Electronic Frontiers Australia Inc

PO Box 382, North Adelaide SA 5006 ■
ABN: 35 050 159 188 ■
Web: www.efa.org.au ■
Email: email@efa.org.au ■
Tel: +61 2 9011 1088 ■
Fax: +61 2 8002 4009 ■

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

By email to: legcon.sen@aph.gov.au

Re: Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2008

Electronic Frontiers Australia Inc. ('EFA') appreciates the opportunity to make this submission to the Committee's inquiry into the provisions of the Telecommunications (Interception and Access) Bill 2008 ('the Bill').

EFA has a long-standing interest in laws relating to interception of telecommunications by law enforcement agencies. In particular, we draw the Committee's attention to section 4.2 of our submission to the Committee's previous inquiry into the provisions of the Telecommunications (Interception) Bill 2006.[1] Many of the objections which EFA raised to device-based interception of telecommunications in our 2006 submission remain unaddressed.

We have had the benefit of reading the submission made by the Law Council of Australia ('LCA') to the Committee's current inquiry. The LCA submission is of excellent quality and comprehensively details the problems of the Bill. We commend the LCA submission to the Committee and fully endorse the analysis and recommendations of that submission.

EFA believes that the Bill would allow blanket authorisation to ASIO and law enforcement agencies to engage in telecommunications interception without meaningful judicial oversight and without adequate safeguards for the privacy of members of the public. The provisions of the Bill are analogous to allowing ASIO and law enforcement agencies to obtain a search warrant which not only authorises them to search the premises identified in the warrant, but *any other premises* that the suspect is *likely* to use.

The decision as to what other premises the suspect is *likely* to use then becomes one for the warrant-seeking agency, and a warrant drafted in those terms becomes in effect a blank cheque, limited only by the restraint of the agency involved. It may be the case that, in such a situation, the agency would show less restraint in engaging in telecommunications interception because there is little, if any chance that such interception would be detected and the conduct of the agency scrutinised.

For the same reasons that such a 'blank cheque' search warrant would be repugnant to the rule of law and respect for the rights of the public, the 'blank cheque' telecommunications interception warrants which the Bill would facilitate must be rejected.

---

[1] http://www.efa.org.au/Publish/efasubm-slclc-tiabill-2006.html

EFA strongly endorses the LCA's recommendations that:

- while a single warrant may authorise interception of telecommunications made by means of multiple devices, each of those devices must be named in the warrant; and

- the issuer of the warrant must be satisfied that:

    - the person named in the warrant is using or is likely to use each device from which communications will be intercepted;

    - each of the devices used or likely to be used by the named person can be uniquely and reliably identified for interception purposes; and

    - the communications likely to be made by means of each device from which communications will be intercepted are likely to yield information useful to the investigation.

EFA is also concerned about how 'likely' it must be that the named person will use the devices specified in the warrant. The mere use of the term 'likely' is lacking in precision and should be clarified. Does 'likely' in this context mean 'more likely than not' -- i.e. on the balance of the probabilities? The meaning of the term in other legislation has been the subject of judicial debate which has at times reached differing outcomes. In the context of the Trade Practices Act 1974 (Cth), Bowen CJ said in *Tillmanns Butcheries Pty Ltd v Australasian Meat Industry employees' Union* that:

> The word 'likely' is one which has various shades of meaning. It may mean 'probable' in the sense of 'more probable than not' -- 'more than a fifty per cent chance'. It may mean 'material risk' as seen by a reasonable man 'such as might happen'. It may mean 'some possibility' -- more than a remote or bare chance. Or, it may mean that the conduct engaged in is inherently of such a character that it would ordinarily cause the effect specified.
>
> In *Australian Telecommunications Commission v. Kreig Enterprises Pty. Ltd.* (1976) 27 F.L.R. 400 Bray C.J. had to consider the meaning of the word "likely" in s. 139B of the Post and Telegraph Act 1901-1973 (Cth). The context, of course, was different. However, Bray C.J. concluded it meant 'more probable than not' in that context. His Honour expressed the view that that was the natural and ordinary meaning of 'likely', though he referred also to the rules of construction applicable where the statute being interpreted is a penal statute or one which, as in the case of s. 139B, imposed an additional liability beyond the liability in tort.[2]

EFA submits that the standard of a 'real chance or possibility' would be unacceptably low, and would both encourage and facilitate fishing expeditions by agencies with interception powers. These fishing expeditions could result in the interception of telecommunications devices belonging to a suspect's friends, relatives, or workmates, not because the agency concerned believes that the suspect *will* use those devices, but merely because they *might*.

If a lower standard than the balance of probabilities is intended, it should be clearly articulated by the Bill.

EFA recommends that:

- where the issuer of the warrant is not satisfied that the person named in the warrant is using a named device, they must be satisfied on the balance of the probabilities that the person will use that device.

- in the alternative, the amendments should clearly articulate how 'likely' it must be that the named person will use the relevant devices before a warrant can be issued.

---

[2] (1979) 42 FLR 331 at 339

Conclusion

The amendments contained in the Bill represent at least an incremental expansion in the telecommunications interception powers of ASIO and law enforcement agencies. At most, they enable the issuing of a 'blank cheque' to those agencies to intercept telecommunications from devices not named in the warrant, without meaningful oversight, and without significant risk of discovery if they should exceed their lawful authority.

In this recent time of heightened security concerns, law enforcement and intelligence agencies both in Australia and overseas appear to have, at least, shown insufficient concern for the civil liberties of their suspects or the population at large.[3]

In the circumstances it is both necessary and appropriate that the powers of Australian law enforcement and security agencies to engage in the interception of telecommunications should be subject to strong legislative restrictions, with judicial oversight, and that those agencies should not under any circumstances be given discretionary powers to decide which telecommunications services or devices should be intercepted.

---

[3] See, e.g. *R v Al-Haque* [2007] NSWSC 1251, where Adams J held that ASIO officers unlawfully kidnapped and falsely imprisoned a suspect. See also http://www.eff.org/issues/nsa-spying which details allegations of unlawful mass wiretapping by the US National Security Agency.