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

10 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 Sir/Madam

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

We enclose herewith submission from Electronic Frontiers Australia Inc. to the Committee's inquiry.

EFA appreciates the opportunity to make a submission and would be pleased to provide further information, including by way of oral testimony, in response to any questions Committee members may have.

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

Yours faithfully

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

Electronic Frontiers Australia Inc. (EFA)
Submission

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

10 July 2007

Contents:

---

1. Executive Summary

a. The Bill includes new powers for security and law enforcement agencies and significantly changes the existing "telecommunications data" access framework. It contains provisions that were not recommended, nor mentioned, in the Blunn Report, and some provisions that are contrary to recommendations in the Blunn Report.

b. New powers (not mentioned in the Blunn Report) would authorise covert access by criminal law enforcement agencies and ASIO, without a warrant, to information or documents about a person's physical location, web browsing and other online activities, and telephone call and email traffic information, during periods of time into the future.

c. Commonwealth and State criminal law enforcement agencies and ASIO would acquire a new power to require mobile phone/device location information to be covertly sent to them by carriers, in "near real time", for up to 45 and 90 days respectively into the future without a warrant. While referred to as "prospective" information in the Bill, when disclosed it will not be "prospective" information, it will be about the actual location of the mobile phone/device.

d. New technologies such as Assisted GPS, reportedly expected to be introduced in Australia by some carriers in 2007 or 2008, will greatly improve the accuracy of mobile phone location information. Access to "prospective" location information enables not only identifying/tracking location but potentially real world, real time, surveillance of a tracked individual's activities.

e. The "prospective" information access powers in relation to mobile phone/device location would enable enforcement agencies to avoid having to comply with the significantly more stringent safeguards and controls, including concerning subsequent disclosure and use of "protected information", applicable to the use of a "tracking device" under Commonwealth and State surveillance devices legislation. A mobile phone meets the definition of a surveillance device (sub-category: tracking device) in such legislation.

f. Granting agencies authority to use a tracking device that a vast number of members of the public normally carry on their person, without a warrant, raises significant potential for misuse and abuse due to the relative ease of using such a tracking device as compared to having to covertly attach a tracking device to a person's clothes or to property they may carry with them (which would require a warrant if covert entry to premises was required).

g. In relation to covert access to details of web browsing sessions, etc, the Explanatory Memorandum appears to be contradictory in relation to whether or not the new "prospective" information access powers will apply to surveilling/monitoring web browsing and other online activities in near real time during a future 45/90 days, but it appears likely that is the intention.

h. Surveillance of web browsing activities is akin to filming individuals' activities in a manner that records every item they purchase in shops, every film they see at the cinema or hire or buy, every book and magazine they glance through and/or purchase or take out on loan from a library and so on. Furthermore, unlike "telecommunications data" about telephone calls and email messages, the address of a web page often, of itself, provides information about the content or substance of the communication and web page addresses can be used to obtain access to the content that was communicated.

i. The Bill would permit criminal law enforcement agencies and ASIO to disclose information they obtained by a request for "prospective" information to other types of agencies (also in near real time) who are not empowered to access "prospective" information directly from carriers, and without the special limitations on disclosure that applied to the primary disclosure.

j. The Bill apparently envisages that Internet Service Providers would be willing to engage in **unlawful** interception (an offence carrying a penalty of up to two years imprisonment and which places an evidential burden in relation to defences on a defendant) in order to give effect to requests for "prospective" information about email message traffic. It appears highly doubtful that legislative drafters have considered, or consulted with technical experts on, the technical *and legislative* feasibility and/or practicality of giving effect to such requests. As an intentional result of the 2006 TI Bill, recording parts of an email message before it ceases passing over a telecommunications system, and hence can be accessed by the intended recipient, is unlawful interception. Waiting until an email message is in the mail box of the intended recipient before recording parts of it is technically impractical in terms of both method and surety of capturing required data before the message is deleted from the carrier's system and, in any case, appears likely to be unlawful access to a stored communication also as an intentional result of the 2006 TI Bill. None of the exceptions to the aforementioned offences appear to be applicable. While the TIAA does contain exceptions to the prohibitions on interception and access in relation to the execution of warrants, giving effect to the proposed authorisations is not in relation to warrants.

k. EFA is strongly opposed to the use of requests issued by enforcement agency and ASIO officers to authorise access to "prospective" mobile phone/device location information, i.e. to authorise tracking and/or surveillance into the future "in near real time" and to authorise access to details of web browsing which provides information about, and access to, the content of communications. A warrant issued by a magistrate under similar provisions as applicable to the issue of stored communications warrants must be required.

l. In relation to access to "historical" information, although the Blunn Report recommended "no change" to the existing telecommunications data access regime, the Bill would implement significant changes to that regime. The Bill:

    i. removes the requirement for issue/receipt of a conforming certificate (contrary to a specific recommendation of the Blunn Report);
    ii. removes the requirement that a senior officer (or anyone else) certify that the disclosure is reasonably necessary for the enforcement of the law;
    iii. reduces the restrictions on secondary and subsequent disclosure and use applicable to all enforcement agencies;
    iv. apparently grants enforcement agencies a new power to obtain access to information that is reasonably necessary for the enforcement of a law that the requesting agency has no responsibility to enforce (as a result of deletion of the definitions of three different types of law enforcement agencies).

m. The Bill would grant new powers to the CrimTrac Agency to apply for stored communications warrants and to issue authorisations for access to historical "telecommunications data", although CrimTrac is, as we understand it, **not** a law enforcement agency authorised to conduct investigations into suspected offences.

n. The Bill would amend the *Telecommunications Act 1997* in a manner that increases EFA's previously expressed concerns that Section 280 of that Act may permit covert access to the content of stored communications without a stored communications warrant. The Bill should amend Section 280 of the *Telecommunications Act 1997* to "make it clear that covert access to stored communications is not permitted without a stored communications warrant" as recommended by the Senate Legal and Constitutional Legislation Committee last year.

o. The proposed provisions concerning reports to the Minister and Parliament do not provide for adequate oversight. If the proposed significant reduction in existing restrictions on secondary and subsequent disclosure and use is to be implemented reporting on such disclosures is essential.

p. The proposed new exception to the prohibition on interception of communications by a "security authority" for "developing and testing interception capabilities" does not provide for adequate controls and the definition of "security authority" is entirely too open ended.

q. A number of amendments made to the *Telecommunications (Interception) Amendment Bill 2006* by the government during its passage through Parliament (i.e. after the completion of the Senate Committee's inquiry) have not resulted in an adequate level of clarity and certainty.

r. EFA considers the Bill requires a number of amendments in relation to the above and other matters. Some are necessary to provide clarity and certainty, and others to establish an appropriate balance between protecting the privacy of telecommunications users and meeting legitimate needs for access by security and law enforcement agencies.

s. As a result, EFA is unable to support passage of the Bill in its current form. EFA considers it highly unlikely that this Bill could be adequately and appropriately patched (amended) during its passage through Parliament. Attempts to do so are likely to unintentionally introduce additional areas of lack of clarity and certainty given the existing complexity of both the *Telecommunications (Interception and Access) Amendment Act 1979* and the *Telecommunications Act 1997* and inter-relationship between those Acts.

t. Accordingly, EFA recommends that this Bill be rejected by the Parliament. EFA considers legislative drafters should go back to the drawing board and develop a replacement Bill which appropriately addresses matters raised in this submission, and also in the recommendations of the Senate Legal and Constitutional Legislation Committee's Report on the provisions of the *Telecommunications (Interception) Amendment Bill 2006*.

---

2. Introduction

EFA appreciates the opportunity to make this submission in relation to the Telecommunications (Interception and Access) Amendment Bill 2007[1].

As members of the Committee may recall, last year EFA generally supported the stored communications provisions of the *Telecommunications (Interception) Amendment Bill 2006* ("2006 TI Bill"). We were pleased to be able to do so after four years of efforts to deal with the vexed issue of stored communications in terms of implementing an appropriate balance between protecting the privacy of telecommunications users and meeting legitimate needs for access by security and law enforcement agencies.

We had hoped that when a Bill to implement recommendations from the Report on the Review of the Regulation of Access to Communications[2] ("the Blunn Report") concerning agency access to "telecommunications data", we would also be able to support it. Unfortunately, however, that is not the case.

The Bill includes new powers for security and law enforcement agencies and significantly changes the existing access framework. It contains provisions that were not recommended, nor mentioned, in the Blunn Report, and some provisions that are contrary to recommendations in the Blunn Report.

In our view, the Bill requires a number of amendments. Some are necessary to provide clarity and certainty, and others to establish an appropriate balance between protecting the privacy of telecommunications users and meeting legitimate needs for access by security and law enforcement agencies.

---

3. Types and meaning of "telecommunications data"

3.1 Lack of definition

EFA submits that, as a result of advances in telecommunications technologies since the original drafting of the *Telecommunications Act 1997* ("the TA"), there is a need to either define "telecommunications data" (information or a document) for the purpose of proposed Chapter 4, or at the least implement legislative restrictions on what types of "information or a document" are authorised to be disclosed by Chapter 4.

The Blunn Report[2] states at 1.5.15:

> "*(b) 'call data' which, although it varies with technology, is basically the 'traffic information' that records that a communication has occurred; (often) the time, duration and location of the 'call'; and the addresses (numbers) of the sender and the intended recipient, in the internet environment this would be the IP address*".[2]

However, existing and proposed legislation does not contain any reference to "call data" or "traffic information", nor does it define "content or substance". While the Bill refers to "telecommunications data" in some headings, it does not define the term.

Furthermore, the Explanatory Memorandum to the Bill[3] indicates that the government/Attorney-General's Department are uncertain and/or confused about what constitutes "telecommunications data", causing lack of certainty in interpretation of the legislation. See Section 3.4 below.

3.2 Mobile phone locational information, etc.

The Blunn Report stated:

> "*1.1.25. An issue which arose during the review was the use of telecommunications data for surveillance purposes. Mobile telephones provide locational data and the precision of that data can be expected to improve. That data is generated without any specific intervention. The use of that data for security and law enforcement purposes is obvious. The privacy implications are equally obvious. However it is far from clear whether access is subject to any regulation. What does seem clear is that the issue is about access to telecommunications data.*
>
> *1.1.26. Accordingly I recommend that the access to such data for surveillance purposes be considered in the context of the requirement for comprehensive and over-riding legislation dealing with the general issue of access to telecommunications data.*"

The government's response to the Blunn Report remarks concerning the privacy implications of the use of mobile phone location information has apparently been to decide that disclosure of such information for surveillance and tracking purposes will be permitted without a warrant or any other type of independent oversight.

The above is not readily apparent in the Bill, as it contains no reference to mobile phone/device location information. However, since the Blunn Report was issued, Part 13 of the TA was amended by the *Communications Legislation Amendment (Content Services) Act 2007* (passed in June 2007) to state, in new s275A, that for the purposes of Part 13 information or a document about the location of a mobile telephone handset or any other mobile communications device is information protected by Part 13. Obviously location information is therefore accessible under exceptions to the protections of Part 13, which would include exceptions enacted by the Bill.

The Explanatory Memorandum to the Bill (p. 8, 9 and 12) makes apparent the intention that mobile phone/device location information will be able to be obtained by merely a written request issued by enforcement agency and ASIO staff members. Commonwealth and State criminal law enforcement agencies will acquire a **new** power to require so-called "prospective" location information to be sent to them, in "near real time" according to the EM, for up to 45 days into the future without a warrant, and ASIO for up to 90 days. While this information is referred to as "prospective" data in the Bill, when the information is disclosed to an enforcement agency "in near real time" it will not be "prospective" information, it will be information about the actual location of the phone or device. All Commonwealth and State/Territory enforcement agencies (criminal, civil penalty and public revenue agencies) will be able to obtain historical location information without a warrant.

In addition, the Bill intends to permit criminal law enforcement agencies to disclose location information they obtained by a request for "prospective" information to other types of agencies (also in near real time) who will not be empowered to access "prospective" information directly from carriage service providers, and without the same restrictions/limitations on such secondary disclosures as applied to the primary disclosure.

The objective of the proposed "prospective" information provisions in relation to location information appears to be to enable enforcement agencies to avoid having to comply with the significantly more stringent safeguards and controls, including concerning subsequent disclosure and use of "protected information", applicable to the use of a "tracking device" under Commonwealth and State legislation regulating and restricting the use of surveillance devices by agencies. A mobile phone meets the definition of a surveillance device (sub-category: tracking device) in such legislation.

While under some, possibly all, of those Acts, agencies are not required to obtain a surveillance device warrant to use a tracking device (unless installation involves entry onto premises without permission or an interference with the interior of a vehicle without permission), the officers who are empowered to authorise use of a tracking device are of a more senior level than "authorised officers" in the Bill. For example, in the Commonwealth Surveillance Device Act, persons who may authorise

use of a tracking device are generally the same as "certifying officers" as defined in the TIAA. Further, whether use of a tracking device was authorised by warrant, or an authorised officer, there are significantly more restrictions on use and disclosure of obtained information by agencies. Such restrictions are more akin to the protections applicable to information obtained under a stored communications warrant than the secondary use/disclosure provisions of the Bill.

However, we do not consider it appropriate that either "authorised officers" or "certified officers" be empowered to authorise access to mobile phone/device location information covertly from carriage service providers. There is a significant difference between authorising the use of a tracking device that a vast number of members of the public normally carry on their person, and authorising the use of a tracking device that needs covert installation. Generally speaking it is significantly more difficult for agencies to covertly install a tracking device on a person (and they would be required to obtain a warrant if they wished to enter premises to attach a tracking device to a person's clothes or property they may carry with them) than it is to covertly use a device the person possesses and normally carries. Hence there is significantly more potential for misuse and abuse due to the relative ease of enabling use of the tracking device.

According to commercial mobile phone location-based service suppliers which use location information provided by Australian telecommunications carriers, a mobile phone can currently be located to within 200 metres in metropolitan areas[4] (and within 100 metres in some urban areas[5]). However, new technologies such as Assisted GPS, which is reportedly expected to be introduced in Australia by some carriers in 2007 or 2008, will greatly improve the accuracy of mobile phone location information.

EFA is strongly opposed to Chapter 4 (titled "Access to telecommunications data") being implemented in the absence of a prohibition on disclosure of mobile phone/device location information under the currently proposed provisions of that Chapter, which would not provide adequate safeguards and controls against misuse and abuse.

EFA submits that a warrant issued by a magistrate under similar provisions as applicable to the issue of stored communications warrants must be required to authorise access to mobile phone/device location information, at the very least, in relation to access to "prospective" location information which enables not only identifying/tracking location but potentially real world, real time, surveillance of a tracked individual's activities.

3.3 Email message "data" and "content"

EFA considers legislative amendments are necessary to clarify, or indeed establish, a dividing line between so-called "call data" and the content or substance of communications, in relation to email messages.

Email messages consist of two parts: a header section and a body section (although this is not readily apparent to those users who do not know how to set their email software to display the whole header).

The body section is plainly "content" because it is the text of message, but it is unclear what parts of the header section are, or are not, regarded as content/substance. For example, the header section contains not only dates, to/from email addresses and IP address/es but also the subject line of the message.

In our view the subject line is part of the content of a message, but existing legislation is silent on this matter and it cannot be known whether the same view would be held by all carriers and enforcement agencies. Furthermore, email messages can carry significantly more other information in the header section than is equivalent to "traffic information" associated with telephone calls. For example, some (probably most) email programs enable the end-user to create their own special header fields in outgoing messages, in which they can place any information they wish. These are often referred to as "X" headers because, to ensure a user-defined name of a field will never conflict

with standard header field names, they should be given field names commencing with "X-". As stated in the technical specification for email, RFC 822 (http://www.ietf.org/rfc/rfc0822.txt):

> "*4.7.5. USER-DEFINED-FIELD*
> *Individual users of network mail are free to define and use additional header fields. Such fields must have names which are not already used in the current specification or in any definitions of extension-fields, and the overall syntax of these user-defined-fields must conform to this specification's rules for delimiting and folding fields. Due to the extension-field publishing process, the name of a user- defined-field may be pre-empted*
>
> *Note: The prefatory string "X-" will never be used in the names of Extension-fields. This provides user-defined fields with a protected set of names.*"

EFA considers that authorisations under proposed Chapter 4 should be limited to authorising access to the equivalent of "traffic information" of telephone calls, that is, dates of sending/receiving and information about the source and destination of the communication such as the sender and recipient's email addresses and IP addresses. The subject line and any other information in the header section should be legislatively regarded as content/substance.

EFA submitted the above view to the Attorney-General's Department in February in response to the exposure draft[6] of the now current Bill, which was issued without any explanatory material.

We observe that the Explanatory Memorandum to the Bill states that: "*The information [data] does not include content such as the subject line of an email...*", but makes no reference to other information in the header portion of some emails that is not in our view "traffic data" or "call data".

Notwithstanding the reference to subject lines in the EM, we remain of the view that relevant definitions, or at least explanatory notes, should be included in the legislation. Carriage service providers and Commonwealth and State/Territory enforcement agencies should not be expected or required to refer to ancillary material to find out what type of information/data can or can not be disclosed without a stored communications warrant. This should be made plain in the legislation to provide greater surety that authorisations will not purport to authorise disclosure of information that requires issue of a stored communications warrant and that carriage services providers will not voluntarily disclose information that is not permitted to be voluntarily disclosed because it is content, according to ancillary material which they may not have read or whose detail they may not recall.

3.4 Internet sessions - web browsing sessions, chat forum sessions, etc

The Bill, or at the very least the Explanatory Memorandum, requires amendment to provide clarity and certainty concerning what type of authority is required for lawful access to historical and prospective information about web browsing sessions, chat forum sessions, etc.

The Explanatory Memorandum appears to be contradictory in the above regard, and the Bill itself provides no relevant definitions or information. The EM states (at page 8 of the PDF version):

> "*Communications associated data will vary according to the type of telecommunications service. ...*
> *For Internet based telecommunications, such as email, **web browsing**, ... [t]he information does **not include** content such as the subject line of an email, the message sent by email or instant message or **the details of Internet sessions**.*" [emphasis added]

In contradiction, the EM states (at page 6):

> "*In relation to internet based applications, telecommunications data includes the Internet Protocol (IP) address used for the session, the web sites visited, and the start and finish time of each session.*"

Common usage and understanding of the term "Internet sessions" is that it includes web browsing sessions, chat forum sessions, etc. Hence, most people reading the EM would understand from page 8 that details of web sites visited during a web browsing session are not lawfully accessible without a stored communications warrant. However, page 6 appears to state to the contrary.

If the term "Internet sessions" as used in the EM does not include web browsing sessions then, at the least, the government should publicly explain what is meant/intended by "details of Internet sessions" that the EM states will **not** be lawfully accessible with a written request under proposed Chapter 4 (and amend the Bill or EM to make that clear).

Access to details of web pages visited is significantly more privacy invasive than access to telephone call data, i.e. numbers to or from which calls were made. It is akin to filming individuals' activities in a manner that records every item they purchase in shops, every film they see at the cinema or hire or buy, every book and magazine they glance through and/or purchase or take out on loan from a library and so on.

Furthermore, telephone numbers and the to/from fields of email messages do not provide any detail about the content of a communication. However, the address of a web page often, of itself, provides information about the content of the communication. It would be inconsistent and not technology neutral for legislation (or an EM) to say that "telecommunications data" does not include the subject line of an email (as the EM states), but does include the address of a web page. What is the difference between, for example:

- Subject: Sydney Protest Rally 29 February
- http://example.com/sydney-protest-rally-29-February.html

The web page address is no less "content or substance" than the subject line. Furthermore although p.6. of the EM appears to say that a web page address such as the above is to be accessible as "telecommunications data", proposed s172(b) of the Bill appears to state to the contrary:

> "*Divisions 3 and 4 do not permit the disclosure of ... a document to the extent that the document contains the contents or substance of a communication.*"

Moreover, details of web pages visited are very likely to provide access to the actual content that was communicated to the person. Obviously when an agency has received the addresses of web pages visited they can readily obtain the content of such pages. In the case of access to historical information, the content may not necessarily be identical by the time an agency accesses the provided web page address, however, the ready availability of web archives such as The Internet Archive's Wayback Machine[7] could enable access to the actual content at a past date. In the case of the proposed new powers to access "prospective" information "in near real time", the probability that enforcement agencies will be able to access, at the provided web page address, the actual content communicated to the person is vastly increased.

The use of existing s282 of the TA to access historical information about web browsing sessions appears to have been the result of evolving technology rather than a decision of Parliament to permit enforcement agency surveillance of Internet users by that means. It appears highly unlikely that the Parliament envisaged surveillance of individuals' activities by way of s282 certificates because, at the time of the *Telecommunications Bill 1996*, few people had sufficient knowledge and understanding of the then recently emerged technology of the World Wide Web to be aware of the possibility of such use of s282.

Although the Attorney-General's Terms of Reference for the Blunn Review stated that "*while the concept of a communication 'passing over' is technology neutral, its application has become more difficult in the context of advanced telecommunications services such as email, Internet browsing, short messaging services and other evolving technologies*", the Blunn Report did not make any recommendations, nor mention, means of lawful access to Internet browsing records.

EFA is strongly opposed to the use of written requests issued by enforcement agencies and ASIO to authorise access to details of web sites/pages visited.

EFA submits that because Internet browsing records provide information about, and access to, the content of communications, a stored communications warrant should be required for lawful access to such records, whether historical or prospective, and that the Bill should be amended accordingly.

---

4. Contents or substance of a communication

4.1 TIA Act: No disclosure of contents or substance of a communication

> *Chapter 4, Division 2—General provisions*
> *172 No disclosure of the contents or substance of a communication*
> *Divisions 3 and 4 do not permit the disclosure 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.*

This provision is welcomed because it resolves the long ongoing issue, that EFA has raised in submissions numerous times in the past, of whether or not s282(1) and (2) of the *Telecommunications Act 1997* ("the TA") could be used to authorise disclosure of the contents or substance of a communication (without a warrant or even certificate). It seems clear that, once enacted, s172 will have the effect of ensuring that the voluntary disclosure provisions (which replace s282(1) and (2) of the TA) cannot be used by agencies to obtain the contents or substance of communications.

However, it is of major concern to EFA that other provisions in the Bill indicate that enforcement agencies might be able to obtain the contents or substance of communications from carriage service providers without an interception or stored communications warrant issued under *Telecommunications (Interception and Access) Act 1979* ("the TIAA"). See Section 4.2 below.

4.2 Telecommunications Act: Disclosures authorised by law (s280 and amendment to s313)

EFA remains highly concerned by the apparent lack of any intention to amend s280 of the TA to clarify that s280 does not permit access by agencies to the contents or substance of communications without a warrant issued under the TIAA. EFA has raised this matter on a number of occasions before, as did the Senate Legal and Constitutional Legislation Committee in its Report on the Provisions of the Telecommunications (Interception) Amendment Bill 2006[8]:

> "*3.18 The Committee recommends that the Bill be amended to include a provision amending* ***Section 280*** *and subsections 282(1) and (2) of the Telecommunications Act 1997, effective from the same date as the Bill, to make it clear that covert access to stored communications is not permitted without a stored communications warrant.*" [emphasis added]

The above recommendation in relation to Section 280 was not implemented, nor to our knowledge has the government responded to the Committee's Report/recommendations.

EFA's concerns in relation to s280 are now exacerbated by proposed amendments to s313 of the TA contained in the Bill. The Bill deletes the provisions of s313(7) and replaces it with new provisions.

The amended provisions include:

> *Part 14—National interest matters*
> *313 Obligations of carriers and carriage service providers*
> *...*
> *(3) A carrier or carriage service provider must, in connection with:*
> *(a) the operation by the carrier or provider of telecommunications networks or facilities; or*
> *(b) the supply by the carrier or provider of carriage services;*
> *give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary for the following purposes:*
> *(c) enforcing the criminal law and laws imposing pecuniary penalties;*
> *(d) protecting the public revenue;*
> *(e) safeguarding national security.*
> *...*
> *(7) A reference in this section to giving help includes a reference to giving help by way of:*
> *(a) the provision of interception services, including services in executing an interception warrant under the Telecommunications (Interception and Access) Act 1979; or*
> *(b) giving effect to a stored communications warrant under that Act; or*
> *(c) providing relevant information about*
> *(i) any communication that is lawfully intercepted under such an interception warrant; or*
> *(ii) any communication that is lawfully accessed under such a stored communications warrant; or*
> *(d) giving effect to authorisations under Division 3, 4 or 5 of Part 4-1 of that Act; o*
> *(e) disclosing information or a document in accordance with section 280 of this Act.*

Sub-section 7(e) above is new, as no mention of s280 is contained in existing s313 of the TA.

It is unclear why ss7(e) is being added given that carriage service providers are required to provide reasonably necessary help in the form of disclosing information or a document only to enforcement agencies and ASIO and ss7(a) and (b) make clear that such help must be given in relation to warrants issued under the TIAA and (new) ss7(d) makes clear that such help must also be given in relation to authorisations that will replace existing Section 282 certificates.

EFA submits that s280(1)(a) of the TA must be amended as follows:

Replace:

> "*280 (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;*"

with:

> 280 (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 by the Telecommunications (Interception and Access) Act 1979;

Alternatively, at the least s280(1)(a) must be amended to state that it does not permit disclosure 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.

5. Access to "telecommunications data" (Chapter 4)

5.1 Voluntary disclosure

Division 3—The Organisation
174 Voluntary disclosure
...
Limitation
(2) This section does not apply if the Director-General of Security, the Deputy Director-General of Security or an officer or employee of the Organisation requests the holder to disclose the information or document.

Division 4—Enforcement agencies
177 Voluntary disclosure
Enforcement of the criminal law
...
Enforcement of a law imposing a pecuniary penalty or protection of the public revenue
...
Limitation
(3) This section does not apply if a relevant staff member of an enforcement agency requests the holder to disclose the information or document.

[relevant staff member of an enforcement agency means:
(a) the head (however described) of the enforcement agency; or
(b) a deputy head (however described) of the enforcement agency; or
(c) any employee, member of staff or officer of the enforcement agency.]

We note that since the February exposure draft, limitation clauses have been added to make clear that the voluntary disclosure provisions (which will replace s282(1) and (2) and s283(1) of the TA) do not apply to requests for disclosure from enforcement agencies or ASIO. This addition is welcomed as it appears to address part of the Blunn Report recommendations in relation to voluntary disclosures to which we drew attention in our submission on the exposure draft[9].

The Blunn Report stated:

> *1.7.5. In as much as they require the eligible person to form an opinion that disclosure is 'reasonably necessary' for the enforcement of the criminal law or the protection of the public revenue they [s282(1) and (2)] appear inappropriate and sit oddly with the requirement established by subsections 282(3), (4) and (5) for a certificate from the requesting agency in which case access to content or substance is precluded.*
> *1.7.6. That said, there is obviously a case for enabling eligible persons who do come across information in the course their employment which they consider relevant to security or law enforcement to report that to an appropriate authority. From a privacy point of view the provisions as presently drafted are not adequate and I recommend that they be reviewed with a view to clarifying the objective and better identifying the process to be followed.*[#]

We remain of the view that the voluntary disclosure provisions should make clear the objective and identify the process to be followed. The addition of the limitation clause goes some way to clarifying the objective, but does not identify the process to be followed.

5.2 Requests by agencies for access

5.2.1 General

Although the EM states:

> "*The Bill will amend the Telecommunications (Interception and Access) Act 1979 (the TIA Act) to implement further recommendations from the Report on the Review of the Regulation of Access to Communications by Anthony Blunn AO (the Blunn Report).*"

the proposed provisions concerning requests by enforcement agencies for access to information or a document are not in accordance with the recommendations in the Blunn Report.

The Blunn Report stated:

> "*1.7. Access to Call Data*
> *1.7.1. As outlined at paragraph 1.2.3 currently under the Telco Act 'call data' may be accessed for security and law enforcement purposes and for the protection of public revenue. Generally the prescribed process involves an authorised officer of a designated agency certifying that disclosure is 'reasonably necessary' for the specified purpose. However under that process access to 'content or substance' is not to be disclosed.*
> *1.7.2.* ***Other than to reinforce the requirement that access should only be provided on receipt of a conforming certificate I see no reason to change that regime and I recommend accordingly.***" [emphasis in original]

However, the Bill would implement significant changes to that regime. The Bill:

- removes the requirement for issue/receipt of a conforming certificate;
- removes the requirement that a senior officer (or anyone else) certify that the disclosure is reasonably necessary for the enforcement of the law;
- grants criminal law enforcement agencies and ASIO **new** powers to obtain information for surveillance and/or tracking purposes for up to 45 and 90 days respectively into the future via a written request that will replace certificates, i.e. without a warrant;
- reduces the restrictions on secondary and subsequent disclosure applicable to all enforcement agencies;
- grants criminal law enforcement agencies the right to use and disclose information to other types of agencies, the original disclosure of which was subject to special conditions, without those special conditions applying to the secondary use or disclosure;
- appears to enable enforcement agencies to obtain access to information that is reasonably necessary for the enforcement of a law that the requesting agency has no responsibility to enforce.

More information about the above matters is provided below.

5.2.2 Changes to definition of "enforcement agency"

The Bill would change the definition of "enforcement agency" with the result that it is different from the existing definitions in both the TA and TIAA.

This change affects not only which agencies are authorised to access "telecommunications data" but also which agencies are authorised to obtain stored communications warrants under the TIAA.

A number of agencies to be added to the definition are agencies with existing interception powers, and we do not object to those additions.

(a) CrimTrac

However, the Bill also adds the CrimTrac Agency to the definition. CrimTrac is not included in the existing definitions in either the TA or TIAA. Hence, the Bill would give the CrimTrac Agency a new power to covertly access the content of communications and telecommunications data, that is, obtain stored communications warrants and access historical "telecommunications data". (The Bill excludes CrimTrac from the definition of criminal law enforcement agencies authorised to obtain access to "prospective" information).

It is EFA's understanding that CrimTrac is not a law enforcement agency except for limited purposes relating to spent convictions legislation.

As CrimTrac is not, to our knowledge, a law enforcement agency authorised to conduct investigations into suspected criminal offences we see no legitimate reason why CrimTrac should be authorised to obtain stored communications warrants, nor compel carriage service providers to disclose information or documents about telecommunications users and their communications.

EFA submits that CrimTrac should be deleted from the definition of enforcement agency.

(b) Civil penalty-enforcement agency and public revenue agency

In addition, the Bill would change the definitions of a civil penalty-enforcement agency and a public revenue agency. Currently, those types of agencies able to apply for stored communications warrants under the TIAA and access "telecommunications data" under the TA are defined as:

"an agency responsible for":
- "administering a law imposing a pecuniary penalty" (a civil penalty-enforcement agency);
- "the administration of a law relating to the protection of the public revenue and includes the Australian Taxation Office" (a public revenue agency).

The Bill changes the above to:

"any body whose functions include:
(i) administering a law imposing a pecuniary penalty; or
(ii) administering a law relating to the protection of the public revenue".

EFA questions what types of bodies have functions which "include" administering such laws but are not responsible for administering such laws. We consider, at the least, the Parliament and public should be informed by the government of the extent to which this change will increase the number and type of entities which are able to covertly access stored communications and "telecommunications data" together with examples of such bodies.

EFA is opposed to the above change because it is not possible to consider whether the change is appropriate or justified in the absence of information about the intended effect of the change.

5.3 Authorisations for access to existing information or documents

Division 4—Enforcement agencies
178 Authorisations for access to existing information or documents—enforcement of the criminal law

179 Authorisations for access to existing information or documents—enforcement of a law imposing a pecuniary penalty or protection of the public revenue

5.3.1 New access powers for all enforcement agencies

In our submission on the February exposure draft, we noted that the then proposed provisions concerning access to **existing** information or documents were substantially similar to existing s282(3), (4) and (5) of the TA in that the provisions did not provide new access powers to the

enforcement agencies currently defined in the TA, except that criminal law-enforcement agencies would gain the new power to issue a written request to emergency call persons for disclosure of information or a document.

However, substantial changes have been made since the exposure draft with the result that the Bill provides new access powers to all enforcement agencies.

Under the existing TA Act, and the February exposure draft, lawful disclosure of information reasonably necessary for the enforcement of a particular type of law requires certification by an authorised officer of the relevant type of law enforcement agency, or by an authorised officer of a criminal law enforcement agency. That is, officers of criminal law enforcement agencies can authorise disclosures reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue. However, officers of civil penalty-enforcement agencies and public revenue agencies can only authorise disclosures reasonably necessary for the enforcement of the specific type of law that their agency is responsible for enforcing.

However, the Bill does not contain the definitions of the three types of agencies that were in the exposure draft (and are in the TA) and has implemented omnibus provisions applicable to all types of "enforcement agencies". As a result, under the Bill, an authorised officer of any type of enforcement agency can authorise disclosure of existing information reasonably necessary for the enforcement of any type of law, i.e. including a type of law which their agency is not responsible for enforcing. For example, an officer of a public revenue agency could authorise disclosure of information that is reasonably necessary for the enforcement of the criminal law, or a civil penalty law.

EFA considers this broadening of agency powers to covertly access information about people's communications and personal affairs is entirely inappropriate and submits that the Bill should be changed back to the provisions in this regard that were in the February exposure draft, which restricted these powers to the same as under the current regime. As noted below, the Blunn Report recommended no change to the current data access regime.

5.3.2 No requirement for a conforming certificate, nor certification

The Blunn Report stated:

> *"1.6.1. ... access to call data should only be provided on production of a certificate; ...*
> ***1.7.2. Other than to reinforce the requirement that access should only be provided on receipt of a conforming certificate I see no reason to change that regime and I recommend accordingly."***[2] [emphasis in original]

However, instead of reinforcing the requirement for a conforming certificate, the Bill completely removes the requirement for a conforming certificate.

Under existing s282 of the TA, disclosure is authorised only, for example, "*if an authorised officer of a criminal law-enforcement agency has certified that the disclosure is reasonably necessary for the enforcement of the criminal law*" and such a certificate "*must comply with such requirements as are determined in writing by the ACMA*". The conditions applicable to civil penalty and public revenue agencies are equivalent. Similarly, s283(2) requires certifications by officers of ASIO.

However, the proposed new provisions do not require the issue of a certificate by enforcement agencies or ASIO, nor that an authorised officer certify that the disclosure is reasonably necessary for the enforcement of the [relevant] law. Instead they merely require that an authorised officer be "satisfied" that the disclosure is reasonably necessary.

Furthermore, it appears that carriage service providers will not only cease to receive a conforming certificate, but will not receive a copy of the actual authorisation either. In this regard the Bill states that: "*If an authorised officer of an enforcement agency makes an authorisation under Division 4 of*

Part 4-1, a relevant staff member [i.e. not necessarily the authorising officer] of the enforcement agency must notify the person from whom the disclosure is sought".

EFA agrees with Mr Blunn that the requirement that access only be provided on receipt of a conforming certificate should be reinforced, not deleted.

Hence, EFA is opposed to passage of the proposed legislation without a requirement for certification by an authorised officer that the disclosure is reasonably necessary and provision of a conforming certificate to the carriage service provider.

It is essential that carriage service providers, who are at risk of criminal or civil proceedings in relation to disclosures that were not "reasonably necessary", be presented with a certificate making it quite clear that an authorised officer has certified that the disclosure is reasonably necessary. Mere "notification" by a relevant staff member of an agency (which is defined as any employee, member of staff or officer of any enforcement agency) that someone else has authorised the requested disclosure, as proposed, is not appropriate nor adequate.

Furthermore it should be borne in mind that these provisions will not only apply to the Australian Federal Police (AFP) but also to the multitude of State and Territory criminal, civil penalty and public revenue agencies, who may not have an equivalent level of external and internal oversight, accountability mechanisms and internal procedures as the AFP (or for that matter any other Commonwealth enforcement agency).

5.3.3 Form of notifications and authorisations

We observe that the proposed provisions require merely that an authorisation, and a notification of an authorisation, be "in written form" or "in electronic form (for example, email)" (s183(1)) and that the Communications Access Co-ordinator "may" determine requirements for authorisations and notifications (s183(2)).

As stated above, EFA agrees with Mr Blunn that a conforming certificate should continue to be required. However, whether it is or not, s183(2) must be changed to state that the Communications Access Co-ordinator **must** determine requirements in relation to the form of authorisations, notifications and revocations, given the ACMA's existing determination in relation to the form of certificates will no longer apply.

It is essential that requirements be determined by the Communications Access Co-ordinator, published, and notified to carriage service providers, **before** the proposed legislation becomes effective. Among other things, systems/procedures must be put in place to ensure a carriage service provider can know whether an email sent to them purporting to be a notification of an authorisation of disclosure does in fact originate from a person authorised to send it. In this regard, for example, ACMA's existing requirements[10] (which will no longer apply) state:

> *f. if the certificate is in electronic form-confirm that a particular authorised officer issued the certificate, by identifying that officer through a unique code or unique identification consisting of a combination of symbols (for example, numbers, letters, marks and signs) which are recognisable to the person being requested to disclose the information or documents*

In the absence of rules such as the above, there would be a risk of unlawful disclosure by carriage service providers in response to emails that were not in fact sent by a person authorised to do so.

The above risk is heightened by the intention that notifications may sent by "a relevant staff member" which means any staff member of any agency. It appears there will be a need, for example, for agencies to specify a limited number of "relevant staff members" for the purpose and notify their codes to carriage services providers. Otherwise it appears that any "employee, member of staff or officer" of any Commonwealth or State or Territory enforcement agency could (without authority of the agency management) send an email to a carriage service provider purporting to have the authority to authorise disclosure and to receive disclosed information in response.

5.4 Authorisations for access to prospective information or documents

"180 Authorisations for access to prospective information or documents
(1) Sections 276, 277 and 278 of the Telecommunications Act 1997 do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under this section.

(2) An authorised officer of a criminal law-enforcement agency may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force. [up to 45 days].
(3) The authorised officer may, in that authorisation, also authorise the disclosure of specified information or specified documents that came into existence before the time the authorisation comes into force.
(4) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.
(5) Before making the authorisation, the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.
(6) An authorisation under this section:
(a) comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation; and
(b) ends at the time specified in the authorisation (which must be a time that is no longer than the end of the period of 45 days beginning on the day the authorisation is made), unless it is revoked earlier."

See also: s176 Authorisations for access to prospective information or documents, by ASIO.

The proposed powers of authorising access to "prospective" information or documents are new. Existing Section 282 of the TA does not contain any provisions authorising access to prospective information or documents, nor does any other section of the TA.

Such new access powers were not recommended (nor even mentioned) in the Blunn Report and are vastly more akin to interception and surveillance powers than existing data access powers in the TA.

The new powers would authorise covert access, without a warrant, to information or documents about a person's location, communications and personal affairs during periods of time into the future.

Written requests/authorisations by criminal law enforcement agency officers and ASIO officers would apply to mobile phone/device locational information and hence enable surveillance and tracking of individuals' whereabouts, in "near real time" according to the Explanatory Memorandum, during a period of 45 days (and 90 days in the case of ASIO) without a surveillance device warrant, or any other type of warrant. As detailed in Section 3.2 earlier herein, these new powers would enable enforcement agencies to avoid having to comply with the significantly more stringent safeguards and controls under Commonwealth and State surveillance device legislation. Further, the relative ease of using a tracking device that many members of the public normally carry on their person, compared to agency staff needing to covertly install a tracking device on a person or property they normally carry, significantly increases the potential for misuse and abuse of mere written requests authorising access to location information. New technologies likely to be introduced into Australia very soon, such as Assisted GPS, will greatly improve the accuracy of mobile phone location information (currently to within 200 metres in metropolitan areas). Hence, mobile phone location information enables not only identifying/tracking location but potentially real world, real time, surveillance of a tracked individual's activities.

In addition, these new powers would enable monitoring individuals' telephone call and email communications traffic for the same periods of time into the future and are probably intended to enable surveilling web browsing and any other online activities for the same periods. As discussed in Section 3.4 above, the EM appears to be contradictory in relation to whether or not these new

powers will also enable surveilling web browsing activities, but it appears likely that is the intention. Such surveillance is akin to filming individuals' activities in a manner that records every item they purchase in shops, every film they see at the cinema or hire or buy, every book and magazine they glance through and/or purchase or take out on loan from a library and so on. Furthermore, telephone numbers and the to/from fields of email messages do not provide any detail about the content of a communication. However, as discussed in Section 3.4, the address of a web page often, of itself, provides information about the content of the communication, and web page addresses can be used to obtain access to the content that was communicated.

The Explanatory Memorandum acknowledges that these new "prospective" information access powers are significantly more privacy invasive than the provisions of existing s282 of the TA and apparently for that reason places additional conditions on such access. Such authorisations may only be issued by criminal law enforcement agencies and ASIO and, in the case of criminal law enforcement agencies, the Bill limits disclosure to when reasonably necessary for the investigation of an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years and states that before making the authorisation, an authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure. No such limitations apply in relation to disclosures to ASIO.

However, EFA does not consider the additional conditions to be adequate. Officers empowered to authorise such access are proposed to be an employee of a criminal law-enforcement agency or ASIO. EFA considers it entirely unrealistic to expect such officers to have **adequate** regard to interference with the privacy of the subject individual or third parties who have merely been, or will be in the near future, in contact with a person of interest to an enforcement agency or ASIO. We consider that many of the same issues which arose in relation to the use of general search warrants and led to the creation of "stored communications warrants" also apply to authorisation of access to prospective "telecommunications data" and more greatly when disclosure may be authorised by mere written request of enforcement agency personnel.

Furthermore, since the exposure draft of the Bill, criminal law enforcement agency personnel who may be empowered to authorise such future/ongoing surveillance and tracking has been changed from "certifying officers" (who have certification responsibilities in relation to use of warrants issued by a judge or magistrate under the TIAA) to "authorised officers", thereby reducing the seniority level of personnel who may be entitled to authorise "prospective" information disclosures from senior executive and higher level to include middle managers and any other lower level management positions. If there is a legitimate and valid reason for this change to a lower level, an explanation should be provided, particularly given that in the case of ASIO only personnel in a position that is equivalent to, or that is higher than, an SES Band 2 position in the Department will be empowered to authorise "prospective" information disclosures. Otherwise the Bill should changed to certifying officer as was in the exposure draft.

In addition, the special conditions/limitations which apply to primary disclosure of prospective information do not apply to secondary and subsequent disclosure. The Bill permits secondary and subsequent disclosure and use of so-called "prospective" information for purposes for which the information could not have been disclosed/obtained in the first place and to non-criminal law enforcement agencies that would not have been eligible/able to obtain such information from a carriage service provider in the first place. For further information in this regard, see Section 5.6 below.

EFA is strongly opposed to the use of requests issued by enforcement agency and ASIO officers to authorise access to "prospective" location information, i.e. to authorise tracking and/or surveillance into the future "in near real time" and to access details of web pages visited which provides information about, and access to, the content of communications. A warrant issued by a magistrate under similar provisions as applicable to the issue of stored communications warrants must be required. In addition, significantly more appropriate restrictions on subsequent disclosure and use of "prospective" information than is contained in the Bill are necessary, for example, similar to the

restrictions applicable to information obtained under a stored communications warrant and such provisions should prohibit criminal law enforcement agencies from disclosing information to agencies that are not authorised to obtain "prospective" information.

Furthermore, unless it becomes publicly apparent during the course of the Committee's inquiry how it is expected, and intended, by the government that ISPs could give effect to "prospective" information authorisations in relation to email messages without engaging in unlawful interception, we will be of the view that an interception warrant must be required. This issue is discussed below.

5.5 Legislative practicality and technical practicality of giving effect to authorisations

EFA questions whether the legislative drafters have considered, or consulted with technical experts on, the technical **and legislative** feasibility and/or practicality of Internet Service Providers (ISPs) giving effect to the proposed authorisations for "prospective" information as envisaged (including "in near real time").

On our reading of the TIAA, it does not appear possible for ISPs to do so, in relation to email traffic information, without engaging in unlawful interception.

As members of the Committee would be aware, the amendments to the TIAA last year dealing with email messages/stored communications inserted the following:

> "*5F When a communication is passing over a telecommunications system*
> *(1) For the purposes of this Act, a communication:*
> *(a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and*
> *(b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.*"

and the TIAA also states:

> "*6 Interception of a communication*
> *(1) For the purposes of this Act, but subject to this section, interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.*"
>
> "*communication includes conversation and a message,* ***and any part of a*** *conversation or* ***message****, whether:*
> *(a) in the form of:*
> *(i) speech, music or other sounds;*
> *(ii) data;*
> *(iii) text;*
> *(iv) visual images, whether or not animated; or*
> *(v) signals; or*
> *(b) in any other form or in any combination of forms.*" [emphasis added]

For an ISP to give effect to the "prospective" information authorisations in relation to email message traffic, they would obviously have to make a record (defined to include copy) of parts of the message. However, an email message does not cease passing over a telecommunications system until it becomes accessible to the intended recipient (s5F), i.e. generally until it is in the intended recipient's mail box ready for downloading by the intended recipient. To record parts of an email message before it ceased passing over a telecommunications system would be interception in contravention of s7(1) of the TIAA. None of the exceptions to that offence appear to be applicable to giving effect to a written request/authorisation (and an evidential burden in relation to reliance on any of the exceptions rests with a defendant, e.g. carriage service provider employee).

Perhaps it is envisaged that an ISP would have to run, for example, a script on the mail box of a person of interest, every second, in the hope of capturing/copying the required extracts from incoming communication/s before they are downloaded by the intended recipient, at which time messages may, depending on the type and configuration of the mail server and mail box, be automatically deleted from the ISP's system. However, if that is what is envisaged, we also question whether legislative drafters have discussed this aspect with both large and small ISP representatives. ISPs are currently unlikely to have systems capable of copying/extracting the required information in such a way, and to run scripts constantly on mail boxes may increase server load and adversely affect efficient operations. EFA is of the view the ISPs should not have to implement such systems to avoid contravening one part of a law in the course of giving effect to another part. Also, it should be noted that while some, possibly all, ISPs' systems automatically log (make records of) some parts of messages passing through their mail servers for system maintenance/operational purposes, logging for such purposes would not include all of the items of "telecommunications data" that enforcement agencies would need/require.

Further, it is open to question whether or not recording parts of a message, without the intended recipient's knowledge, that has ceased passing over a telecommunications system and is stored in the person's mail box on a carrier's equipment would constitute unlawful access to a stored communication (see s6AA) in contravention of s108(1) of the TIAA (enacted last year together with amendments to definitions). Again none of the exceptions to that offence appear to be applicable to giving effect to a written request/authorisation. However, whether or not such access would be in contravention of s108(1) appears to depend on the correct interpretation of the intention of item (c) of the definition of "stored communication" - which was changed after completion of the Committee's inquiry last year - and is discussed in Section 7.1 later herein.

We note that s7(2) and s108(2) state that the offences referred to above do not apply to or in relation to intercepting a communication under an interception warrant, or accessing a stored communication under an interception warrant or a stored communications warrant. However, giving effect to the proposed authorisations is not related to warrants.

EFA objects to legislation which either does, or appears to, require ISPs to contravene the law in order to give effect to their obligations to provide "reasonably necessary" help to enforcement agencies and ASIO. Such a situation would bring the law into disrepute and encourage contempt for compliance with the law. Providing reasonably necessary help should not require contravening the law, and if it does not, that should be readily apparent from reading the legislation.

Accordingly, if the prospective information access provisions are not amended to require a stored communications or interception warrant (in relation to which exceptions to offences currently apply), as we submit they should be, then we consider the Bill requires amendments to enable ISPs to give effect to written authorisations for prospective information issued by enforcement agency and ASIO officers without engaging in unlawful interception. In any case, the Bill may require amendment to enable lawfully giving effect to authorisations for historical information, depending on the correct interpretation of the intention of item (c) of the definition of "stored communication".

5.6 Secondary disclosure/use offence

Division 6—Secondary disclosure/use offence
182 Secondary disclosure/use offence
(1) A person commits an offence if:
(a) information or a document is disclosed to the person as permitted by Division 4; and
(b) the person discloses or uses the information or document.
Penalty: Imprisonment for 2 years.
Exempt disclosures
(2) Paragraph (1)(b) does not apply to a disclosure of information or a document if the disclosure is reasonably necessary:
(a) for the performance by the Organisation of its functions; or
(b) for the enforcement of the criminal law; or
(c) for the enforcement of a law imposing a pecuniary penalty;
or
(d) for the protection of the public revenue.
Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the Criminal Code).

In relation to criminal law-enforcement agencies, proposed s182(2) permits secondary disclosure and use of "prospective" information for purposes for which the information could not have been disclosed/obtained in the first place, i.e. secondary disclosure/use in relation to investigation of offences with a penalty of **less than 3 years**. The authorisation of initial/primary disclosure of prospective information is restricted to when reasonably necessary for the investigation of an offence that is punishable by imprisonment for **at least 3 years** and before making the authorisation the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

EFA submits that, if the "prospective" information provisions are to remain (which EFA opposes), s182(2) must be amended so as to prohibit secondary disclosure and use of such information except under the same conditions as the initial disclosure, that is, when reasonably necessary for the investigation of an offence that is punishable by imprisonment for **at least 3 years** and before deciding to disclose information an officer must be required to have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

In addition, the proposed s182(2) secondary disclosure/use exceptions are significantly wider than the existing provisions in s298 of the TA. Unlike s298, proposed s182:

- permits secondary and subsequent disclosure and use for different purposes than the initial (or previous) disclosure and between different types of agencies;
- does not restrict third and subsequent disclosure or use;
- does not restrict secondary or subsequent disclosure or use of information that was initially voluntarily disclosed to an agency.
- permits secondary and subsequent disclosure to ASIO.

None of the above changes were recommended in the Blunn Report.

EFA submits that s182(2) must be amended to the equivalent of s298 of the TA, and if the prospective information provisions are to be implemented, s182 must also restrict secondary and subsequent disclosures of "prospective" information to the same limitations as the authorisation of the initial disclosure.

For reference, existing s298 of the TA states:

> "*Division 4—Secondary disclosure/use offences*
> ...
> *298 Law enforcement and protection of public revenue*

(1) If information or a document is disclosed to a person as permitted by subsection 282(1) or (3) [for enforcement of a criminal law] or this subsection, the person must not disclose or use the information or document unless the disclosure or use is reasonably necessary for the enforcement of the criminal law.
(2) If information or a document is disclosed to a person as permitted by paragraph 282(2)(a), subsection 282(4) [for enforcement of a pecuniary penalty law] or this subsection, the person must not disclose or use the information or document unless the disclosure or use is reasonably necessary for the enforcement of a law imposing a pecuniary penalty.
(3) If information or a document is disclosed to a person as permitted by paragraph 282(2)(b), subsection 282(5) [for protection of the public revenue] or this subsection, the person must not disclose or use the information or document unless the disclosure or use is reasonably necessary for the protection of the public revenue.
Note: Section 282 deals with the disclosure or use of information or documents reasonably necessary for law enforcement purposes or the protection of the public revenue."

We also observe that proposed s182(1) applies only to secondary disclosure and use by enforcement agencies (Division 4) and does not apply to ASIO (Division 3). Hence it appears that ASIO will be free to disclose information to any person at all for any purpose. We submit that secondary and subsequent disclosure and use limitations should apply to information disclosed to ASIO, especially in view of the new powers to be granted to ASIO to obtain "prospective" information without a warrant and without the limitations/restrictions applicable to criminal law enforcement agency access, so that secondary and subsequent disclosure by ASIO of historical and prospective information is only permitted in connection with the performance by the Organisation of its functions.

5.7 Report to Minister and Parliament

We note that the February exposure draft required enforcement agencies to give written reports to the Communications Access Co-ordinator concerning authorisations during each financial year, but did not require a report to be given to the Minister or Parliament.

We are pleased to observe that, instead, the Bill requires enforcement agencies to report to the Minister and a report prepared by the Minister to be laid before each House of the Parliament (as we advocated in our submission on the draft).

However, we are disturbed to find that the reporting requirements have been significantly reduced from the requirements of the draft. The draft required reporting on not only primary disclosures (as the Bill does) but also on secondary disclosures by enforcement agencies including:

- if it was to another enforcement agency or to ASIO, the reason for the disclosure; and
- if it was to another enforcement agency, the name of that other agency.

As detailed earlier herein, the secondary disclosure/use provisions of the Bill are significantly more permissive than the existing provisions of the TA. Unlike the TA, the Bill enables agencies to disclose both historical and "prospective" information to other types of enforcement agencies and to ASIO for a different reason than, and without the same limitations/conditions on, the primary disclosure by the carriage service provider.

EFA considers it is essential that there be Parliamentary oversight of the extent of use, and purposes of use, of secondary disclosures. This should also include reporting on secondary disclosures of "prospective" information, separately from secondary disclosures of historical information.

Accordingly EFA submits that, unless the secondary disclosure provisions are amended to become the equivalent of s298 of the TA, the Bill should be amended to require reporting on secondary disclosures including the same information as was required in the draft plus separately listing secondary disclosures of historical and "prospective" information.

5.8 Destruction of information or documents

The Bill should be amended to require enforcement agencies to destroy information or documents accessed/obtained under proposed Chapter 4 when the information is no longer likely to be required. Such provisions should be similar to s150 of the TIAA:

> "*150 Destruction of records*
> *(1) If:*
> *(a) information, or a record, that was obtained by accessing a stored communication (whether or not in contravention of subsection 108(1)) is in an enforcement agency's possession; and*
> *(b) the chief officer of the agency is satisfied that the information or record is not likely to be required for a purpose referred to in subsection 139(2);*
> *the chief officer must cause the information or record to be destroyed forthwith.*
> *(2) The chief officer must, as soon as practicable, and in any event within 3 months, after each 30 June, give to the Minister a written report that sets out the extent to which information and records were destroyed in accordance with this section.*"

5.9 Civil Proceedings and/or administrative action

Section 303C of the TA currently applies in relation to the secondary disclosure/use offences in s298 of Division 4, Part 13 of the TA. As the Bill deletes s298 and places secondary disclosure/use offences in new Chapter 4 of the TIAA, we submit that provisions equivalent to s303C are required in the TIAA. Individuals should continue to have the same rights, notwithstanding that s298 of the TA is to be in effect replaced by Chapter 4 of the TIAA.

Section 303C of the TA states:

> "*303C Prosecution of an offence against this Part does not affect proceedings under the Privacy Act 1988*
> *(1) The prosecution of an offence against Division 2 [Primary disclosure/use offences] or 4 [Secondary disclosure/use offences] of this Part for disclosure or use of information or a document does not prevent civil proceedings or administrative action from being taken under the Privacy Act 1988 or an approved privacy code (as defined in that Act) in relation to the disclosure or use.*
> *(2) This section applies regardless of the outcome of the prosecution.*
> *(3) This section does not affect the operation of section 49 of the Privacy Act 1988.*"

5.10 Civil Remedies

EFA submits that Part 3-7 of the TIAA which provides civil remedies in relation to unlawful access to, or communication of, stored communications should be amended to also apply to contraventions of proposed Chapter 4, i.e. to unlawful access to or communication of "telecommunications data". Alternatively similar civil remedies should be added to proposed Chapter 4.

---

6. Authorisation of interception for developing and testing interception capabilities (Chapter 2, Part 2-4)

> *31A Attorney-General may authorise interception for developing and testing interception capabilities*
> *(1) Upon receiving the request, the Attorney-General may authorise interception of communications passing over a telecommunications system by employees of the security authority authorised under section 31B.*

EFA is opposed to this proposed new exception to the prohibition on interception of communications.

Firstly, we question the need for such an exception in the absence of information justifying a legitimate need for same. In this regard, the brief comments in the Blunn Report do not justify the broad exception proposed in the Bill. While the Blunn Report states that:

> "*Currently this is done in a controlled environment to avoid contravening the Interception Act. Because the tests are not real time they may not identify problems that arise in the commercial provision of services. Testing real time data would assist agencies to establish whether C/CSPs are meeting their obligations under the Telco Act.*"[#]

it provides no indication that there has been any problem that was not identified during controlled environment testing. Furthermore, we note that it is the ACMA's responsibility to ensure CSPs are meeting their obligations, not law enforcement and/or defence and/or intelligence agencies.

Secondly, if the proposed exception can be justified, as currently drafted it nevertheless does not contain adequate controls and accountability mechanisms.

The definition of "security authority" is *entirely* too open ended:

> *security authority means an authority of the Commonwealth that has functions primarily relating to:*
> *(a) security; or*
> *(b) collection of foreign intelligence; or*
> *(c) the defence of Australia; or*
> *(d) the conduct of the Commonwealth's international affairs.*

When dealing with matters of this nature, legislation should exhaustively list the specific agencies/authorities involved. The proposed definition could include:

- the AFP, ASIO, ASIS, DSD, etc.
- the Defence Department generally (including the army, the navy, the air force);
- the Department of Foreign Affairs and Trade

Furthermore, since the exposure draft, clause (a) of the definition has been changed from "national security" to "security". We question what types of authorities that change is intended to allow to conduct interceptions. It appears it could include, for example, authorities with responsibility for:

- border security;
- aviation security;
- infrastructure security;
- water security;
- etc.

If this exception is to be implemented, it requires stringent safeguards, such as:

a. listing the specific agencies to which an authorisation may be granted;

b. the authorisation being required to nominate a specific point in a specific telecommunications service provider's network at which the performance of interception is authorised, and the authorisation being restricted to that specific point on that specific network;

c. a requirement that the Managing Director of the carrier/CSP be notified, in advance, of the interception of their network;

d. a requirement that the technologies/system must have been well tested in a controlled environment prior to the issue of an authorisation permitting interception of communications on a public telecommunications network;

e. restrictions on issue of multiple authorisations to an agency designed to prevent the issue of rolling 6 monthly (or any other period) authorisations, that is, so that a second authorisation cannot be issued immediately the first one terminates, nor shortly thereafter.

f. teeth be given to the conditions of authorisation in proposed s31A(2) (i.e. prohibiting interception of communications for purposes other than development/testing, and communicating, using or recording such communications except for such purposes) by enacting criminal penalties applicable to an individual who breaches those conditions.

g. the authorisation being required to be laid before Parliament (or otherwise publicly reported on) and preferably made disallowable;

h. independent audit provisions in relation to the conduct of the interception activities;

---

7. Matters arising from amendments to the 2006 TI Bill

In EFA's view a number of amendments made to the 2006 TI Bill during its passage through Parliament (i.e. after the completion of the Committee's inquiry) have not resulted in an adequate level of clarity and certainty.

As the current Bill does not include clarification in relation to these matters, we take this opportunity to draw these issues to the Committee's attention. Some of these matters have also been the subject of Committee Recommendations which have not been implemented nor, to our knowledge, has the government responded to the recommendations.

7.1 Access to stored communications by carrier employees

The 2006 TI Bill as amended during passage through Parliament, changed the definition of "stored communication" as follows:

> ~~*stored communication* means a communication that:~~
> ~~(a) has passed over a telecommunications system; and~~
> ~~(b) is not passing over that or any other telecommunications system; and~~
> ~~(c) is held on equipment that is operated by, and is in the possession of, a carrier; and~~
> ~~(d) is accessible to the intended recipient of the communication.~~
>
> *stored communication* means a communication that:
> (a) is not passing over a telecommunications system; and
> (b) is held on equipment that is operated by, and is in the possession of, a carrier;
> and
> (c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

Our understanding is that the above change was made to enable lawful access to emails in draft boxes and sent boxes with a stored communications warrant - an issue raised during the Committee's inquiry.

However, the replacement of original (d) with new (c) of the definition of 'stored communication' appears to have unintentionally resulted in a situation where communications stored on a carrier's equipment that can be accessed thereon "without the assistance of an employee of a carrier" are not "stored communications".

As a result, it appears that if an employee of a carrier accesses communications stored on the carrier's system "without the assistance of" another employee (for non-specified purposes when

neither the sender nor recipient have knowledge of that access), such access may not be prohibited by s108 (or any other provision) because in such circumstances the communications are arguably not "stored communications" as defined.

The above would be contrary to the situation that would have existed if the amendment to the definition had not been made for an unrelated reason during passage of the Bill through Parliament, and contrary to the intention of the specified purpose exceptions for carrier employees in s108(2)(d) and (e).

We consider item (c) of the definition of stored communication should be amended to state either:

- *"(c) cannot be accessed on that equipment, by a person who is not a party to the communication* ***and who is not an employee of the carrier****, without the assistance of an employee of the carrier"*; or
- *"(c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of* ***and/or involvement of*** *an employee of the carrier*".

7.2 Knowledge/Notice Provisions and Part 13/s280 of the TA

EFA has concerns about the amendment to section 108(1)(b) of the TIAA to provide that access via a carrier is not prohibited if it takes place with the knowledge of one of the parties to the communication/s and the related amendment inserting s108(1A) regarding the giving of written notice to a party to attain knowledge.

In our opinion, these amendments have resulted in less, not more, clarity and certainty than before the 2006 TI Bill was enacted.

EFA is under the impression that it was the government's intent that the TIAA as amended, effective from 13 June 2006, would be the sole legislative basis for accessing stored communications. However, in our view it remains uncertain as to whether that objective has been achieved due to the amendments to the 2006 TI Bill concerning 'notice' and the provisions of Part 13 of the *Telecommunications Act 1997* ("the TA").

The current situation appears to be as follows:

- If an enforcement agency has given written notice to a party to the communication/s of an intention to access same (s108), then it is not an offence under the TIAA to access those communications with the assistance of the carrier.
- However, the TIAA does not authorise access or disclosure, that is, it does not authorise carriers to disclose communications.
- Carriers remain prohibited from disclosing communications by Part 13 of the TA, unless an exception applies under that Act (or another Act).
- A relevant exception is Section 280(1)(a) of Part 13 of the TA which in effect allows carriers to disclose information or a document "*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*".

As a result, it appears that enforcement agencies, such as for example ASIC, now have two choices:

1. Obtain a stored communications warrant; or

2. Give written notice to a party (so that the TIAA s108 offence would not apply) and obtain a normal search warrant for execution on the carrier's premises.

Obviously if an agency desired covert access they would have to use option 1. However, option 2 has the potential to be used when a stored communications warrant could not be obtained by an

agency because the threshold for issue of a stored communications could not be met (e.g. the suspected offence does not carry a high enough penalty, or an issuing officer would consider that other factors resulted in issue of a stored communications being inappropriate).

EFA considers amendments are necessary to eliminate option 2 and ensure that a stored communications warrant is in fact the sole legislative basis for access to stored communications by agencies with the assistance of a carrier.

EFA would be opposed to any provisions that enabled agencies to access stored communications from a carrier by providing written notice of the intention to do so to one of the parties to the communication/s, whether or not an agency is also required to obtain a general search warrant. 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 notified by the agency of the intention to access communications at the carrier. Therefore there would be:

- potential for misuse of any such powers, i.e. failure to notify a party, by Commonwealth, State and Territory criminal law, civil penalty and public revenue enforcement agencies;
- carriers [includes ISPs] who disclosed the content of communications could be sued by a customer who had not been notified, under the civil remedy provisions of the TIAA and/or TA. In our view carriers should not be placed in the difficult position of having to decide whether to take such a risk or decline to provide the communications the agency claims to have a right to obtain from them.

To resolve the above issues, EFA considers s280(1)(a) of the TA should be amended as proposed in Section 4.2 hereof.

7.3 Access to communications that are not in the "possession" of the carrier, nor a party to the communication

It appears that the definition of "stored communication" may have created a loophole that may enable agencies to obtain access to communications that are intended (by government policy intent) to be regarded as "stored communications" without a stored communications warrant; and/or may enable Australian based telecommunications service providers to decline to provide communications required by stored communications warrant because the communications do not match the definition of "stored communications".

This is because the definition requires that the communications be held on equipment that is in the "possession" of a carrier, otherwise they are not "stored communications" as defined.

To address this issue, EFA considers item (b) of the definition of stored communication should be amended to state "in the possession or control of a carrier".

An example scenario is that an ISP may make daily or weekly etc backups of communications stored on their system and send the backup tapes/disks to another entity that is not a carrier but is in the business of providing secure off-site storage facilities. We understand some telecommunications service providers use such services with a view to assisting disaster recovery in the event of fire, flood, etc, at their own premises.

The question arises as to what type of lawful authority is necessary if an agency seeks to obtain access to communications held at that storage facility, e.g. with a general search warrant to be executed on those premises. If agencies can raid such data storage facilities or media directly (without the assistance of a carrier employee), they could access communications of parties not subject to the investigation. It should be remembered that this type of situation could exist under a State/Territory law/powers. Potential issues in relation to lawful access are more wide ranging than merely in relation to the AFP's, or ASIC's, powers under Commonwealth law.

EFA observes that the term "possession" in Commonwealth laws apparently does not necessarily encompass control in the absence of physical possession. For example, the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004* stated:

> "473.2 Possession or control of data or material in the form of data
> A reference in this Part to a person having possession or control of data, or material that is in the form of data, includes a reference to the person:
> (a) having possession of a computer or data storage device that holds or contains the data; or
> (b) having possession of a document in which the data is recorded; or
> (c) having control of data held in a computer that is in the possession of another person (whether inside or outside Australia)."

Accordingly, for clarity and certainty, the definition of stored communication should be amended to ensure that where communications are stored and in the control of a carrier, but not in their physical possession, such communications are legislatively regarded as stored communications and therefore cannot be accessed covertly by agencies without a stored communications warrant. As suggested above, item (b) of the definition of stored communication should be amended to state "in the possession or control of a carrier".

In relation to consideration of such an amendment, it may also be pertinent to note that some Australian based telecommunications service providers provide email services/boxes to their customers where the equipment on which the email boxes of the intended recipient is located is owned by, and in the premises of, other companies, including overseas companies. The Attorney-General's Department may wish to consider whether or not, if a stored communications warrant was served on such an Australian based service provider, the service provider would be justified in declining to provide the required access on the grounds that the subject communications do not meet the definition of "stored communications" because they are not "held on equipment that is operated by, and is in the possession of" the Australian based service provider. EFA considers adding "or control" as suggested above would eliminate the potential for such a possibility.

7.4 Type of lawful authority required for agency access to recordings made by a carrier and stored on a carrier's equipment

EFA has previously raised the question of whether a **copy** of a communication, for example copies made by recording onto back up tapes/disks for disaster recovery purposes, is encompassed within the definition of 'communication'.

We are of the view that the point we have been trying to make may not have been adequately understood by the Attorney-General's Department and therefore not addressed. For example, the Senate Legislation Committee Report[8] states:

> "*3.97 EFA suggest that copies of communications stored in a sender's sent box on a carrier's equipment, or communications stored on a carrier's backup device are examples of communications which may be regarded as copies of communications rather than stored communications.*
>
> *3.98 The Attorney-General's department advised:*
>
> > *A copy of a stored communication accessed by the person on the premises – so any end point of the communication – will not require a stored communications warrant. It is only those communications which are accessed directly from the carrier which will require a stored communications warrant.*"

It is the issue of a copy being accessed directly from a carrier that EFA seeks to have addressed, not a copy held "at any end point" as referred to by the Attorney-General's Department above.

EFA remains concerned that it could be argued that when, for example, an ISP makes a recording of a communication (normally of multiple communications, many of which would be unrelated to any particular investigation) onto a backup tape/disk that what is on that tape/disk is "a copy of a communication" not "a communication" and that as a result access could be obtained with the assistance of the carrier, but without a stored communications warrant, on claimed grounds that the material does not consist of communications, but of copies of communications, and therefore does not meet the definition of "stored communications".

Our concern in this regard is enhanced by the definition of accessing a communication:

> *6AA Accessing a stored communication*
> *For the purposes of this Act, accessing a stored communication consists of listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.*

The above definition shows that "a communication" and "a recording of a communication" could be regarded as two different things. The issue of concern therefore is what type of lawful authority is necessary for an agency to access, directly from the carrier, "a recording of a communication" that has been made by the carrier (e.g. made lawfully under an exception to the prohibition on access such as backup for maintenance/disaster recovery purposes).

EFA agrees with Recommendation 14 of the Senate Legislation Committee:

> "*3.107 The Committee recommends that the Bill be amended to ensure that copies of communications can not be accessed without a stored communications warrant.*"[8]

We had previously recognised that making an appropriate amendment was somewhat problematic due to the definition in the 2006 TI Bill referring to being accessible by the intended recipient. However, an amendment to that definition for other reasons removed that reference.

We therefore now suggest the definition of "stored communication" be amended to state:

> "**stored communication** means a communication (and includes a copy of a communication) that:"

We are under the impression such an amendment would be consistent with the government's policy objective, i.e. that it would not change the intent of the existing Act. We also wish to make clear that we are not concerned about for example the AFP misunderstanding the legislation. We are concerned about the multitude of agencies, including State/Territory agencies, that are no longer prevented from accessing stored communications and the potential for carriers to be presented with general search warrants requiring access to "copies" on e.g. backup tapes and carriers, including small ISPs, having to attempt to correctly interpret legislation that in our opinion is insufficiently clear in this regard at present.

7.5 Definition of accessing a stored communication and "record"

We remain of the view that the definition of "record" should be amended so that it applies in relation to, not only an interception, but also accessing a stored communication. This matter is discussed in detail in s3.1.2 of our submission to the Senate Legislation Committee[11]. See also Senate Committee Recommendation 15[8]:

> "*3.108 The Committee recommends that the definition of 'record' be amended so that it applies in relation to accessing a stored communication.*"

We note that this matter was raised during the Committee hearing and Mr Gifford remarked that "*This is the first time I have had a chance to have a look at this particular part of the EFA submission. It is certainly something that we are more than open to considering.*" We had hoped that

the reason it was not dealt with before passage of the 2006 TI Bill was lack of time and that it would be incorporated in forthcoming amendments.

However, such an amendment is not included in the Bill. We remain of the view that it should be.

7.6 Inappropriate requirement to notify carriers of remote access to communications during execution of s3L warrant

As the 2006 TI Bill amendments to the TI Act appear to have made clear that the AFP is not prohibited from remotely accessing communications stored on a carrier's equipment when executing a warrant authorising them to search a residence (etc) and computer equipment therein, EFA continues to be of the view (as stated in s6.2.1 of our submission to the Blunn Review[12]) that subsection 3LB of the Crimes Act must be amended to prohibit notification to telecommunications service providers in such circumstances.

In this regard, subsection 3LB states that if "data that is held on premises other than the warrant premises is accessed under subsection 3L(1)" the executing officer must "notify the occupier of the other premises that the data has been accessed under a warrant" as soon as it is "practicable" to do so.

It is totally inappropriate for police to disclose to a telecommunications service provider (the occupier of the other premises) that they have remotely accessed a customer's email under warrant executed at the customer's premises. This type of information about a customer should not be disclosed to the service provider; it is none of the service provider's business.

Amendment to subsection 3LB of the Crimes Act is essential to protect the right of individuals whose premises are searched not to have personal, or any other, information about them unnecessarily disclosed to uninvolved parties by law enforcement agencies.

7.7 Recommendations of the Senate Legal and Constitutional Legislation Committee

The recommendations of the Senate Legal and Constitutional Legislation Committee[8] in relation to the stored communications provisions of the 2006 TI Bill, included a number of recommendations addressing issues of concern raised by EFA. We understood from the Minister for Justice's remarks during the 2006 Senate chamber debate that the Committee's recommendations would be further considered by the government with a view to possibly further amendments in the spring sessions.

However, it appears from the Bill that the majority of the Committee's recommendations are not to be implemented. EFA hopes that the Attorney-General's Department and/or the Government intends to issue a public response to the Committee's Report on the 2006 TI Bill explaining why the recommendations are, apparently, not being implemented.

---

8. Conclusion

EFA strongly supports proposed s172 which would satisfactorily resolve the long ongoing issue of whether s282(1) and (2) of the TA might allow disclosure of the contents or substance of a communication, (without a warrant or even certificate).

However, the majority of other proposed changes in relation to interception and access are of major concern to EFA, such that any advantages of enactment of this Bill are outweighed by disadvantages because it would not establish an appropriate balance between protecting the privacy of users of the telecommunications system and meeting legitimate needs for access by security and law enforcement agencies.

As a result, EFA is unable to support passage of the proposed legislation in its current form.

EFA considers it highly unlikely that this Bill could be adequately and appropriately patched (amended) during its passage through Parliament. Attempts to do so are likely to unintentionally introduce additional areas of lack of clarity and certainty given the existing complexity of both the TIAA and TA and inter-relationship between those Acts.

Accordingly, EFA recommends that this Bill be rejected by the Parliament. EFA considers legislative drafters should go back to the drawing board and develop a replacement Bill which appropriately addresses matters raised in this submission, and also in the recommendations of the Senate Legal and Constitutional Legislation Committee's Report on the provisions of the *Telecommunications (Interception) Amendment Bill 2006.*

---

9. References

1. Telecommunications (Interception and Access) Amendment Bill 2007
<http://parlinfoweb.aph.gov.au/piweb/TranslateWIPILink.aspx?Folder=
BILLS&Criteria=BILL_ID:r2743%3BSEQ_NUM:0%3B>

2. Blunn Report of the Review of the Regulation of Access to Communications, August 2005.
<http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Blunnreportofthereviewofthe
regulationofaccesstocommunications-August2005>

3. Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment Bill 2007
<http://parlinfoweb.aph.gov.au/piweb/TranslateWIPILink.aspx?Folder=
EMS&Criteria=BILL_ID:r2743%3BEM_TYPE:EM%3BSOURCE:House%3B>

4. Zero in on the business target, Next, Sydney Morning Herald, 6 Feb 2007
<http://www.smh.com.au/news/biztech/zero-in-on-the-business-target/2007/02/
05/1170524024923.html>

5. GOFINDER® Mobile - Terms & Conditions of Use (accessed 7 July 2007).
<http://www.gofinder.net/gofinder/GoFinder_Mobile/terms.htm>

6. Exposure Draft of Telecommunications (Interception and Access) Amendment Bill 2007, February 2007.
<http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Exposuredrafttelecom
municationsinterceptionprovisions-February2007>

7. The Internet Archive's Wayback Machine
<http://www.archive.org/>

8. Senate Legal and Constitutional Legislation Committee Report and Recommendations, Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006, 27 March 2006.
<http://www.aph.gov.au/senate/committee/legcon_ctte/ti/report/index.htm>

9. EFA submission on the Exposure Draft of Telecommunications (Interception and Access) Amendment Bill 2007, 23 February 2007
<http://www.efa.org.au/Publish/efasubm-agd-tia-expdraft-2007.html>

10. ACMA Determination of Requirements Certificates under subsections 282(3), (4) or (5), 10 December 1998.
<http://www.acma.gov.au/ACMAINTER.1638528:STANDARD::pc=PC_335>

11. EFA submission to the Senate Legal and Constitutional Legislation Committee, Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006, 12 March 2006.
<http://www.efa.org.au/Publish/efasubm-slclc-tiabill-2006.html#47_19>

12. EFA submission to the Blunn Review of the Regulation of Access to Communications under the Telecommunications (Interception) Act 1979, 20 May 2005.
<http://www.efa.org.au/Publish/efasubm-agd-tiactreview2005.html>

10. About EFA

Electronic Frontiers Australia Inc. ("EFA") is a non-profit national organisation representing Internet users concerned with on-line rights and freedoms. EFA was established in January 1994 and incorporated under the *Associations Incorporation Act* (S.A.) in May 1994.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of computer based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA policy formulation, decision making and oversight of organisational activities are the responsibility of the EFA Board of Management. The elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities.

EFA has long been an advocate for the privacy rights of users of the Internet and other telecommunications and computer based communication systems. An EFA representative was an invited member of of the Federal Privacy Commissioner's National Privacy Principles Guidelines Reference Group and the Research Reference Committee (2001) and the Privacy Consultative Group (2004-2005). EFA participated in NOIE's Privacy Impact Assessment Consultative Group relating to the development of a Commonwealth Government Authentication Framework (2003), Centrelink's Voice Authentication Initiative Privacy Impact Assessment Consultative Group (2004-2007), the ENUM Discussion Group and Privacy & Security Working Group convened by the Australian Communications and Media Authority ("ACMA" formerly ACA) (2003-2007), and the ACA's Consumer Consultative Forum meeting (April 2005). EFA has presented written and oral testimony to Federal Parliamentary Committee and government agency inquiries into privacy related matters, including amendments to the *Privacy Act 1988* to cover the private sector, telecommunications interception laws, cybercrime, spam, etc.
