Australian Government

Australian Law Reform Commission

Emeritus Prof David Weisbrot AM
President

Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

16 October 2009

Dear Committee Secretary,

ALRC submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2009

1. The Australian Law Reform Commission (ALRC) makes the following submission to the Senate Legal and Constitutional Affairs Committee Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2009 (Cth) (the Bill).

2. The ALRC does not intend to provide detailed comments on the issues raised by the Bill. However, the ALRC would like to highlight its major inquiry into the *Privacy Act 1988* (Cth), which culminated in the final report *For Your Information: Australian Privacy Law and Practice* (ALRC 108, 2008) (*For Your Information*).

3. *For Your Information* (the report is available online at <www.alrc.gov.au>) was tabled in Parliament on 11 August 2008. The report represents the culmination of a 28 month inquiry into the extent to which the *Privacy Act 1988* (Cth) and related laws provide an effective framework for the protection of privacy in Australia.

4. As with all ALRC inquiries, there was a strong focus on community input. The breadth of the subject matter covered in this Inquiry required the ALRC to undertake one of the largest community consultation programs in its history. The ALRC organised: about 250 face-to-face meetings; major public forums; a series of roundtables on a variety of themes, including telecommunications; and a highly publicised 'National Privacy Phone-In' during which more than 1,300 members of the public contacted the ALRC about privacy matters.

5. The ALRC also received 585 written submissions from a broad cross-section of individuals, private sector organisations and government agencies. The high level of public engagement with the ALRC Inquiry reflected the extent of public interest and concern about privacy protection. Community and stakeholder concerns assisted the ALRC in the development of its priorities and the ultimate reform agenda.

6. *For Your Information* contains 74 chapters and 295 recommendations for reform. Some of the key recommendations include:

Australian Law Reform Commission
Level 25, 135 King Street
Sydney NSW 2000

Postal Address:
GPO Box 3708
Sydney NSW 2001

Tel (02) 8238 6333
Fax (02) 8238 6363

Web www.alrc.gov.au
Email president@alrc.gov.au

- Uniform privacy principles and national consistency: the *Privacy Act* should prescribe a single set of Privacy Principles—the model Unified Privacy Principles (UPPs)—to apply to all federal government agencies and the private sector.
- Rationalisation of exemptions and exceptions: the *Privacy Act* should be amended to rationalise the complex web of exemptions and exceptions. Exemptions only should be permitted where there is a compelling reason.
- Cause of action for a serious invasion of privacy: federal law should provide for a private cause of action where an individual has suffered a serious invasion of privacy, in circumstances in which the person had a reasonable expectation of privacy.

7. Part J of *For Your Information* deals with telecommunications privacy issues, including the interaction between the *Privacy Act* and the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA). A large number of telecommunications issues were raised during the ALRC's inquiry—many extending beyond the Terms of Reference for the ALRC inquiry. For example, a number of submissions questioned whether the *Telecommunications Act* and the TIA continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. The ALRC recommended that the Australian Government should initiate a review specifically to consider these issues.[1]

8. On 11 August 2008, Senator John Faulkner, the then Special Minister for State and Cabinet Secretary, announced that the Australian Government would respond to *For Your Information* in two stages. The Australian Government issued the first stage of its response to *For Your Information* on 14 October 2009, addressing 197 of the 295 recommendations in the ALRC report, and accepting approximately 90% of those recommendations. The remaining 98 recommendations—including the recommendations relating to telecommunications privacy—will be considered in stage two of the Government's response.

Destruction of intercepted information

9. Item 22 of the Bill would insert a new s 79A into the TIA which provides that a responsible person for a computer network must ensure the destruction of a restricted record that is a record of a communication that was intercepted under paragraph 7(2)(aaa). This requirement extends only to the destruction of the original record. There is no obligation on the responsible person to destroy copies of restricted records. The Explanatory Memorandum notes that this is not necessary as often copies of records are no longer in the possession of the responsible person.

10. The ALRC considered the destruction of intercepted information in *For Your Information*.[2] Section 79 of the TIA provides that a record, 'other than a copy', obtained by means of an interception must be destroyed if the chief officer of an agency is satisfied that it is unlikely that it will be required for certain permitted purposes. Section 150 of the TIA contains a similar requirement to destroy information or a record obtained by accessing a stored communication. However, this section does not distinguish between a record and a copy of a record. The Blunn Report noted that it was 'curious' that the requirement to destroy a record under s 79 did not extend to copies of the record.[3]

---

1 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC 108, 2008), Recommendation 71–2.

2 Ibid, [73.47]–[73.52].

3 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department, [9.4].

11. A number of stakeholders in the ALRC inquiry expressed the view that the same destruction rules should apply to records and copies of records.[4] However, the Australian Government Attorney-General's Department (AGD) submitted that the requirement to destroy copies was excluded from s 79 because of enforcement issues. For example, agencies could not enforce destruction of copies given to other agencies for permitted purposes, or where the information appeared on the public record. The AGD also noted that copies of lawfully intercepted information may be made only in limited circumstances under the TIA, and that any copies of the information continued to be protected from further use or communication. [5]

12. One stakeholder submitted that lawfully intercepted information is often included in operational documents, and that it would be impossible to comply with a requirement that these types of documents be destroyed because they include copies of intercepted material. The stakeholder also submitted that the proposal could create an unjustified administrative burden on interception agencies. A requirement to destroy all copies would mean that very stringent record-keeping measures would need to be in place to ensure that the whereabouts of every copy was logged.[6]

13. The ALRC can see no reason why copies of information obtained from a stored communication warrant must be destroyed, but that copies of information obtained from an interception warrant are not. The ALRC therefore recommended that s 79 of the TIA be amended to provide that the chief officer of an agency must cause a record—including any copy of a record—made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.[7]

14. The covert nature of interception and access to communications requires the safeguard that the intercepted or accessed information is destroyed as soon as it is no longer required. The recommended 'Data Security' principle under the UPPs provides that an agency or organisation must destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law.[8] In our view, this rule should apply to records as well as copies of records of intercepted information—agencies should not be able to retain copies of records indefinitely.

15. I hope this information is of some value to Committee members.

Yours sincerely

4 See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC 108, 2008), [73.82].

5 Ibid.

6 Ibid, [73.82]. A confidential submission.

7 Ibid, Recommendation 73–1.

8 Ibid, Ch 28.