Electronic Frontiers Australia Inc

P.O. Box 382 North Adelaide SA 5006
www.efa.org.au
email@efa.org.au
Fax: 07 3424 0241
Tel: 07 3424 0201

18 May 2004

The Secretariat
Senate Legal and Constitutional Committee
Room S1.61, Parliament House
Canberra ACT 2600

Attention: Mr Phillip Bailey

Dear Mr Bailey

Inquiry into the provisions of the *Surveillance Devices Bill 2004*

I refer to my telephone call on Friday 14 May when I advised that EFA had only just become aware of the Committee's inquiry into the *Surveillance Devices Bill 2004* and that we have serious concerns about various provisions of the Bill. As mentioned, we had briefly looked into the Bill in late March. However, as there were four Federal Parliamentary and government agency inquiries underway on matters of concern to EFA, we had left dealing with the *Surveillance Devices Bill 2004* to a later date as we did not expect that such a complex and lengthy Bill concerning such serious issues would be brought up for debate in the House or referred to a Senate Committee so rapidly.

We would like the Committee members to be aware that EFA certainly does have the concerns that various Committee members remarked during the hearing that they expected privacy advocates and civil libertarians would have. While many of the issues that EFA would have raised in a submission were raised by respondents to the inquiry and/or Committee members, we are very concerned that it appears from submissions and the Hansard transcript that little, if any, attention has been given to the matter of data surveillance devices, as distinct from listening and optical surveillance devices. We believe the Bill in its current form presents high potential for data surveillance devices to be used to avoid the need for a telecommunications interception warrant.

We realise that the closing date for public submissions has passed and that the Committee is not under any obligation to accept late submissions. We nevertheless take this opportunity to offer some information and comments on the data surveillance provisions of the Bill in an attachment to this letter and hope that the Committee will see its way clear to take these matters into consideration in preparing its report and recommendations.

As the Committee's reporting date is approaching, we have prepared the attached document quickly and it therefore contains less detail than we would otherwise have provided. If any aspect is unclear or the Committee would like more information, we would be happy to provide same including by way of telephone discussion with a Secretariat staff member if that may be of assistance.

Yours sincerely

Irene Graham
Executive Director − Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)

Comments on the *Surveillance Devices Bill 2004*

18 May 2004

EFA is highly concerned that the **data** surveillance device provisions of the *Surveillance Devices Bill 2004* ("SD Bill") will remove the need for law enforcement agencies ("LEAs") to obtain a telecommunications *interception* warrant ("TI warrant") to covertly record electronic communications consisting of written information. It will also enable LEAs to covertly record electronic communications and other written information in circumstances where a TI warrant is not allowed to be issued. In addition, the Bill allows such information to be given to foreign countries, although the information could not be provided to a foreign country if it had been obtained under a TI warrant.

Although the SD Bill states, in relation to both warrants (s18(9)) and emergency authorisations (s32(4)), that:

> "*Nothing in this section authorises the doing of anything for which a warrant would be required under the Telecommunications (Interception) Act 1979*."

a data surveillance device warrant ("data SD warrant") could be used to covertly install software or hardware (e.g. a keystroke logger) in a computer. Such a device could record all information entered into the computer before it passes over a telecommunications system, thereby obviating the need for a TI warrant because the information is not passing over the telecommunications system at the time it is being recorded.

We consider the purported assurance in the SD Bill, concerning TI warrants, is totally inadequate in relation to electronic communications because the *Telecommunications (Interception) Act 1979* ("TI Act") is not clear with regard to where a telecommunications system begins and ends, nor when a TI warrant is required to intercept electronic communications. As the Committee is well aware the Attorney−General's Department ("A−G's Department") and the Australian Federal Police ("AFP") and their associated legal advisers have differing opinions on the correct interpretation of both existing and proposed versions of the TI Act and concerning AFP powers under the *Crimes Act 1914*. Furthermore, it is not known whether the government's third attempt to 'clarify' the provisions of the TI Act will be appropriate and successful.

We wonder whether the A−G's Department is of the view that the SD Bill would not remove the need for a TI warrant on the basis reported in the Committee's report on TI Amendment Bill 2004, that is:

> "3.18 ... in the Department's opinion, the telecommunications network extends to all equipment within Australia connecting a user to the public switched telephone network, up to and including a user's personal equipment. The Department stated that it had received independent legal advice supporting this view."

However, we consider it very doubtful that a user's personal computer would be regarded as part of the telecommunications network at the time a person was, for example, typing an email message, and especially if the computer was not actually connected to the Internet at the time of drafting the message prior to transmission. In any case, as the Committee is aware, the AFP does not agree with the A−G Department's opinion. It seems likely that the AFP would consider that the SD Bill

obviates the need for a TI warrant for the purposes of data surveillance because a data SD warrant would allow them to record information while it was being typed on a user's personal computer before it was actually transmitted over a telecommunications system.

We also recall that the AFP argues, in part, that Section 3L of the Crimes Act over−rides the TI Act because it was enacted after the TI Act and no reference was made to the contradictory nature of s3L and the TI Act when the Cybercrime Bill (which implemented s3L) was being considered. We are concerned that a similar view may be taken in relation to the provisions of the SD Bill and we consider it essential that the contradictory nature of the SD Bill and TI Act regarding data surveillance and electronic communications be addressed and resolved in a way that ensures it is abundantly clear that data SD warrants can not be used to avoid obtaining a TI warrant.

Even if, however, the current problems and issues with the TI Act are satisfactorily resolved in the very near future, that would not overcome the serious concerns about the vast extension of LEAs covert surveillance powers by way of use of data surveillance devices.

The privacy intrusiveness of data surveillance devices goes far beyond the intrusiveness of interception of telephone calls (as outlined later herein) but this is not recognised in the SD Bill. Generally speaking, issue of TI warrants is restricted to the investigation of serious offences punishable by imprisonment for a maximum period of at least 7 years. However, the SD Bill proposes to allow issue of data SD warrants in relation to far less serious offences, that is, those punishable by imprisonment for a maximum period of only 3 years and various other offences under the Financial Transaction Reports Act 1988 and the Fisheries Management Act 1991. In addition, the Bill inappropriately provides the ability to extend the use of data SDs by specifying additional offences in the regulations.

As defined in the Bill, data SDs include both software programs and hardware devices. We note that the definition specifically includes a "program", i.e. software, which is a broader definition than is used in the Victorian and NT Surveillance Acts (and probably others). Whether software programs are covered by e.g. the Victorian Act would depend on whether a software program is considered to be "apparatus" or "equipment" which seems doubtful. The Bill enables LEAs to covertly install spyware (software and hardware) on people's computers to record, for example:

- communications being typed on the computer, such as emails and conversations in Web−based chat rooms and in Internet Relay Chat, etc,
- addresses of Web pages and other files on the Internet, e.g. addresses typed into a Web browser for the purpose of visiting the page,
- information entered into programs such as word processing and spreadsheet programs,
- PIN numbers and passwords associated with banking, email and other accounts, and private encryption keys (notwithstanding that it is already a criminal offence involving up to 6 month's imprisonment for refusing to provide such information to Federal Police),
- etc, etc.

While some of the above types of information could be obtained by LEAs with a search warrant enabling them to seize a computer, such surveillance is not conducted covertly and accordingly there is less potential for abuse of police powers. Covert surveillance powers in relation to information entered on computers should be highly restricted.

Of even greater concern, the spyware would over−ride an individual's fundamental right to silence and also to avoid self−incrimination. In the process of recording information entered into a computer, the spyware would record what is little more than a person's thoughts. It would record words/paragraphs etc that a person wrote in an email message or other document and then decided

to delete or change. Thoughts that were not intended to be communicated to anyone else, nor even kept by the writer, would be caught and made available to LEAs.

A data SD installed in a computer would not only record the writings of a suspect, but also of any other person who used the computer, e.g. an entire family, flat mates, etc.

Due to the highly privacy invasive nature of data SDs and that they can record information that would otherwise require a TI warrant, EFA submits that the issue of data SD warrants should be subject to, at a minimum, the same requirements as the issue of TI warrants. Data SD warrants should only be issued for the serious offences listed as Class 1 and Class 2 offences in the TI Act and with the accompanying requirements of sections 45 and 46 of the TI Act.

We also consider that LEAs should not be permitted to use a data SD without judicial approval. Whether or not there is a claimed 'emergency', a warrant should have to be obtained before installation of spyware in a computer. Given LEA comments to the Committee concerning the pre−planning and organisation necessary to enter premises to covertly install SDs, we find it extremely difficult to believe that it would not be possible to obtain an urgent warrant by telephone while other LEA officers are pre−planning covert entry and installation.

EFA also objects to the provisions of the SD Bill that allow the use of data (and other types of) SDs to be extended to include "an offence that is prescribed by the regulations". Any additional offences must require an Act of Parliament and the accompanying potential for Parliamentary scrutiny and public debate. The opportunity for a disallowance motion is totally inadequate.

We observe that Section 18 of the SD Bill states:

> (3) Each surveillance device warrant also authorises:
> ...
> (f) the connection of the surveillance device or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the device or equipment; and ...

Obviously that permits LEAs to install data SDs that are also capable of automatically and secretly sending information entered on a computer to LEAs over the telecommunications system (e.g. via the Internet or a telephone line). We question whether it alone, and/or in conjunction with other provisions concerning use of third party property, could also permit LEAs to hack into people's computers via for example the Internet to install data SDs in computers. We have not had sufficient time to date to consider this aspect in detail. To our knowledge, currently only ASIO has such powers and we hope this Bill does not give other LEAs powers to do so in relation to suspected offences involving a threshold penalty of only three years.

While EFA supports the general intent of the Bill in regulating the use of surveillance devices by Federal LEAs and considers that LEAs should be able to use data and other SD devices in limited circumstances, in our view the provisions of the Bill go far beyond what is reasonable and appropriate. The Bill is heavily weighted towards granting the wishes of LEAs and therefore does not strike an appropriate balance between individuals' fundamental rights to privacy and freedom from intrusion and the legitimate needs of LEAs. The Bill requires a significant number of amendments before it would contain an appropriate balance, not only with regard to data SDs, but also in relation to matters raised by non−LEA submitters such as the Law Council of Australia, the Office of the Victorian Privacy Commissioner and the New South Wales Council for Civil Liberties Inc.