New South Wales Council for Civil Liberties

New South Wales Council for Civil Liberties Inc
149 St Johns Road
Glebe NSW 2037
Australia
www.nswccl.org.au

Ph 61 2 9660 7582
Fax 61 2 9566 4162
Email office@nswccl.org.au
DX 1111 Sydney

Correspondence to:
PO Box 201
Glebe NSW 2037
Australia

11 July 2007

Committee Secretary
Senate Legal and Constitutional Committee
Department of the Senate
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

Dear Sir/Madam:

Inquiry into *Telecommunications (Interception and Access) Amendment Bill 2007*

The New South Wales Council for Civil Liberties ("CCL") appreciates this opportunity to comment on the *Telecommunications (Interception and Access) Amendment Bill 2007* ("the Bill").

1. Privacy Concerns

- CCL is concerned with several aspects of the Bill. In an age of developing technology, "…there are no longer any technical barriers to the kind of Big Brother surveillance society envisioned by George Orwell…the barriers that remain are political and legal."[1]
- The Attorney General acknowledged that the increase in availability of telecommunications information "involves a much greater impact on privacy." In light of the increasing capabilities of technology to grant access to information, there must be an increased emphasis on the protection of privacy.

---

[1], Barry Steinhardt, "Liberty in the Age of Technology" (2004) *Global Agenda,* at 154. See also M D Kirby, "Privacy in Cyberspace" (1998) 21(2) *UNSWLJ* 323 at 325, in which Justice Michael Kirby similarly notes:

> The speed, power, accessibility and storage capacity for personal information identifying an individual are now greatly increased. Some of the chief protections for privacy in the past arose from the sheer costs for retrieving personal information; the impermanency of the forms in which that information was stored; and the inconvenience experienced in procuring access (assuming that its existence was known). Other protections for privacy arose from the incompatibility of collections with available indexes and the effective undiscoverability of most personal data. These practical safeguards for privacy largely disappear in the digital age.

- CCL supports the inclusion of privacy as a consideration in Clauses 180, 183, and 189 of Schedule 1. However, CCL would welcome further elaboration of this requirement in the Bill by way of substantive requirements for protection of privacy. In other words, the lip service given to privacy could use some teeth.

2. Access Without a Warrant

- CCL is extremely concerned that the Bill retains the power of police and other agencies to access data **without a warrant**. Subsequent to Clause 183 of Schedule 1, only "written" or "electronic authorisation" is required for access to data. This provision means that access can effectively be granted by as informal a means as email. This represents far too low a threshold for such an invasion of privacy.
- A warrant is of vital importance because it safeguards the individual from arbitrary interference, as guaranteed by the *International Covenant on Civil and Political Rights*:

  1. **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.

  2. Everyone has the right to the protection of the law against such interference or attacks.[2]

- This covenant, to which Australia is a signatory, applies to *correspondence* as well as to traditional physical interference.
- Without the requirement of a warrant, the person whose data is examined is defenceless, with no opportunity to contest. No grounds for interception are required, only mere "satisfaction" as to its reasonable necessity. If telecommunications data need be accessed for purposes of law enforcement, then a warrant should be required in order to bring these investigations out into the sunlight.
- Although the Blunn Report recommends warrants for access to both real time communications and stored communications, the Bill does not require a warrant for telecommunications data.[3]
- The Bill limits disclosure to telecommunications data *about* a communication while prohibiting disclosure of the *contents or substance* of a communication.[4] However, as the Office of the Federal Privacy Commissioner comments, the distinction between information and content may be indiscernible at times.[5]

---

[2] Office of the United Nations High Commissioner for Human Rights, *International Covenant on Civil and Political Rights*, Article 17 (emphasis added).

[3] See 2. Blunn Report of the Review of the Regulation of Access to Communications, August 2005, available at http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Blunnreportofthereviewoftheregulationofaccesstocommunications-August2005

[4] See proposed Clause 172.

[5] See Office of the Federal Privacy Commissioner, *Submission to the Australian Attorney-General's Department: Exposure Draft of the Telecommunications (Interception and Access)*

The nature of modern communications exacerbates the risk of a slippery slope to excessive access. For example, call data and content are difficult to separate with respect to mobile phone locational information, e-mail content, and web browser logs.[6]

- A free and democratic society requires respect for the autonomy of individuals, and **limits on the power of both state and private organisations to intrude** on that autonomy.[7]
- For these reasons, CCL opposes the overbroad governmental power to access telecommunications without a warrant.

3. Prospective Access

- The bill proposes a new two-tiered system of access for existing and future telecommunications data. CCL is concerned about the expansion of access to data that is **not yet in existence** pursuant to Clauses 176 and 180.
- While accompanied by a higher threshold for authorisation relative to that proposed for existing data, this broad new power is bounded by regulation much weaker than the *Surveillance Devices Act 2004,* which would normally require a warrant for access.
- The capability of technology to allow virtually immediate access to data can effectively amount to real time surveillance.
- Future data, like existing data, should be accessible only by warrant.

4. Limits on Access

- CCL supports the record keeping and review of law enforcement surveillance activities in order to promote accountability among these parties. CCL supports the requirement that the report be published by the Minister for Parliamentary review.
- CCL supports the positive obligations of destroying information and revoking authorisations when no longer required.

5. B-Party Warrants

- CCL opposes the increased police powers to monitor those with a tangential connection to individuals suspected of involvment with child pornography. This amendment takes the principle of "judging one by the company he keeps" too far by enabling the government to broadly intercept all

---

Amendment Bill 2007, February 2007, available at: <http://www.privacy.gov.au/publications/subtel0207_print.html>.

[6] Electronic Frontiers Australia, *Submission to the Attorney-General's Department in Response to the Exposure draft of Telecommunications (Interception and Access) Amendment Bill 2007*, 23 February 2007, available at: <http://www.efa.org.au/Publish/efasubm-agd-tia-expdraft-2007.html#26_2>.

[7] The Australian Privacy Charter, Australian Privacy Charter Council, 'The Australian Privacy Charter' [1995] PLPR 31 at 31 (emphasis added).

telecommunications of someone who has done absolutely nothing illegal, and is not even suspected of such.

- Any one suspect is likely to be connected to a large number of people, who probably have no knowledge of the suspect's potential involvement with child pornography. Any one person under surveillance could have a large volume of information intercepted – text messages, emails, phone calls. Such broad intrusion is not justified, for a crime where the suspect himself usually gets a maximum sentences of two years.[8]
- The Attorney-General's office has responded this amendment represents a reaction to the "increasing tactical sophistication" of perpetrators[9]. However, that strategies are evolving, as they inevitably will, does not justify encroaching on the rights of innocent people to privacy. In enacting new legislation, we must not let panic get the better of us without full consideration of the impacts on the fundamental rights of Australians to privacy. If privacy is "the right to be let alone," no one should be more entitled than innocent third parties.
- Furthermore, a little knowledge can be a dangerous thing. As CCL has previously raised, the covert gathering of information combined with the power to limit individuals' rights risks a synergism that could lead to misdrawn conclusions applied unfairly.[10] For example, snippets information gleaned from third parties without their knowledge might be taken out of context to falsely implicate a suspect. The covert nature of this gathering eliminates the opportunity for explanation or reply.

6. Conclusion

- While the Minister assures us that this bill "does not represent new powers for security and law enforcement agencies," we conclude by generally cautioning that police powers must be examined in light of the civil liberties of Australians.
- The *International Covenant on Civil and Political Rights* states two related rights:

    1. Everyone shall have the **right to hold opinions** without interference.
    2. Everyone shall have the **right to freedom of expression**; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either

[8] Allard, Tom and AAP, "New powers to fight child porn," *Sydney Morning Herald,* 15 June 2007, available at: <http://www.smh.com.au/news/national/new-powers-to-fight-child-porn/2007/06/14/1181414469798.html.

[9] "Govt to boost police powers to find porn," *The Age*, 14 June 2007, available at: <http://www.theage.com.au/news/National/Govt-to-boost-police-powers-to-find-porn/2007/06/14/1181414434621.html>.

[10] See also Dr. M. Bibby, *Submission of the NSWCCL to the Senate Legal and Constitutional Committee's Inquiry into the Provisions of the Telecommunications (Interception) Amendment Bill 2006,* 13 March 2006, available at: <http://www.nswccl.org.au/docs/pdf/ti%20bill%202006%20submission.pdf>.

> orally, in writing or in print, in the form of art, or through any other media of his choice.[11]

- The effect of more and more intrusion into individual privacy, accelerated by the increasing availability of technology, will have a chilling effect on the precious freedom of Australians to think and speak freely. The aim of facilitating the prosecution of crimes should not trample on these rights.

[11] Office of the United Nations High Commissioner for Human Rights, *International Covenant on Civil and Political Rights*, Article 19 (emphasis added).