Electronic Frontiers Australia Inc

PO Box 382 North Adelaide
SA 5006 AUSTRALIA
www.efa.org.au
email@efa.org.au
Tel: 02 9011 1088
Fax: 02 8002 4009

19 July 2007

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

Email: legcon.sen@aph.gov.au

Dear Ms Morris

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

We enclose herewith supplementary submission containing additional comments and information arising from the government response to the Committee's Recommendations in relation to the 2006 TIA Bill.

The undersigned can be contacted via the above phone number or directly on 0412 997 163.

Yours sincerely

Irene Graham
on behalf of the Board of Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)
Supplementary Submission

To: Senate Standing Committee on Legal and Constitutional Affairs
Re: Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007

19 July 2007

Contents:

---

1. Introduction

We thank the Committee/Secretariat for sending EFA a copy of the government response to the Committee's Recommendations in relation to the 2006 TIA Bill together with an invitation to provide any further comments that may arise from information therein. We had previously searched for such a response on the Parliament web site, without success, and therefore were not aware that a government response to the Committee's March 2006 Report was recently issued.

While the information in the government response does not result in a need to amend any parts of EFA's submission dated 10 July 2007, we provide further comments and information on several matters below.

We also take this opportunity to advise the Committee of the legislative provisions which give rise to our understanding that the Bill would grant a new power to the CrimTrac Agency to apply for stored communications warrants.

---

2. Govt. Response to Recommendation 1

The government response to Committee Recommendation 1 reinforces the concerns we expressed in Section 7.2 of our submission dated 10 July 2007. It is now clear that the government intent is that the provisions of Section 280(1)(a) of the TA and the notice/knowledge provisions of Section 108 of the TIAA operate as we stated we thought might be the situation in Section 7.2 of our submission.

As stated therein, we are opposed to that situation because there is no reliable means by which a carrier presented with a general search warrant can know whether or not the intended recipient, or the sender, has in fact been previously notified by the enforcement agency of their intention to access communications at the carrier. Therefore the provisions are open to misuse and abuse, e.g. failure to give prior notice to the sender or recipient, by Commonwealth, State and Territory criminal law, civil penalty and public revenue enforcement agencies.

Accordingly we still consider Section 280 of the TA should be amended as suggested in Section 4.1 of our submission on the current Bill.

If that is not done, we would still be of the view that Section 280 of the TA requires amendment to make it clear to readers of that section (e.g. to enforcement agencies and carriers) that access to the content or substance of stored communications is not rendered lawful solely by a general warrant, that is, to make clear that knowledge of or notice to the intended recipient or sender is also required.

We consider the above may be achieved by amending s280 of the TA as shown in bold italic text below:

280 Authorisation by or under law

(1) Division 2 does not prohibit a disclosure or use of information or a document if:

(a) in a case where the disclosure or use is in connection with the operation of an enforcement agency—the disclosure or use is required or authorised under a warrant;

(b)...

(2) Subsection (1)(a) does not apply to disclosure or use of:

(a) information that is the contents or substance of a communication; or

(b) a document to the extent that the document contains the contents or substance of a communication;

unless:

(i) the warrant is issued under the Telecommunications (Interception and Access) Act 1979; or

(ii) disclosure or use under a warrant takes place with the knowledge of a person specified in Section 108(1)(b)(i) or (ii) of the Telecommunications (Interception and Access) Act 1979.

---

3. Govt. Response to Recommendation 4

We note the government response states that the person who is the subject of a stored communications warrant is now required to be identified in the warrant by the *Telecommunications (Interception) Amendment Regulations 2006 (No. 1)*, or that a telecommunications service is required to be identified in the warrant if the person's name is not known. While this goes some way to addressing the issue raised and the Committee's recommendation, it does not fully do so. We remain of the view that the person's name and also the telecommunications service/s (whether or not the person's name is known) should be required to be identified in the warrant, the same as is the case for an interception warrant. Furthermore, we remain of the view that such requirements should be incorporated into the actual legislation, as is the case in relation to interception warrants (s42(4A)(a) and (b) of the TIAA), not left for determination after legislation is enacted. Moreover such important requirements should not be able to be changed at some future time by way of replacement regulations. Any change to such important requirements should require enactment of a Bill.

---

4. Govt. Response to Recommendation 10

In our view the government response to Committee Recommendation 10 does not address the core point, as stated in the Committee Report, that under the legislation "*an obligation to destroy irrelevant information does not arise until after the chief officer has formed a view that the information is no longer required without the Bill specifying a time limit for this to occur*". As there is no obligation on a chief officer to form a view one way or the other at any point/s in time, irrelevant information could be kept indefinitely without breach of the law. We remain of the view that Recommendation 10 should be implemented.

5. Govt. Response to Recommendation 14

EFA is pleased to see in the government response that the government is of the view that the Committee's recommendation of an amendment to ensure that **copies** of communications (stored on a carrier's equipment) can not be accessed without a stored communications warrant is not necessary because that "is already the legal position".

However, unfortunately EFA is unable to feel confident that that is in fact the legal position. In this regard, we recall for example that in 2004 the Committee's inquiry found that the Attorney-General's Department/Solicitor-General disagreed with the Australian Federal Police/Commonwealth Director of Public Prosecutions on the legal position concerning lawful access to stored communications under legislation existing at that time (see Senate Legal and Constitutional Legislation Committee Hansard 22 March 2004). While amendments since then have resolved that difference of opinion on the legal position, in our view there is now potential for difference of opinion on the legal position in relation to lawful access to copies of stored communications.

Hence, we remain of the view that for clarity and certainty the TIAA should be amended as recommended in Section 7.4 of our submission dated 10 July 2007.

---

6. Govt. Response to Recommendation 15

The government response appears to us to be saying that amendment to the definition of "record", as recommended by the Committee, is not considered necessary due to the government's interpretation of the existing definition of "record". For the same reasons as stated in relation to Recommendation 14 above, we remain of the view that the definition of "record" should be amended as recommended in Section 7.5 of our submission dated 10 July 2007.

---

7. Govt. Response to Recommendation 16

Recommendation 16 dealt with an issue which we raised concerning lawful means of access to communications stored in a person's Sent box on a carrier's equipment. While, as the government response states, an amendment was made which resolved that issue, it is that amendment that has also apparently unintentionally resulted in the unsatisfactory situation detailed in Section 7.1 of our submission dated 10 July 2007.

---

8. Govt. Response to Recommendations 18,19,20,21,22,23,24,25

EFA was and is opposed to the so-called "B-Party" interception provisions. In the absence of deletion of those provisions, we consider that at the least the Committee Recommendations should be implemented.

---

9. Govt. Response to Other Recommendations

The majority of other recommendations, not mentioned above, addressed issues raised by EFA (and also other submitters in most instances). The government response to those recommendations - generally that the government does not accept the Committee's recommendations - does not alter EFA's concerns and position on those matters, as set out in our submission on the 2006 TIA Bill.

---

10. CrimTrac and Stored Communications Warrants

In our submission dated 10 July 2007, we stated that "the Bill would grant new powers to the CrimTrac Agency to apply for stored communications warrants..." (Item (m) Executive Summary). However we did not refer to the legislative provisions which give rise to that assertion.

We are under the impression, from remarks made by a representative of the Attorney-General's Department during the Committee hearing on 16 July (the transcript of which is not yet available), that the Attorney-General's Department does not agree with the above assertion. We therefore take this opportunity to advise of the provisions of the TIAA and Bill which under pin our understanding of the effect of the Bill in this regard.

The existing definition of "enforcement agency" in the TIAA (which refers to the definition in s282 of the TA) does not include the CrimTrac Agency in the list of enforcement agencies. The Bill would replace the definition of "enforcement agency" in the TIAA with a list which does include CrimTrac.

The existing TIAA states:

> "*Part 3-3—Access by enforcement agencies to stored communications*
> *Division 1—Applications for warrants*
> *110 Enforcement agencies may apply for stored communications warrants*
> *(1) An* ***enforcement agency*** *may apply to an issuing authority for a stored communications warrant in respect of a person.*" [emphasis added]

Accordingly it seems quite clear that the Bill would give CrimTrac a new power to apply for stored communications warrants.

EFA is of the view that if it not intended that CrimTrac be empowered to obtain stored communications warrants, then legislation should not include them in a list of agencies empowered to apply for such a warrant.
