent people. Persons not suspected of crimes should not be subjected by the State to surveillance. This proposal abrogates fundamental freedoms and human rights of people not suspected of any crime or wrong doing.

2. While the Law Council opposes measures in schedule 2 of the Bill, if these measures are endorsed by the Senate Legal and Constitutional Legislation Committee ("the Committee"), the Law Council strongly urges the Committee to ensure that they are accompanied by proper legal safeguards and protections including the following:

    a. Guidelines clarifying the scope of who can be monitored as a B-Party. For instance, factors including frequency of contact should be expressly stated in legislation;

    b. If the intention is that Schedule 2 should apply as a last resort, the interception warrant should only be available for investigations of very serious offences, for instance, some of the offences contained in the current classification of Class 1 Offences in the Act, eg. murder and terrorist offences;

    c. The Law Council has serious concerns in extending the power of the Attorney General to issue telecommunication interception warrants in respect of innocent third parties. Issuing warrants against innocent parties are a serious intrusion into human rights and require judicial oversight. The seriousness of taking away a person's liberty combined with the inability of the person to detect the intrusion and therefore challenge the State's action, warrants a person faced with this prospect to be accorded fair and balanced treatment from an independent judicial officer. This approach will also minimise issues in relation to an abuse of power, as unchecked powers can provide an irresistible temptation for abuse.

    d. Rolling telecommunications interception warrants should not be permitted unless there are exceptional circumstances. For instance, where a higher threshold is satisfied including where crucial information was obtained under an earlier interception warrant;

    e. Similar to other legislation which erode fundamental rights of the Australian people, schedule 2 should be subject to independent review, for instance, 2 or 3 years after its commencement;

    f. A sunset clause should be incorporated in the Act consistent with other legislation which erodes fundamental human rights, such as the recent Anti-Terrorism Act 2005;

    g. The measures should contain express exemption categories. Exempt communications should include the confidential communications with lawyers, doctors and the clergy;

h. The proposed measures should expressly provide that Schedule 2 does not abrogate Legal Professional Privilege;

i. Each year, the government should be required to report specific details including the:

   i. number of applications by agency for interception warrants to the Attorney General, judicial officers and Nominated AAT member; and

   ii. the number of warrants issued by the Attorney General, judicial officers and Nominated AAT member pursuant to schedule 2;

   iii. The grounds upon which they were issued;

   iv. The safeguards in place to prevent abuse.

j. Parliament should disclose to the public, the potential impact of these laws on fundamental human rights and the justifications they see for it.

Introduction

3. The Telecommunications (Interception) Amendment Bill 2006 ("t**he Bill**") was introduced in the House of Representatives on 16 February 2006. The Bill purports to implement certain recommendations which were made in the Blunn Report[1] in relation to the review of the regulation of access to communications under the *Telecommunications (Interception) Act* 1979 (the Act).

4. The Law Council continues to be critical of the Federal Government's failure to properly and fairly consult the Australian people on these proposed laws.

5. On 1 March 2006, the Senate referred the Telecommunications (Interception) Amendment Bill 2006 to the Senate Legal and Constitutional Committee for inquiry and report by 27 March 2006. Submissions on the Bill were called in which the community was provided with seven days to respond. Subsequently, three days notice was given on to interested members of the community including the Law Council to give evidence at the public hearings to be held on 15 March.

6. In the context of the Bill, it is particularly important to provide reasonable time for consultation to ensure that the government can properly consider concerns of the Australian community and to achieve an appropriate balance between safeguarding fundamental human rights and the "threat to the Australian people".

7. As stated in previous submissions, the lack of consultation undermines trust in parliamentary democracy and in particular the presumption that parliamentarians will act fairly and with decency. The Law Council reminds the government that to ignore Australia's strong democratic traditions will place at risk public confidence in the Parliament and the rule of law.

[1] Available at: http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~xBlunn+Report+13+Sept.doc/$file/xBlunn+Report+13+Sept.doc

8. Due to the limited time provided to review the Bill, the Law Council submission has raised some serious issues and concerns with respect to the controversial measures contained in Schedule 2 of the Bill – B Party Interception.

Schedule 2 of the Bill - B-Party Interception

9. The Law Council strenuously opposes the proposed measures in schedule 2 of the Bill and urges the Committee to recommend that the proposal to expand the powers of certain law enforcement agencies and Australian Security Intelligence Organisation ("ASIO") to monitor the telecommunications of innocent third parties who are not suspected of involvement in a crime, to be abandoned.

10. According to schedule 2, a telecommunication interception warrant may be sought where a third party (a "B-Party") "sends communication from or to another person who is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, such activities".[2]

11. Consistent with the Act, an interception warrant will be able to be issued by the Attorney General, a judge or a nominated AAT member.

12. An interception warrant will be available for investigations of offences punishable by a maximum period of at least 7 years and where the issuing authority is satisfied that:

    a. there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the telecommunications service; and

    b. information that would be obtained by interception is likely to assist with the investigation; and

    c. the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the suspect.

13. Where these tests are satisfied, the certain law enforcement agencies would be able to intercept telecommunications under a warrant for 45 days and ASIO for 90 days.

Issues

Breach of Privacy

14. The right to privacy is a fundamental human right guaranteed under the International Covenant on Civil and Political Rights 1966 and other international instruments and is entrenched in Australian legislation including the *Privacy Act* 1988 and legislation in the states and territories.

15. Article 17 of the International Covenant on Civil and Political Rights 1966 ("ICCPR"), to which Australia is a party, declares:

[2] Proposed section **9(1)(a)(i)**(ia) of the *Telecommunications (Interception) Act* 1979

a. No one shall be subjected to arbitrary or unlawful interference with his privacy,family, home or correspondence, nor to unlawful attacks on his honour and reputation.

b. Everyone has the right to the protection of the law against such interference or attacks.

16. The Law Council submits that schedule 2 of the Bill breaches Article 17 of the ICCPR.

17. Schedule 2 of the Bill if enacted allows certain law enforcement agencies and ASIO to intercept telecommunications of a person who has no knowledge or involvement in a crime, but who may be in contact with someone who does. In other words, people suspected of nothing will be under surveillance.

18. This is the first time ever in Australia's history that law enforcement agencies will be given power to intercept telecommunications of people who are not suspects, who are innocent people.

19. As Paul Chadwick, the Victorian Privacy Commissioner said,

> "Telecommunication 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."[3]

20. In view of such considerations, the *Telecommunication Interception Act* 1979 was enacted with the following object:

> "An Act to prohibit the interception of communications except where authorised in special circumstances or for the purpose of tracing locations of callers in emergencies and for related purposes".[4]

Lack of Proper Limits and Controls

21. Currently, telecommunications interception is directed at persons suspected of being involved in crimes. The implication of extending the law in relation to interception warrants to apply to innocent third parties is that all Australians may potentially be targeted. This defeats the express intention of the *Telecommunications Interception Act* 1979.

22. The Law Council submits that consideration must be given to the manner in which these new provisions would work and who would be targeted.

23. The test that would be applied under the Act is in relation to "a person who sends communication from or to a suspect."[5] The nature of the communication is not specified nor is the method by which law enforcement discovers that the

---

[3] 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) Amendment Bill 2004*, 12 March 2004, page 2.
[4] the Preamble in the *Telecommunications Interception Act* 1979
[5] Proposed section **9(1)(a)(i)**(ia) of the *Telecommunications (Interception) Act* 1979

communication occurred. This can be, and would likely be innocent communication and have nothing to do with the commission of a crime.

24. Monitoring would likely begin with the family of the suspect. Then perhaps the members of the suspect's religious group might be monitored. Perhaps the teachers at the suspect's children's school would be monitored. It is likely that communications of co-workers of the suspect would be monitored as would the communications of the professionals serving the suspect. This includes all of the communications of his or her lawyer, doctor, and clergy. People with whom the suspect comes into contact regardless of whether contact occurs rarely, occasionally, or frequently can be subject to telecommunication interception. In this respect, schedule 2 requires clarification.

Potential Impact on Confidential Communications and Legal Professional Privilege

25. The Law Council is seriously concerned about the use of telecommunications interception warrants in relation to confidential communications including with respect to lawyers, doctors and priests. There needs to be constraints placed on the application of such interception warrants particularly in this regard.

26. This broad power to monitor telecommunications of third parties brings into question the status of the confidential relationships between a doctor and patient, and between clergy and parishioner and lawyer and client. The information contained in these professionals' communication is confidential to their clients, patients, and parishioners. These professionals are highly regulated. If it is believed that monitoring their communications would be productive, it is likely a monitoring warrant them as named persons could be obtained.

27. It is unclear whether legal professional privilege is abrogated by Schedule 2 of the Bill. The Full High Court in *Baker v Campbell*[6] stated that in the absence of some legislative provision restricting its application, the doctrine of legal professional privilege applies to all forms of compulsory disclosure of evidence. While an assumption may be made, the Law Council submits that it would be in the interests of good public policy to expressly provide that schedule 2 does not override legal professional privilege.

28. The suspect thus becomes the pebble in the pond. Law enforcement agencies could be in a position of monitoring every person around the suspect, but not the suspect on the basis that there are "no practicable methods of identifying the telecommunications used…by the person involved in the offence…"

Lack of Proper Legal Safeguards

29. Mr Blunn in his report ("the Blunn Report") said the following in relation to B-Party intercepts[7]:

    a. Security and law enforcement agencies argue the need to intercept B-Party communications more widely. However there are obvious and serious privacy implications involved. That said the usefulness of such intercepts in appropriate circumstances is equally obvious.

[6] (1983) 153 CLR 52; 49 ALR 385
[7] Anthony S Blunn AO, *Rep ort of the Review of the Regulation of Access to Communications*, Commonwealth of Australia, August 2005.

b. In my opinion the proposition that there are circumstances which warrant B-Party intercepts is convincing but the privacy implications are such that those intercepts should not depend on non-judicial interpretation of the relevant sections, the meaning of which is certainly open to argument.

c. What in my view must be prevented is using B-Party intercepts as 'fishing expeditions'.

d. Appropriate controls might include a requirement that any agency requesting such a warrant must establish to the satisfaction of the issuing authority evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation. The agency should also establish that it cannot be obtained other than by telecommunications interception or the use of a listening device. It is then for the issuing authority to consider that evidence along with any other relevant matters such as the invasion of privacy involved and the gravity of the alleged offence in deciding whether to issue a warrant. Warrants should be for limited periods and the destruction of non-material content in whatever form should be strictly supervised. The number and justification of B-Party intercept warrants should be separately recorded by the Agency Co-ordinator and reported to the Attorney-General. The use of such warrants should be separately reported to the Parliament.

30. To better protect the rights of privacy of Australians, schedule 2 must contain better safeguards including addressing concerns expressed in the Blunn report.

31. The Law Council submits that privacy considerations are not properly balanced if gathering evidence against a person suspected of committing a crime punishable by seven years imprisonment outweighs the rights of the innocent to privacy. The Law Council questions the value that the government has placed on the right to privacy. A crime punishable by seven years imprisonment is not sufficiently serious to warrant the serious abrogation of the right to privacy.

32. A safeguard that is incorporated in clauses 3 and 9 of the Bill provides that the Attorney-General, judge or nominated AAT member must not issue a warrant for a B-Party intercept unless he or she is satisfied that:

a. the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person involved in the offence or offences referred to in paragraph (1)(d); or

b. interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

33. Schedule 2 does not provide safeguards to prevent rolling warrants from being issued in relation to telecommunication interception of an innocent B-Party. Similarly, without legislative guidelines on the range of B-Parties able to be monitored, the scope of the invasion of privacy is potentially far reaching.

34. The Attorney General in his second reading speech has said:

> "The ability, as a last resort, to intercept the communications of an associate of a person of interest will ensure that the utility of interception is not undermined by evasive techniques adopted by suspects…"

35. While the Attorney General believes that this measure is to be applied as a last resort, the Law Council believes that in order for the measure to be applied as a last resort, the agency should have exhausted all other means of surveillance and tracking of the suspect and not merely exhausted all other practicable methods pertaining to telecommunications services used or likely to be used by the suspect.

36. The Bill according to Attorney-General Philip Ruddock aims to balance the threats faced by the Australian people, with privacy considerations.

37. However, it is unclear in relation to B-Party interception, what proper safeguards are provided to achieve this in reality. Particularly, as the users of telecommunications services are unable to detect whether their communications are being monitored and therefore they have no opportunity to object to the surveillance and to determine the validity of the law, it is imperative to provide procedural safeguards and protections and independent oversight.

Role of the Attorney General in Issuing B-Party Interception Warrants

38. The Law Council has serious concerns in extending the power of the Attorney General to issue telecommunication interception warrants in respect of innocent third parties. Issuing warrants against innocent parties are a serious intrusion into human rights and require judicial oversight.

39. The Law Council has advocated this approach in relation to the detention of unlawful non citizens pursuant to the Migration Act.

40. However, the executive government continues to make decisions in relation to the detention of persons suspected of being unlawful non citizens. Recently the Palmer Inquiry found that many of the departmental officers interviewed, had used the detentions powers with little understanding of what, in legal terms, constituted a "reasonable suspicion". The Palmer Report also found that there was a lack of understanding by departmental officers of the gravity in taking away a person's human right to liberty.

41. The circumstances of Cornelia Rau and Vivian Alvarez and those of the estimated 200 other wrongful arrest cases demonstrates the consequences of granting power to the executive government to make decisions which erodes a person's fundamental human rights.

42. The Law Council maintains that judicial oversight is the best approach where decisions erode fundamental human rights such as interference with a person's liberty such as the unlawful interference with a person's right to privacy. The seriousness of taking away a person's liberty combined with the inability of the person to detect the intrusion and therefore challenge the State's action, warrants a person faced with this prospect to be accorded fair and balanced treatment from an independent judicial officer. This approach will also minimise issues in relation to an abuse of power, as unchecked powers can provide an irresistible temptation for abuse.

Conclusion

43. The United Nations High Commissioner for Human Rights in her review of provisions of human rights law which seek to strike a balance between legitimate national security concerns and fundamental freedoms noted that human rights law requires that, in the exceptional circumstances where it is permitted to limit some rights for legitimate and defined purposes other than emergencies, the principles of necessity and proportionality must be applied.

    a. "The measures taken must be appropriate and the least intrusive to achieve the objective. The discretion granted to certain authorities to act must not be unfettered."[8]

44. The Australian government seeks to expand telecommunications interception power pursuant to schedule 2 of the Bill in order to address crimes punishable by imprisonment of seven or more and which intrudes on the rights of the innocent. The Law Council strongly submits that schedule 2 is disproportionate to the threat to the Australian people and potentially breaches Article 17 of the ICCPR.

45. The Law Council has repeatedly called for the government at the very least before it "strengthens" the existing laws by removing vital protections for human rights, to assess whether the proposed measures are proportionate to the threats that the Government seeks to counter.[9]

46. The absence of a defined threat where risk and probability have not been fully analysed is a powerful reason not to enact schedule 2 of the Bill which has far reaching implications for fundamental human rights.

47. The response by President Aharon Barak of the Supreme Court of Israel in a case in which his Court held that violent interrogation of a suspected terrorist was unlawful even if it might save human life has relevance. He said:

48. "We are aware that this decision does not make it easier to deal with the reality. This is the fate of democracy, as not all means are acceptable to it, and not all methods employed by its enemies are open to it. Sometimes, a democracy must fight with one hand tied behind its back. Nonetheless, it has the upper hand. Preserving the rule of law and recognition of individual liberties constitute an important component of its understanding of security. At the end of the day, they strengthen its spirit and strength and allow it to overcome its difficulties."[10]

49. Even in the struggle against terrorism and not in relation to ordinary crimes, it is evident that Israel has the experience and wisdom to appreciate that the preservation of the rule of law and the protection and recognition of individual rights are important. In relation to Schedule 2 of the Bill, rights of the innocent to a life free of unlawful interference with his or her privacy, family and home is eroded in an attempt to gather evidence in relation to alleged ordinary crimes.

50. The Law Council submits that a government cannot defend and promote a free and democratic society by taking away the very freedoms that made it a

---

[8] Commission on Human Rights, *Statement by the United Nations High Commissioner for Human Rights, Fifty-eight session, Summary Record of the first meeting*, UN Doc E/CN.4/2002 SR.1(25 March 2002), para 14
[9] UK Joint Committee on Human Rights, *Report of the Joint Committee on Human Rights* (6 May 2004), paragraph 47.
[10] See President Aharon Barak, "A Judge on Judging: The Role of a Supreme Court in a Democracy" (2002) 116 Harvard Law Review at p. 148.

democracy in the first place. All that happens is that the country becomes unfree and unpleasant and the threat of terrorism looms perhaps even larger. [11]

[11] The Chair of the UK Bar Council, Guy Mansfield QC in his letter to the Law Council on 3 November 2005 expressing serious concerns in relation to the Anti-Terrorism Bill (No. 2) 2005.

Attachment A

Profile – Law Council of Australia

The Law Council of Australia is the peak national representative body of the Australian legal profession. The Law Council was established in 1933. It is the federal organisation representing approximately 50,000 Australian lawyers, through their representative bar associations and law societies (the "constituent bodies" of the Law Council).

The constituent bodies of the Law Council are, in alphabetical order:

ACT Bar Association;

Bar Association of Queensland;

Law Institute of Victoria;

Law Society of the ACT;

Law Society of NSW;

Law Society of the Northern Territory;

Law Society of South Australia;

Law Society of Tasmania;

Law Society of Western Australia;

New South Wales Bar Association;

Northern Territory Bar Association;

Queensland Law Society;

The Victorian Bar; and

Western Australian Bar Association.

The Law Council speaks for the Australian legal profession on the legal aspects of national and international issues, on federal law and on the operation of federal courts and tribunals. It works for the improvement of the law and of the administration of justice.

The Law Council is the most inclusive, on both geographical and professional bases, of all Australian legal professional organisations.