Electronic Frontiers Australia Inc

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

26 July 2004

The Secretary
Senate Standing Committee for the Scrutiny of Bills
Suite SG − 49, Parliament House
CANBERRA ACT 2600

Email: scrutiny.sen@aph.gov.au

Dear Mr Pye

Subject: Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation

Please find attached 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.

EFA's Executive Director is based in Brisbane and can be contacted directly at the telephone and fax numbers shown above and by email to ed@efa.org.au.

Yours sincerely

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)
Submission to

Senate Standing Committee for the Scrutiny of Bills re Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation

26 July 2004

Contents:

---

1. Introduction

This submission is provided in response to the Committee's letter dated 13 April 2004 inviting Electronic Frontiers Australia Inc. ("EFA") to make a submission.

EFA welcomes the Committee's Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation and appreciates the opportunity to make a submission. We thank the Committee for granting EFA an extension of time to prepare and lodge a submission. As advised to the Acting Secretary on 28 June, we were unable to prepare a submission prior to the Committee's preferred date because there had been six other Commonwealth Parliamentary and government agency inquiries during the same period involving issues of serious concern to EFA. The majority involved search/seizure provisions in proposed legislation.

EFA is of the view that if all proposed Commonwealth legislation fully and transparently complied with the principles set out in the Committee's April 2000 *Report on the Inquiry into Entry and Search Provisions in Commonwealth Legislation*, EFA would spend less time criticising proposed legislation and advocating amendments to same.

This submission addresses items (1), (2) and (3) of the Inquiry Terms of Reference.

We provide examples of legislation that has been drafted since the Committee's 2000 Report which in our opinion demonstrate that there has been insufficient impact on the practices and drafting of entry and search provisions.

We also provide information concerning the taking of material, particularly from computers, that is not relevant to an investigation and the use and protection of such material. We believe the rights and liberties of individuals would be better protected by the development of protocols governing the seizure of material.

▲ Go to Contents List

2. 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 ten elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities. The role of Executive Director was established in 1999 and reports to the Board.

EFA has long been an advocate for the privacy rights of users of the Internet and other telecommunications and computer based communication systems. EFA's Executive Director was an invited member of the Federal Privacy Commissioner's National Privacy Principles Guidelines Reference Group and Research Reference Committee during 2001. EFA participated in NOIE's Privacy Impact Assessment Consultative Group relating to the development of a Commonwealth Government Authentication Framework in 2003 and is currently participating in Centrelink's Voice Authentication Initiative Privacy Impact Assessment Consultative Group and the ENUM Privacy and Security Working Group convened by the Australian Communications Authority. EFA has presented oral testimony to Federal Parliamentary Committee inquiries into privacy related matters, including amendments to the *Privacy Act 1988* to cover the private sector, telecommunications interception laws, cybercrime, spam, etc.

▲ Go to Contents List

3. Spam (Consequential Amendments) Act 2003

The *Spam (Consequential Amendments) Act 2003* ("SCA Act")[1] was enacted in conjunction with the *Spam Act 2003*[2] and amended the *Telecommunications Act 1997*[3] (and other Acts).

As stated in EFA's submission to the inquiry into the Spam Bills 2003[4] conducted by the Senate Environment, Communications, Information Technology and the Arts Legislation Committee, EFA strongly objects to the following provisions of the SCA Act:

a. the assistance order provisions that enable a suspect or other person who has forgotten or lost a password, encryption key or other information to be imprisoned for six months, although even a person found guilty of breach of the *Spam Act 2003* is not subject to imprisonment. This provision is completely absurd in legislation that does not involve imprisonment even when a person is found guilty of having sent spam;
b. the search and seizure provisions that empower government employees and police to search and seize an individual's computer and other possessions *without* a search warrant and *without* the consent of the relevant individual; and
c. the search and seizure powers (both with and without a warrant) applicable to the premises and possessions of a **recipient** of spam, i.e. a person who is a victim of a spammer, and who is not suspected of having breached the *Spam Act 2003*; and
d. that the legislation may have the apparently unintended consequence of authorising an Internet Service Provider ("ISP") to allow an ACA inspector (i.e. a civil penalty−enforcement agency employee) to search the ISP's customers' email boxes without a warrant or even a written request due to the pre−existing "reasonably necessary assistance" provisions of Section 282(2) of the *Telecommunications Act 1997*.

Further information concerning (a) above is provided later herein under the heading *Assistance Orders and Imprisonment Penalties*.

Issues referred to in (b), (c) and (d) above are discussed in detail in the following extract (updated to present tense) from EFA's submission concerning the SCA Bill under the headings:

- Search and Seizure Powers
- Searches without a warrant
- Searches of innocent recipients' homes and possessions
- Searches of stored messages/ISP equipment without a warrant

It should be noted that amendments addressing some of the issues below were made to the Bill by the Senate, however the government/House refused to support those amendments and subsequently the major parties in the Senate failed to insist on the Senate's previously passed amendments. EFA finds the blatant disregard for individuals' privacy rights and other civil liberties extremely disturbing.

The section numbers below refer to the relevant sections of the *Telecommunications Act 1997* as amended by the SCA Act.

Search and Seizure Powers

EFA is highly concerned by the search and seizure powers effected by the *Spam (Consequential Amendments) Act 2003* ("SCA Act") that do not require a warrant.

Inspectors (who are ACA appointed full−time, part−time or temporary Commonwealth or State Government employees and police officers) have been empowered to enter and search homes *without* a warrant and *without* the consent of the relevant occupier of the home, that is, without the consent of the owner of the things (computers, files, documents, etc) to be searched and potentially seized.

These provisions fail to strike an appropriate balance between enforcing the proposed law and the privacy of individuals and families, including the privacy of people who are not suspects.

The SCA Act empowers inspectors to conduct two types of searches, both of which may be conducted with, and without, a warrant:

1. Searches **relating to breaches** of the *Spam Act 2003* may be conducted either:
    a. **with a search warrant** issued by a magistrate (s.535) if an inspector suspects on reasonable grounds that there **may** be something related to breach of the Spam Act 2003 on any land, or in or on any premises, vessel, aircraft or vehicle, or
    b. **without a search warrant**, with the consent of the **owner or occupier** (s.542) of the land, premises, vessel, aircraft or vehicle, if an inspector suspects on reasonable grounds that there **is** on any land, or on or in any premises, vessel, aircraft or vehicle "anything connected with" a particular breach of the Spam Act 2003.

    In either instance, an inspector may enter; search; break open and search a cupboard, drawer, chest, trunk, box, package or other receptacle, whether a fixture or not; and examine and seize anything that the inspector suspects on reasonable grounds to be "connected with" the offence or breach (s.542(2)).
2. Searches **to monitor compliance** with the *Spam Act 2003* ("for the purpose of finding out whether the *Spam Act 2003* has been complied with") may be conducted:
    a. **with a monitoring warrant** issued by a magistrate (s.547D), or
    b. **without a warrant**, with the consent of the **occupier** (s.547A).

    In either instance, an inspector may enter any premises and exercise the monitoring powers (s.547D(5)(a) and s.547A) set out in s.547B which include:

    > (a) to search the premises;
    > (b) to inspect and take photographs, or make sketches, of the premises or any substance or thing at the premises (including operate equipment at the premises to determine whether it or a disk, tape or other storage device contains relevant information (s.574B(2)) and if so put the information in documentary form or on a storage device and remove it from the premises (s.574B(3));
    > (c) to inspect any document kept at the premises;
    > (d) to remove, or make copies of, any such document;
    > (e) to take onto the premises such equipment and materials as the inspector requires for the purpose of exercising powers in relation to the premises;
    > (f) to secure a thing, until a warrant is obtained to seize it,

(g) to secure a computer, until an order under section 547J (an access assistance order) is obtained in relation to it.

Note: Items (e) to (g) above are new powers that inspectors did not previously have in relation to enforcement of Part 21 − Technical Regulations. The powers in item (b) above to operate equipment, copy and remove information on disks etc. are also new powers.

Searches without a warrant

EFA is strongly opposed to the provisions empowering inspectors to conduct searches **without** a warrant for the reasons set out below.

Section 542 (searches relating to breaches of the Spam Act) gives inspectors the power to enter and search homes and property therein without a warrant and without the consent of the owner of the things (computers, files, documents, etc) to be searched and potentially seized and without the consent of the occupier. For example an inspector could enter a home with the consent of the landlord (the owner) and search the tenants' computers and other possessions. In addition, in the case of a residence shared by several people (e.g. joint owners/tenants, flat mates, family, etc.), an inspector could enter the home with the consent of one occupier and search possessions belonging to a different occupier, and computers used by more than one person.

Sections 547A and 547B (searches to monitor compliance with the Spam Act) also give inspectors the power to enter and search homes and property therein without a warrant and without the consent of the relevant occupier, although they do not allow inspectors to conduct searches with the consent of a landlord, only of one of the occupiers. (It is unclear why searches relating to breaches (s.542) may be conducted with the consent of the owner/landlord, but not searches to monitor compliance (s.547)).

The above circumstances apparently arise because inspectors' powers prior to the SCA Act to enter and search premises with the consent of the owner or occupier were extended to suspected breaches of the *Spam Act 2003*. However, inspectors' previous powers were limited to enforcement of Part 21 of the *Telecommunications Act 1997* dealing with technical regulations. As such, they were only empowered to conduct searches in peoples' home to investigate matters such as whether illegal customer telephone equipment and/or cabling has been connected to the telecommunications network and/or compliance with the conditions of a connection permit. These matters can normally be ascertained without searching individuals' filing cabinets and cupboards, and certainly without searching individuals' computers and email etc.

The previous search powers were therefore far less privacy intrusive than those introduced by the SCA Act which permit inspectors to search through people's personal possessions such as their computers and email without a warrant. While arguably inspectors may have had such powers previously, it seems most unlikely an inspector could have legitimately claimed a necessity to search a computer to see whether illegal telephones or cabling were installed in the premises.

Furthermore, a search of a suspect's computer (including email etc) is very likely to invade the privacy of innocent people who have been in contact with the suspect at some time, and innocent people who use the same computer as a suspect. In this regard, the new search powers are as privacy invasive as interception of a telephone call − during which the conversation of people who are not suspects are monitored as well. This is a primary reason for the special and strict rules applicable to issue of a telecommunications interception warrant. It is completely inappropriate to permit inspectors to search email without a warrant of any type. Judicial scrutiny is required to minimise the potential for invasion of the privacy of non−suspects and innocent persons without adequate justification.

In addition, under Sections 547A and 547B (searches to monitor compliance with the Spam Act), an inspector is empowered to enter and search a residence without a warrant in circumstances in which they would not be able to obtain a monitoring warrant. The SCA Act states that monitoring warrants must not be issued by a magistrate unless an individual who ordinarily resides at the premises has either been found by the Federal Court in the last 10 years to have breached the *Spam Act 2003* or has previously given an undertaking to comply (s.547D(4)). Contrary to these provisions however, an inspector will be empowered to enter and search a residence, *without* a warrant, when:

- no person who ordinarily resides at the premises has previously been found to have breached the *Spam Act 2003* or has given an undertaking to comply; or
- it is more than 10 years since the Court finding or undertaking was given.

This situation is unsatisfactory because inspectors' powers in relation to monitoring compliance by a prior offender appear to be more extensive than in relation to searches associated with a person who is not a prior offender. It appears these more extensive powers, which are able to be used without a warrant in circumstances in which a warrant could not be obtained, could be conveniently used to conduct searches associated with persons who are **not** prior offenders. While any evidence obtained in such circumstances may not be admissible in a Court, the SCA Act seems to facilitate or enable the potential use of the extra privacy invasive monitoring powers in relation to non prior offenders.

Searches of innocent recipients' homes and possessions

Both Sections 535 (with search warrant) and 542 (without search warrant) enable searches of the homes and other premises of ***recipients*** of spam.

This situation appears to arise because the entry and search powers are not limited to premises/property associated with a suspect, but apply to:

- "anything that may afford evidence about a breach" (s.535(1)), and
- a "thing" that is "connected with a particular breach" (s.542(1)).
  The SCA Bill states that "a thing is connected with a breach of the *Spam Act 2003* if it is ... a thing that may afford evidence about the breach" (s.541A).

Obviously, an unsolicited commercial electronic message that has been received is a thing that may afford evidence about a breach. While it may be considered unlikely that inspectors would search the homes of recipients of spam, it is essential that the law specifically not allow that to occur without the consent of the relevant individual, e.g. the owner of the computer, email or "thing", as applicable, to be searched.

EFA notes that some proponents of the Acts regard the provision enabling search of innocent recipients' homes and possessions as unimportant because they do not expect the law would be used for that purpose. EFA considers a law enacted on the basis that it would only be applied selectively is a bad law. Such laws are not only open to abuse, they bring the law and the Parliament's competence into disrepute. If particular provisions of the proposed law would not be used, they should be deleted from the Bills.

EFA is aware it has been claimed that recipients of spam should not be outside the scope of the search and seizure provisions because spammers would include themselves on their own mailing lists and claim "recipient" status. This argument is unpersuasive because it is readily possible to avoid that situation without permitting searches of the property and possessions of recipients of spam who are not suspected on reasonable grounds of being in breach of the law.

Searches of stored messages/ISP equipment without a warrant

In addition, the enactment of the *Spam Act 2003* apparently has the effect of authorising an Internet Service Provider ("ISP") to allow an ACA inspector (i.e. a civil penalty−enforcement agency employee) to search the ISP's customers' email boxes (possibly including the actual content of messages) without a warrant under the existing "reasonably necessary assistance" provisions of Section 282(2) ("Law enforcement and protection of public revenue") of the *Telecommunications Act 1997*.

In this regard, the removal of the owner/occupier consent provisions (as recommended earlier herein) may be insufficient to ensure a warrant is required for searches of communications information held by ISPs because the existing provisions of Section 282 of the *Telecommunications Act 1997* appear to be applicable to investigation of suspected breaches of the *Spam Act 2003*.

EFA has long been of the view that Sections 282(1) and (2) of the *Telecommunications Act 1997* require amendment to ensure that the content of messages cannot be accessed by law enforcement agencies without a warrant, in order to adequately protect Internet users' privacy and minimise the potential for "fishing trips" without a warrant. Whether or not Sections 282(1) and (2) authorise disclosure of the *content* of communications (as distinct from, for example, the 'To' and 'From' fields of messages) has long been a recognised grey area of the *Telecommunications Act 1997*. (See for example Section 4.3 of the *Telecommunications Interception Policy Review − May 1999* issued by the Attorney−General's Department[5].)

Further information concerning Section 282 of the *Telecommunications Act 1997* is provided below.

▲ Go to Contents List

4. Telecommunications Act 1997

EFA submits that Section 282 of the *Telecommunications Act 1997* is in need of urgent law reform to achieve an appropriate balance between the privacy rights of law−abiding citizens and the legitimate needs of law enforcement agencies. EFA considers the existing provisions too readily facilitate fishing trips by government agencies, lack adequate controls and safeguards and are being used for purposes not envisaged by the Parliament.

Section 282 of Part 13 of the *Telecommunications Act 1997* authorises criminal law enforcement, public revenue and civil penalty enforcement agencies (defined in Section 282(10) of the Act) to obtain/seize information about individuals and their communications from telecommunications carriers and carriage service providers, including Internet Service Providers ("ISPs"), without obtaining a warrant and, in approximately half a million instances each year, without even preparing a written request.

Section 282 permits covert seizure of information about individuals by way of a certified request or an uncertified request (made by an officer of an agency) to a telecommunications service provider:

- Certified Requests
  Sections 282(3), (4) and (5) permit government agencies to obtain/seize information and documents about individuals and their communications from telecommunications service providers by making a certified request stating that the disclosure is "reasonably necessary" for the enforcement of the criminal law, or the enforcement of a law imposing a pecuniary penalty, or the protection of the public revenue. A certified request cannot, however, be used to lawfully obtain the *content* of communications (as stated in Section 282(6)).
- Un−certified Requests
  Sections 282(1) and (2) are of even greater concern than the above. These provisions permit telecommunications service providers to disclose documents and information about individuals and their communications to government agencies without a warrant or even a written certified request, if the service provider considers the disclosure or use is "reasonably necessary" for the enforcement of the criminal law, or the enforcement of a law imposing a pecuniary penalty, or the protection of the public revenue. The Act is silent on whether or not Sections 282(1) and 282(2) permit disclosure of the content of communications. While s282(6) states that a certified request can not be used to obtain content of communications, it does not mention the use of un−certified requests in this regard.

EFA submits that Section 282 is in need of urgent law reform to clearly exclude the use of uncertified requests under s282(1) or (2) to obtain/seize the content of communications and ensure a warrant is required.

The Attorney−General's Department acknowledged the possibility of obtaining the content of communications under Section 282(1) and (2) of the *Telecommunications Act* (i.e. without a warrant of any type) in their 1999 Report titled *Telecommunications Interception Policy Review*[5] and this aspect of the *Telecommunications Act* has not been amended since 1999. The Report states:

> "Section 4.3 − Access to stored data
> ...
> 4.3.11 Access by enforcement agencies to information held by C/CSPs [under the Telecommunications Act] is by means of two primary mechanism, certified and uncertified requests.

> 4.3.12 Subsection 282(6) of the Telecommunications Act provides that the certificate provisions [also known as certified requests] in subsections 282(3), (4) and (5) **do not apply** to the contents of a communication whether or not the communication has been received by the intended recipient. [emphasis added]
>
> 4.3.13 However, this still leaves the possibility that subsections 282(1) and (2) [non−certified requests] can apply in respect of the content of stored communications. That is, an enforcement agency (including civil penalty−enforcement and public revenue protection agencies) could get access to the contents of a stored communication if the disclosure of the stored communication is reasonably necessary for one of the purposes listed in subsections 282(1) and (2). [i.e. enforcement of a criminal law or a civil law]
>
> 4.3.14 The draft ACIF Assistance to Enforcement Agencies Code has had to address this issue. ... Currently Clause 2.7.2 says−
> 'S282(1) and (2) may authorise disclosure of content and substance. In view of the sensitive nature of the disclosure where content and substance are involved it would be prudent for Organisations (that is carriers and carriage service providers) to obtain legal advice. ...' "
>
> [Note: The same Clause 2.7.2 was contained in final industry code issued in 2001 − ACIF C537:2001.]

The uncertainty concerning s282(1) and (2) is also apparent in documents issued by the Australian Communications Authority ("ACA"). The ACA's Fact Sheet *Internet Service Providers and Law Enforcement and National Security*[6] states:

> "What about stored communications?
> Access to the content of communications (for example, electronic mail) stored on an ISP's server is unlikely to fall within reasonably necessary assistance [i.e. s282(1) and (2)]. An agency may use a general search or interception warrant or some other statutory provision to access stored communications."

That the ACA is only able to say "unlikely" demonstrates that they, like the Attorney−General's Department, recognise the possibility that s282(1) and (2) might apply in respect of the content of stored communications. Obviously the *Telecommunications Act* is insufficiently clear to ensure protection of the contents of communications from access/seizure without a warrant.

During the 2002−2003 year, there were 400,766 instances in which government agencies obtained information about individuals and their communications from telecommunications service providers and number database operators without a warrant or even certificate (i.e. non−certified requests under s282(1) and (2)). This is 60% of the total disclosures (666,521) under Part 13 of the Act. Certified requests were used in 251,077 instances (37%). Warrants (s280) were obtained in less than 3,109 instances (0.47%). (Source: ACA Annual Report 2002−2003[7]).

Section 282 is very frequently used to obtain call charge records etc. It enables disclosure of information such as customer identification details and the source, path and destination of communications (for example, telephone numbers dialled, and the "To" and "From" fields of an email message, etc).

It is of significant concern to EFA that Section 282 has also been used to obtain details of all web pages etc that Internet users visit − names/URLs of files and pages down loaded − over a period of

time. It is not known whether certified, or uncertified, requests have been used in such instances. It appears highly unlikely that the Parliament envisaged such use of either certified or uncertified requests because at the time the Telecommunications Bill was introduced into Parliament in 1996 few, if any, politicians had sufficient knowledge and understanding of the technology of the Internet to be aware of the potential for such use of s282.

EFA also submits that the existing provisions lack adequate controls and safeguards. The current provisions far too readily facilitate "fishing trips" by government agencies. Further, there is no means knowing whether uncertified requests have been used to seize the content of communications nor whether certified or uncertified requests have been used to surveil Internet users and seize details of information they view, distribute or download.

Although telecommunications service providers are required to record details of disclosures (s.306) and give a written report concerning such disclosures to the Australian Communications Authority Authority ("ACA") annually (s.308), the ACA is not required to monitor compliance with this aspect of the law, nor to publish statistics or any other information, nor report to the Minister or Parliament on the matter.

The Act confers the function of monitoring compliance with the law concerning disclosures on the Privacy Commissioner (s. 309) including "whether a record made under section 306 sets out a statement of the grounds for a disclosure; and whether that statement is covered by Division 3 (which deals with exceptions)". However, the Commissioner's office is under funded and under staffed.

The Privacy Commissioner informed a Senate Estimates Committee in February 2003 that due to the number of complaints being received since the commencement in December 2001 of privacy laws covering the private sector, it had been necessary to divert staff from other areas of the office to the complaints area. The Commissioner advised that in the 2002−2003 year his office would undertake only four audits of Commonwealth and ACT agencies and people who fall under the credit provisions of the Privacy Act. Senator Ellison informed the Committee that "The government is well aware of what Mr Crompton has said and the matter is being considered in the budgetary context. ... But this budget, as the Treasurer has said, is going to be a tight one because of other demands of the budget, and everything will have to be considered in that light" [8].

The Privacy Commissioner's ability to monitor compliance with the *Telecommunications Act* was not discussed during the above hearing. However, it appears most unlikely that Commissioner's office is sufficiently well funded and staffed to be able to adequately do so.

Furthermore, the Telecommunications Act does not require the Privacy Commissioner to report to the Minister, nor the Minister to report to the Parliament, concerning compliance with the privacy and disclosure provisions of the law.

EFA submits that the *Telecommunications Act* should be amended to require the Minister to issue a report annually concerning disclosures of information, including the effectiveness of such disclosures in combatting crime, that is, similar to reports required to be issued in accord with Part IX Division 2 of the *Telecommunications Interception Act*.

▲ Go to Contents List

5. Cybercrime Act 2001 / Crimes Act 1914

The *Cybercrime Act 2001* amended the *Crimes Act 1914* and was rushed through Parliament in the wake of September 11. It contains a number of poorly drafted and problematic provisions, at least two of which are relevant to the Committee's current inquiry:

a. Assistance orders involving imprisonment penalties which are discussed later herein under the heading *Assistance Orders and Related Imprisonment Penalties*;
b. New search and seizure powers allowing agencies to remotely search computers, as discussed below.

The *Cybercrime Act 2001*[9] amended the search and seizure provisions of the *Crimes Act 1914*[10] by, among other things, inserting Section 3L which states that when executing a search warrant the officer "may operate electronic equipment at the warrant premises to access data (including data not held at the premises)".

EFA submits that Section 3L of the *Crimes Act 1914* should be amended to plainly exclude its use for the purpose of covert search and seizure of the content of communications stored on telecommunications service providers' equipment.

Whether or not s3L currently permits such search and seizure has become the subject of much controversy this year following it becoming publicly known during a Senate Legal & Constitutional Legislation Committee inquiry[11] that government agencies and their legal advisers disagree about the correct interpretation of the law. The Australian Federal Police, relying on the advice of the Commonwealth Director of Public Prosecutions, contend that s3L allows them to remotely access and seize the content of communications. However, the Attorney General's Department, relying on the opinion of the Solicitor−General, contends that Section 3L does not over−ride the *Telecommunications (Interception) Act 1979*, that is, that agencies cannot use s3L and must obtain a telecommunications interception warrant to access the content of emails, SMS and voice mail messages temporarily delayed and stored during transit[11].

In EFA's opinion, it is also unclear whether or not s3L permits covert access and seizure of the content of communications that remain stored on telecommunications service providers' equipment after a message has been delivered to the intended recipient (as distinct from communications temporarily stored during transit). EFA is of the view that this is debatable given the definition of "data" in the *Crimes Act 1914* and also the definition of communication in telecommunications legislation. It may become even more debatable after definitions of "data" and "communication" in the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004*[12] are enacted.

EFA submits that covert, remote access to and seizure of the content of communications stored on service providers' equipment should not be permitted under general search warrants because the information obtained invades the privacy of law−abiding third parties who are not suspects, that is, any person who has been in communication with a suspect. Remote search and seizure is especially inappropriate because it constitutes secret surveillance that is vastly more open to misuse of search powers than are search warrants executed on a suspect's premises or on a telecommunications service provider's premises.

▲ Go to Contents List

6. Assistance Orders and Related Imprisonment Penalties

Both the *Cybercrime Act 2001* (establishing s3LA of the *Crimes Act 1914* and s201A of the *Customs Act 1901*) and the *Spam (Consequential Amendments) Act 2003* (establishing s547J of the *Telecommunications Act 1997*) contain assistance order provisions which enable imprisonment for six months of a person who has lost or forgotten a password or encryption key. EFA objects to these provisions and considers the provision in the *Spam (Consequential Amendments) Act 2003* to be even more problematic than that in the *Cybercrime Act 2001*.

Section 547J of the *Spam (Consequential Amendments) Act 2003* (as incorporated into the *Telecommunications Act 1997*) enables a person to be imprisoned for six months for failure to provide information, notwithstanding that even a person found guilty of committing the offence of sending spam is not subject to imprisonment.

Section 547J empowers a magistrate to issue an order compelling a person who is "reasonably suspected of having been involved in a breach" to disclose encryption keys and/or passwords and any other any information or assistance that is considered "reasonable and necessary" to allow an inspector "to do one or more of the following:

> (a) access data held in, or accessible from, a computer that is on those premises;
> (b) copy the data to a data storage device;
> (c) convert the data into documentary form."

The penalty for failure to provide the information or assistance is imprisonment for six months.

A person who is merely suspected of having been "involved in" sending one single unsolicited commercial electronic message (spam) could be the subject of an order and imprisoned for six months if they decline, or are unable, to provide the required information or assistance.

It is completely absurd that a person who is merely suspected of having been involved in a breach could be imprisoned for six months for failing to provide information or assistance to an investigator, when they could not be imprisoned even if they were found guilty of having committed the suspected breach.

These provisions are a great example of overkill. They are almost identical to those in the *Cybercrime Act 2001* (as incorporated in the *Crimes Act 1914*), although sending unsolicited commercial electronic messages (spam) is *not* a *criminal* offence.

The only difference between the assistance order provisions of the Spam Acts and the *Cybercrime Act* is that under the Spam Acts an order would be obtainable in relation to a larger number of people than under the *Cybercrime Act*. The *Cybercrime Act* provision is limited to persons "reasonably suspected of having **committed an offence**" while the Spam Act provision applies to persons "reasonably suspected of having been **involved in the breach**".

These types of assistance orders have long been controversial in relation to criminal offences and are even more controversial in relation to non−criminal offences. As the drafters of the Model Criminal Code ("MCC") stated (in Chapter 4 of the MCC Report):

> *The issues involved are both difficult on a technical level and controversial in relation to the protection of individual human rights and the rights of corporate entities.*

The matter of assistance orders is aimed squarely at the problems presented by security passwords and, more particularly, encrypted data. One of the major problems is the cursory treatment of the requirement for persons to reveal encryption keys.

There may sometimes be legitimate reasons why a password, private key or plain text could not be handed over to an Australian Communications Authority spam inspector or law enforcement agency, and it would be difficult for the subject of an assistance order to provide proof that they did not possess or have access to a key or plain text. The prospect of users of encryption being jailed despite having genuinely lost their private keys is a major and quite legitimate concern. Any legislation containing such provisions should, at the very least, provide an indication as to how those served with assistance orders requiring provision of plain text or encryption keys or a password can successfully prove that they cannot comply with the order.

It is also of concern that these requirements will rapidly fall behind the technology that is being used for encryption and data protection. For example, various biometrics around voice recognition (that may not work with a shaky voice), various movement registers such as keystrokes, mouse movements, etc. All of these could very be feasibly be "lost" by an individual during the stress of an investigation.

Furthermore, the 1997 OECD cryptography guidelines, which Australia has adopted, specifically recognize the fundamental right of privacy in relation to encrypted data:

> *Article 5. The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.*

A further problem is that a single encryption key often serves the dual purpose of ensuring confidentiality and providing secure authentication of the signatory to a document (through a digital signature). Revealing the key (or the passphrase thereto) can therefore compromise the integrity of the owner's digital signature. (It should be noted that a person on whom the assistance order is served is not assumed to have committed a breach.)

In addition, increasing numbers of individuals are becoming conscious of the risks of disclosure of private and/or business information in the case of loss or theft of computers and therefore encrypt the entire hard drive of the computer. It is completely unreasonable that a person can be required to give up the "keys to the castle" to provide an investigator with access to a single piece of email or data.

Clearly there is tension between privacy rights and legitimate law enforcement needs. An approach needs to be found that balances these issues, or at least recognises in the law that an offence is not automatically criminalised in the event of failure to provide assistance.

In its present implementation, the law enforcement provisions in the *Cybercrime Act* and *Spam Acts* totally fail to address these potential problems, or even acknowledge that the measures are controversial.

The law enforcement provisions may also have the effect of over−riding the common law privilege against self−incrimination. This situation could arise where a person was compelled to reveal a password or encryption key as a requirement of an assistance order. The right to silence is a

long−standing right in most jurisdictions and it is unacceptable that it should be potentially over−ridden in the Bill without strong justification. There does not appear to be any strong justification for such provisions in relation to non−criminal offences such as those in the Spam Acts.

Go to Contents List

7. Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

EFA is strongly opposed to enactment of the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*[13]. The Bill would remove the need for a telecommunications interception warrant under the *Telecommunications (Interception) Act 1979*[14] to access the content of communications temporarily delayed and stored on a telecommunication service provider's equipment during passage (i.e. that have not completed their passage to the intended recipient).

Access to undelivered email, SMS and voice mail messages would become available to a wide range of Commonwealth, State and Territory government agencies (not only police), private investigation agencies, telephone companies and ISPs and other people, not only with a search warrant, but also without a search warrant.

The Bill would result in even less protection for temporarily delayed and stored communications than provisions in a similar 2002 Bill. The provisions concerning stored communications were deleted from the 2002 Bill by the government when it became clear they did not have sufficient support in the Senate.

Comprehensive information about the 2004 Bill is contained in EFA's submission dated 28 June 2004[15] to the Inquiry into the provisions of the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* conducted by Senate Legal & Constitutional Legislation Committee.

Go to Contents List

8. Surveillance Devices Bills 2004

EFA has major concerns about aspects of the *Surveillance Devices Bills 2004* including provisions that would give law enforcement agencies new powers to, in effect, covertly search individuals' and businesses' computers and electronic communications and covertly seize information about about them and also about law−abiding third parties, for example by way of data surveillance devices including keystroke logging device. Further information is available in EFA's submission[16] to the Inquiry into the Provisions of the *Surveillance Devices Bill (No. 1) 2004* conducted by Senate Legal & Constitutional Legislation Committee.

While some amendments have been made to the original Bill and a revised Bill, *Surveillance Devices Bill (No. 2) 2004*[17] has been passed by the House, that Bill does not incorporate all amendments recommended by the Committee, nor resolve a matter of major concern to EFA. In this regard, for example, the Committee Report[16] stated:

> "3.49 The Committee takes the view that ambiguity in the application of this kind of legislation has the potential − however unintentional − to give rise to use of powers which would be proscribed under one statute but permitted under another, as in the example given by EFA. Accordingly, the Committee makes the following recommendation:
> Recommendation 3
> 3.50 The Committee recommends that the bill and the TI Act be amended to ensure that the circumstances in which similar kinds of surveillance devices are authorised, are clearly described, and that the limitations on their respective use are also clear."

Recommendation 3 has not been dealt with in the revised Bill (No. 2).

It was stated in the House by Senator McClelland (ALP) on 24 June 2004[17] that:

> "The opposition supports these amendments, which in some instances give effect to the bipartisan recommendations of that Senate committee and, in others, respond to requests by the state and territory governments for amendments to the bill, as outlined by the Attorney−General. Where the amendments do not pick up specifically the recommendations of the Senate committee, the opposition is satisfied from discussions with officials of the Attorney−General's Department that the concerns of the committee are being met in other ways that are appropriate."

EFA is of the opinion that if officials of the Attorney−General's Department claim concerns are being met in other ways, the detail of such other ways should be made available to the Parliament and the public before, or at the same time as, proposed legislation is introduced into Parliament. (The disagreement between the A−G's Department and the Australian Federal Police, referred to earlier herein, is notable in relation to reliance on advice from a single government agency).

The concern raised by EFA and in the Committee's Recommendation No. 3 above cannot be addressed in any way other than by amendment to legislation.

Furthermore, we point out that the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* will not resolve the issues referred to above. That Bill deals only with the issue of *stored communications* which is not the same issue as raised in EFA's submission on the SD Bill.

The issue raised in EFA's submission on the SD Bill is, for example, whether when an individual is engaged in a live chat session (e.g. using Internet Relay Chat) whether law enforcement agencies are required to obtain a TI warrant or a data surveillance device warrant in order to lawfully intercept such highly transitory communications during transit.

▲ Go to Contents List

9. Computers, Search Warrants & Anton Piller Orders

We understand that the Committee is already well aware of serious issues arising in connection with search warrants authorising search of computers when a "vacuum cleaner" approach is used. In particular, the protection of the rights of not only a suspect, but also third parties, in relation to matters of privilege, confidentiality and privacy[18].

We wish to draw to the Committee's attention that the same issues are arising in relation to seizure of information from computers during search and seizure raids by civil litigants who have obtained an Anton Piller order made by the Federal Court and other courts.

An Anton Piller order directs a person to permit representatives of a civil litigant to enter the person's premises to search for and seize information and/or property comprising evidence that is alleged by the civil litigants to be at high risk of destruction or tampering.

The Federal Court's power to order people to permit civil litigants to search their homes and/or other premises and seize property including information from computers exists as a result of the Parliament having conferred such power on the Court in the *Federal Court of Australia Act 1976*[19]. As stated by Branson J in *Microsoft Corp v Goodview Electronics Pty Ltd* [1999] FCA 754[20]:

> "10 The power of this Court to make an Anton Piller order is to be found in s 23 of the *Federal Court of Australia Act 1976* (Cth) ("the FCA Act") (*Television Broadcasts Ltd v Nguyen (1988) 21 FCR 34*).
> 11 Section 23 provides:
>
> > '*The Court has power, in relation to matters in which it has jurisdiction, to make orders of such kinds, including interlocutory orders, and to issue, or direct the issue of, writs of such kinds, as the Court thinks appropriate.*'"

Although Anton Piller orders have been used for many years by business interests in Australia, few members of the general public had heard of them before 2003/2004 when they hit the headlines following music industry raids at universities, Internet Service Providers and people's homes.

Anton Piller orders have been the subject of controversy within the legal fraternity and in the public arena since they were first invented by a U.K. court in the mid 1970s. They are controversial because the way in which they are issued is contrary to normal principles of justice and they order people to permit activities that are normally regarded as trespass and invasion of privacy.

Anton Piller orders are made 'ex parte'. The court hears the applicant's reasons for seeking an Anton Piller order in secret, that is, without the person whose premises and property are to be searched being present, nor his/her lawyers. Therefore, the person has no opportunity to inform the court of any reasons why the order should not be granted. The court only hears the applicant's claims and allegations about the person.

As learned judges have said on many occasions, Anton Piller orders stand "at the extremity of the court's jurisdiction"[21]. Judges have also said that an Anton Piller order is "a 'nuclear weapon' in the law's armoury" and that as such it "is a weapon of last resort"[22].

Further, "[t]he making of an Anton Piller Order has been described as 'Draconian'. The impact that this type of order can have and the interference upon a party's rights to enjoy the privacy of their residence, and the freedom to trade are convincingly argued by Scott J in *Columbia Pictures Industries Inc & Ors v. Robinson & Ors*"[23].

Some members of the Law Council of Australia's Intellectual Property Committee have said that they are "of the view that Anton Piller orders are a draconian remedy which should be used sparingly"[24].

The Australian Law Reform Commission ("ALRC") discussed the matter of Anton Piller orders in an ALRC Report[25] issued in 1995. Among other things the ALRC said "Is there cause for concern?" and then remarked that "[t]here is widespread international concern about the execution of Anton Piller orders". The ALRC also referred to the Federal Court's 1994 Practice Notes concerning Anton Piller orders and commented that there can be

> "other problems in the execution of Anton Piller orders which it may be appropriate to consider in subsequent Practice Notes. For example, particular issues arise in relation to access to documents obtained using a computer and the scope of the power to examine, copy and secure goods including documents which may be stored on a computer. Related issues concern the compensation for loss or damage caused by the use of computers during searches in the execution of Anton Piller orders".

Nevertheless, the Federal Court has not revised its Practice Notes to address such issues. According to the Court's web site as at 20 July 2004, the Practice Notes concerning Anton Piller orders[26] have not been changed since first issued in 1994.

While there was cause for concern in 1995, since then the law relating to Anton Piller orders in Australia has been extended by Courts in ways which have "greatly increased the scope and effect" of Anton Piller orders[27].

In EFA's opinion, the extension of the law since 1996 suggests that there is now cause for alarm. EFA is extremely concerned that the novel applications for Anton Piller orders that the Court has been faced with in 2003/2004 and the practices of the courts to date appear to have high potential to result in inappropriate and unnecessary invasion of the privacy of third and fourth parties, that is, of law−abiding members of the public. If this has not already occurred, it seems almost certain that it is only a matter of time before it will, unless court rules and practices are changed, or the Parliament amends or enacts relevant legislation.

A number of raids conducted under Anton Piller orders in 2003 and 2004 at homes, universities and Internet Service Providers have resulted in increased public concern, in part because orders made by the Federal Court have included authorising copying of information from computers, including entire hard−drives. Some orders have appeared, whether inadvertently or intentionally, to allow inappropriate invasion of the privacy of respondents and third parties without adequate safeguards and controls. This gives rise to the question of whether the *Federal Court Act 1976* should be amended to regulate the Courts powers in this regard, and/or specifically require the Court to develop additional Rules and/or Practice Notes concerning search and seizure, particularly of computers and information contained in computers.

EFA has been reliably informed that during execution of an Anton Piller order at an Internet Service Provider's premises in Sydney in October 2003[28], material copied and seized included server log files of emails sent and received by the ISP's customers during a period of eight days. The log files seized are over 14 Mb in total size (when uncompressed) and contain sender and recipient email

addresses of many individuals (both customers of the ISP and non−customers) who are not respondents or defendants in the proceedings, as well as the dates of the emails (but not the content of the email messages).

Seizing email server log files is an indiscriminate means of attempting to obtain evidence about one or a small number of people. It unnecessarily invades the privacy of many third parties who have not even been in email contact with the respondent/s. EFA is of the view that Anton Piller orders should not authorise access to entire email server log files because this enables persons obtaining such files to find out who third parties (who have nothing to do with the proceedings) have communicated with and when.

In addition, Anton Piller orders have, on their face, permitted a "vacuum cleaner" approach to computer searches and seizures conducted by civil litigants at the premises of third parties. For example, an Anton Piller order made by the Federal Court in February 2004 permitted the applicants to enter the homes and premises of third parties including universities and Internet Service Providers and seize electronic materials including "information recording communications" by way of making "bitstream images" [29].

The making of a "bitstream image" is a computer forensic process used to make a copy of the entire hard drive of a computer. It is what has been referred to as the "vacuum cleaner" approach to search and seizure.

According to statements made by attorneys in an application for protective order lodged in the United States District Court, during the raid on a person's home in Australia:

> "Computers were a principal target and hard drives were actually downloaded on the spot. In the process, plaintiffs seized and destroyed the hard drive of the computer at [one of the homes]. As as a result, [the person] lost all of the vitally important information maintained on his computer"[30].

Obviously such reports give rise to serious questions about the competence of civil litigants' representatives to avoid destroying computer hard drives and hence whether the law should allow Anton Piller orders to be used for attempting to copy entire hard drives. While the courts are able to order applicants to pay compensation for damage occurring during Anton Piller searches, in our opinion there is no adequate compensation for the loss of all information on a hard drive. In our view, the making of bitstream images and use of related techniques should only be permitted by police acting under search warrant pertaining to breach of the criminal law, not in civil litigation.

We also note the Australian Federal Police informed the Senate Legal & Constitutional Legislation Committee on 1 July 2004[31] that:

> "Mr Van Dam [Chief Operating Officer, Australian Federal Police]−As I indicated, it is not our normal practice to interrogate the computers on the premises. In fact, it is generally not good forensic practice to do that."

Serious questions also arise concerning the breadth and particularity of Anton Piller orders. For example, following the execution of the above Anton Piller order at Telstra premises in February 2004, it was reported by PC World Magazine (*Telstra perplexed by MIPI court order*, 9 Feb 2004)[32] that:

> "Telstra is unsure why it has been issued a court order pertaining to music piracy by the Australian record industry.

> On Friday, MIPI (Music Industry Piracy Investigations) was granted a court order to search the offices of ... several ISPs including Telstra ...
> ...
> The order left Telstra's legal team perplexed. 'It is exactly unclear to Telstra what the order is seeking,' said a Telstra spokesperson.
>
> Although the investigators were given the right to search Telstra premises, the spokesperson said they did not take anything. She attributed this to the paucity of information contained in the order.
>
> 'We have not been accused of any wrongdoing,' she added."

Apparently, however, electronic information was seized from another third party, iHug ISP. According to information in a Federal Court judgment dated 1 July 2004[33], information passing through a router at iHug's premises was recorded and seized. Given the purpose of a router in an ISP's premises, which is much like a switching device in a telephone exchange, it seems very likely in EFA's opinion that attaching a device[34] to an ISP's equipment to enable capturing and "recording transitory information"[35] while it is passing through an ISP's router would involve illegal interceptions under the *Telecommunications (Interception) Act 1979* unless the recording was carried out under authority of a telecommunications interception warrant. In the above judgment, the Court pointed out that it had not been presented with sufficient information to determine whether or not illegal interception had occurred.

The above matters give rise to serious concerns that some or all civil litigants and their hired investigators may not have adequate awareness or understanding of the provisions of the *Telecommunications (Interception) Act 1979*. It is also of concern that many ISPs would not be familiar with Anton Piller orders and may assume the Court is ordering them to permit a civil litigant's representative/s to intercept communications in a manner that is a criminal offence under the *Telecommunications (Interception) Act 1979* in the absence of a telecommunications interception warrant.

To EFA's knowledge it has not been made publicly known whether or not information seized during the raids on three universities, four ISPs and various other premises included privileged, confidential or irrelevant information about ISPs' customers or university staff or students or other members of the public. Whether or not such information was seized in those instances, we consider it of significant concern that orders are apparently being made in such a way that an ISP such as Telstra is unable to determine what they have been ordered to allow to be seized. While large ISPs with significant legal resources may be willing to refuse to allow seizure in the absence of clarity, there is a risk that smaller ISPs may provide whatever the applicant's representatives verbally claim the order means, rather than risk being found in contempt of court.

We believe that there are serious issues that need to be addressed and resolved in relation to the protection of privacy of not only the respondents and third parties who are the subject of an Anton Piller order, but also fourth parties (e.g. customers, staff, students, etc of the third parties to a proceeding). A court's ability to use its discretion to protect the privacy of such parties currently appears to be dependent on respondents and third parties expending their resources on applications to the Court seeking to protect the interests and rights of their customers, staff, students, and other members of the public. It is highly questionable whether all such entities can be relied on to do so.

According to the Anton Piller orders referred to above, the respondents and also the third parties were ordered to permit all electronic materials seized to be placed in the possession of the Applicant's solicitors (15 solicitors were listed in the order) **except** bitstream images. Order 14

stated that "Any images of the kind referred to in paragraph 13(b) above [i.e. bitstream images] must be kept in the secure custody of one or more of the [18] Forensic Experts [appointed by the applicants] and not subjected to further analysis without a further order of the Court."[29].

It appears however that after the raids had commenced, one or more of the persons whose premises were being raided, applied to the Court to have the order amended so that seized material would be kept in the custody of independent solicitors. In this regard, a Court judgment of 4 March 2004[36] states:

> "Action taking advantage of the orders was undertaken on 6 February 2004. During the course of that day, I was asked to amend the orders in certain respects. I did so, by consent. The amendments did not affect orders 4, 5, 6 or 13 or Schedule 2. They did vary the detail of order 14".

The above judgment does not state the changes made to order 14. However, subsequently it was reported in *The Australian IT*[37] that:

> "Justice Wilcox ordered the documents be sorted after claims some irrelevant material was taken during the raids, with an independent solicitor and a forensics expert to oversee that process.
> The sorting process would ensure only documents covered by his orders was included in the seized material, he said.
> 'I have the strong impression it wasn't done with the care and consideration you have described,'" he said of the search process. 'I think it's a bit of a mess.'"

and by the *Sydney Morning Herald*[38] that:

> "The music industry will be unable to examine material seized during February raids at the premises of Sharman Networks, owner of the Kazaa peer−to−peer software, for several more weeks.
> Federal Court Judge Murray Wilcox said the applicants were 'flogging a dead horse' in their attempts to get immediate access to material which is being held by an independent law firm. ...
> The judge's directions give Sharman and other parties raided an opportunity to review the material seized. Sharman can identify irrelevant and privileged material, which falls outside the Anton Piller order in consultation with independent solicitors, a forensic expert and solicitors from both sides."

and by TechNewsWorld[39] that:

> "During the proceeding, Justice Murray Wilcox denied lawyers for the recording industry direct access to any of the materials seized in the so−called Anton Piller raids earlier this year.
> 'The discovery process that would have resulted from the Anton Piller raid has been replaced with a regular process of discovery' ...
> Under that process, lawyers for the recording industry must provide written requests to Sharman and the other defendants in the case for particular items or categories of items. Those requests can be challenged by Sharman if it thinks they go beyond the scope of discovery parameters for the case."

While the above media reports indicate that Court has subsequently dealt with the issue in the best way available to it in the above proceedings, we believe it should be a standard requirement that

Anton Piller orders clearly state that all information seized by a "vacuum cleaner" approach to computer searches and in any other indiscriminate manner must be provided only to an independent solicitor. It should remain in safe−custody of the independent solicitor until after the Court has heard any objections from the respondents or third parties and made orders concerning disclosure, or the persons from whom the information was seized voluntarily consent to its disclosure to the applicants.

EFA also believes there is a need for amendment to Court practices or the law to clarify that respondents and third parties have an indisputable right to be present during the search of their premises and property, and that they are informed in writing of this right prior to any entry or search. In this regard, we note with great concern that *Australian Computer Magazine* reported on 9 May 2004[40] that when one of the individual's whose home was searched arrived at her home:

> "forensic analysts were already at her house, analysing hard drives of servers found inside. She was told to make herself comfortable in the front yard."

It is disturbing that it appears individuals may have less "rights" and be afforded less courtesy when their homes are invaded by a civil litigant's representatives than when a search is undertaken by the Australian Federal Police {"AFP"). In this regard, we note that AFP representatives informed the Senate Legal & Constitutional Legislation Committee on 1 July 2004[31] that the AFP undertakes best efforts to enable a person whose home is to be searched to be present during that search:

> "Mr Van Dam [Chief Operating Officer, Australian Federal Police]−For a search warrant at premises, our normal practice is to afford the person to whom that warrant is being served the opportunity to be present. ...
>
> Senator LUDWIG−You used the word 'ordinarily'; you are not required to by law, though.
>
> Mr Van Dam−Our own guidelines and provisions have it as an expectation that that will be the norm.
>
> Federal Agent Weldon−The legislation provides that if the occupier is present a copy of the rights of the occupier must be provided to them. Our practice is that if the occupier is not present we get an independent person and take all measures to try to locate the occupier. Where we cannot locate the occupier we either execute it at another time or we get an independent person like a JP to accompany us."

Given that civil litigants must first obtain the consent of the occupier before entering, EFA submits that a reasonable safeguard would require civil litigants to undertake best efforts to facilitate the occupier being present during a search (for example, at least waiting a reasonable amount of time for the occupier to arrive). In the event that the occupier is not able to be present, the civil litigant should be required to report to the Court on the efforts made to enable the occupier's presence and be subject to penalty if the Court determines that the efforts made were inadequate.

Plainly if an occupier is not able to be present, they are not able to inform the Court of any activity undertaken that they believe went beyond the Court order. The level of invasion of an individual's privacy is made apparent in a report in *Australian Personal Computer Magazine*[40]. The report states that another individual, who was a third party at the time of the raid on his home, said:

> "There were five people that I would never under any circumstances let into my home, and it was a complete search of the entire house. They went through my

> kitchen drawers and my bedroom cupboards. . . they weren't just taking digital copies of disks; it was a complete invasion of privacy. I was extremely angry about it."

Questions also arise as to whether persons attending the raids are or should be allowed to take photographs, which could invade individuals' privacy, and provide same to the media. For example, *ZDNet Australia* reported on 14 May 2004[41] that:

> "Senior counsel for Sharman Networks Robert Ellicott QC drew the court's attention to a media article that appeared in the latest issue of a technology trade publication. It featured pictures of raids that took place at premises occupied by Sharman Networks, and its associates, early in February."

It also appears that there is a need to put in place better controls and safeguards to protect the physical safety and well−being of people involved in searches conducted under Anton Piller orders. In this regard, *ABC News* reported on 10 February 2004[42] that:

> "The Federal Court in Sydney has heard claims of heavy−handed tactics and assault as part of a music industry investigation...
> The court heard that complaints about alleged strong−arm tactics during a raid on one of Sharman's affiliates on Friday have been referred to New South Wales police. Two lawyers have made the complaint, alleging that property was destroyed and two workers were assaulted."

and *Computerworld* reported on 25 February 2004[43]:

> "Just what happens when an Anton Pillar comes knocking on your door also raised a few eyebrows. Justice Wilcox said he had been 'horrified' by aspects of the way one of the orders relating to the premises of Brilliant Digital Entertainment (BDE) had been served, noting 'the situation seems to have not been well handled'.
> ...
> It is understood an argument involving physical contact ensued and has become the subject of a complaint to Randwick police. The two female independent solicitors sent to serve the orders are currently on indefinite sick leave after the incident. ..."

EFA considers there may be a need to require that civil ligitants (at their cost) be accompanied by either plain−clothes police or a suitably qualified security guard, that is, by at least one person trained in the prevention and management of physical violence.

EFA notes that it is not presently possible for the general public to know whether or not allegations reported in the media are true or not. As far as we have been able to ascertain from publicly available information, the Court has not yet dealt with allegations made in the Court concerning events during the searches in February. In this regard, a Court ruling of 4 March 2004[44] states:

> "40 ... Evidence about what happened at the time of implementation of the orders on 6 February 2004 is irrelevant. This includes evidence ... alleging excessive or inappropriate seizure of documents. These are important matters, but they are for another day.
>
> 41 Some affidavits contain complaints about the adverse effects, for the respondents and the Brilliant Digital parties, of the Attending Representatives' intrusion into their premises and the removal of material from them. I understand these complaints. Without commenting on their justification (if any), I note the complaints are a further

> reminder, if one were needed, about the need for caution in making Anton Piller orders. However, the complaints are irrelevant to the issue I now have to determine.
> ...
> 82 It would be desirable for the parties to consult together about the material taken on 6 February 2004. In the rush of that day, it seems likely that some material was taken that fell outside the authority of the Anton Piller orders. ... this situation ought to be rectified..."

EFA considers that the matters raised above demonstrate that there are serious issues of public concern in relation to the issue and execution of Anton Piller orders and that it is in the public interest that these issues be addressed and resolved in the very near future.

We respectfully suggest that the Committee consider inviting an appropriate representative of the Federal Court to advise the Committee whether or not the Court intends to revise, in the near future, its procedures and practices in relation to "vacuum cleaner" approaches to computer searches and the other issues raised above. We also urge the Committee to give consideration to whether the Court currently has adequate powers available to it to resolve all of the issues raised above, or whether there is a need for legislative changes to provide improved safeguards and protections for respondents and/or third and fourth parties in relation to seizure of privileged or irrelevant information, especially from computers, and the physical safety of persons present during searches conducted under Anton Piller orders.

▲ Go to Contents List

10. Conclusion

EFA recognises and supports the need to counter criminal use of the Internet. We also accept that in countering such use it may sometimes be necessary to examine private information held by or relating to law−abiding Internet users in order to isolate and identify criminal conduct by others and thereby secure the prosecution and conviction of guilty parties.

It is essential, however, that legislative provisions protect the privacy of law−abiding citizens to the maximum extent possible in the circumstances. We are highly concerned that insufficient attention is given in drafting and enacting legislation to ensuring an appropriate balance between individuals' right not to be "subjected to arbitrary interference with [their] privacy, family, home or correspondence"[45] and the legitimate needs of law enforcement agencies.

A number of provisions relating to entry, search and seizure in existing, and proposed, Commonwealth legislation are seriously deficient in that they fail to provide adequate privacy protection for the innocent without any evidence that the measure would have the intended impact on criminal activity.

There is an urgent need for provisions governing the seizure, disclosure and use of information seized from computers, both under search warrant and under a court order, to protect privileged information and information that is irrelevant to alleged infringements of the law.

The extension of the law relating to Anton Piller orders in recent years gives rise to cause for alarm in relation to the protection of the privacy, and physical safety, of law−abiding citizens. There is an urgent need for either changes to court rules and practices, or amendment or enactment of relevant legislation.

In addition, provisions of the law permitting the collection and examination of private information held by or relating to persons who are not the subject of an investigation, in order to isolate and identify illegal conduct by others, must specifically require that such information not be used for any other purpose and be discarded within a specified time frame in accordance with recognised privacy principles.

▲ Go to Contents List

11. References

1. Spam (Consequential Amendments) Act 2003
   [http://www.austlii.edu.au/au/legis/cth/num_act/saa2003n1302003333]
2. Spam Act 2003
   [http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366]
3. EFA submission to Inquiry into the Spam Bills 2003, conducted by the Senate Environment, Communications, Information Technology and the Arts Legislation Committee
   [http://www.efa.org.au/Publish/efasubm−ecitaspam.html]
4. Telecommunications Act 1997
   [http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/]
5. Telecommunications Interception Policy Review Report − Section 4.3, Attorney−General's Department, 1999
   [http://www.law.gov.au/agd/Department/Publications/publications/teleintreview/teleintreview2.html#dat
6. ACA Fact Sheet: Internet Service Providers and Law Enforcement and National Security
   [http://www.aca.gov.au/consumer_info/fact_sheets/industry_fact_sheets/fsi13.pdf]
7. ACA Annual Report 2003
   [http://www.aca.gov.au/aca_home/publications/reports/annual/0203/ar_corrigendum.htm]
8. Office of the Federal Privacy Commissioner, Senate Legal and Constitutional Legislation Committee, Budget Estimates, Hansard, 10 February 2003.
   [http://www.aph.gov.au/hansard/senate/commttee/s6143.pdf]
9. Cybercrime Act 2001
   [http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112]
10. Crimes Act 1914 Section 3L
    [http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3l.html]
11. Senate Legal and Constitutional Legislation Committee Inquiry into the *Telecommunications (Interception) Amendment Bill 2004*:
    - Australian Federal Police Submissions (No. 7 & 7a)
      [http://www.aph.gov.au/senate/committee/legcon_ctte/tel_intercept04/submissions/sublist.htm]
    - Attorney General's Department Submission (No. 6b)
      [http://www.aph.gov.au/senate/committee/legcon_ctte/tel_intercept04/submissions/sublist.htm]
    - Hansard Transcript of Committee hearing (Witnesses: AFP, A−G's Dept, EFA), 22 March 2004
      [http://www.aph.gov.au/hansard/senate/commttee/S7460.pdf]
    - Committee Report and Recommendations, 30 March 2004
      [http://www.aph.gov.au/senate/committee/legcon_ctte/tel_intercept04/report/report.pdf]
12. *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004*
    [http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=1681&TABLE=BILLS]
13. *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*
    [http://parlinfoweb.aph.gov.au/piweb/Repository/Legis/Bills/Linked/27050402.pdf]
14. Telecommunications (Interception) Act 1979
    [http://www.austlii.edu.au/au/legis/cth/consol_act/ta1979350/]

15. EFA submission to Inquiry into the provisions of the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*, 28 June 2004
[http://www.aph.gov.au/senate/committee/legcon_ctte/TI_stored_data/submissions/sub02.pdf]
16. *Surveillance Devices Bill (No. 1) 2004*, March 2004
[http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=1568&TABLE=BILLS]
EFA submission to Inquiry into the provisions of the *Surveillance Devices Bill 2004*, 18 May 2004
[http://www.efa.org.au/Publish/efasubm−slclc−sdbill2004.html]
Senate Legal and Constitutional Legislation Committee, Report on the *Surveillance Devices Bill 2004*, 27 May 2004
[http://www.aph.gov.au/senate/committee/legcon_ctte/surveillance/report.pdf]
17. *Surveillance Devices Bill (No. 2) 2004*, June 2004
[http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?TABLE=bills
House Hansard, Speech by Senator R McClelland, 24 June 2004
[http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=924833
18. Senate Privileges Committee, *Execution of Search Warrants in Senators' Offices − Senator Harris − 114th Report*, tabled 20 August 2003
[http://www.aph.gov.au/senate/committee/priv_ctte/report_114/report.pdf]
Clerk of the Senate, Submission to Inquiry into Entry, Search and Seizure Provisions in Commonwealth Legislation
[http://www.aph.gov.au/senate/committee/scrutiny/inquiries/submissions/entry_search/sub02.pdf]
19. *Federal Court of Australia Act 1976*
[http://www.austlii.edu.au/au/legis/cth/consol_act/fcoaa1976249/]
Federal Court Rules
[http://scaletext.law.gov.au/html/pastereg/0/49/top.htm]
20. *Microsoft Corp v Goodview Electronics Pty Ltd* [1999] FCA 754 (4 June 1999)
[http://www.austlii.edu.au/cgi−bin/disp.pl/au/cases/cth/federal_ct/1999/754.html]
21. *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55; *Bhimji v. Chatwani* [1991] 1 WLR 989 quoted in *William Henry Overholt v. Monina Acab Overholt* HCA002624A/1997 − [1999] HKCFI 208; and numerous others.
[http://www.worldlii.org//hk/cases/HKCFI/1999/208.html]
22. For example, *William Henry Overholt v. Monina Acab Overholt* HCA002624A/1997 − [1999] HKCFI 208; see also *Bank Mellat v. Nikpour* [1985] FSR 87
[http://www.worldlii.org//hk/cases/HKCFI/1999/208.html]
23. *Columbia Pictures Industries Inc & Ors v. Robinson & Ors* (1987) Ch 38; (1986) 3 All ER 338 quoted in *Coney Fair Amusement Pty Ltd v. Heath* [2000] QDC 238
[http://www.courts.qld.gov.au/qjudgment/QDC%202000/dc00−238.pdf]
24. Law Council of Australia's Intellectual Property Committee 2002, Submission to the ACIP Review of the Enforcement of Trade Marks, 18 June 2002
[http://www.acip.gov.au/submissions/council.pdf]
25. Australian Law Reform Commission 1995, Report No. 74: Designs, Chapter 14
[http://www.austlii.edu.au/au/other/alrc/publications/reports/74/ALRC74Ch14.html#ALRC74Ch14Anto
26. Federal Court of Australia, Practice Note No. 10 − Anton Piller orders, issued by the Chief Justice, 08 Apr 1994
[http://www.fedcourt.gov.au/how/practice_notes_cj10.htm]
27. *Anton Piller Orders: From T−Shirts to MP3s*, Seet, S and Kennedy, F (Gilbert and Tobin Lawyers), 6 November 2003
[http://www.gtlaw.com.au/t/publications/default.jsp?pubid=498]
28. *Universal Music Australia Pty Ltd & Ors v Cooper & Ors N1551/03*
29. Extracts of Anton Piller orders quoted in *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2004] FCA 183* (4 March 2004)
[http://www.austlii.edu.au/au/cases/cth/federal_ct/2004/183.html]

and
Full copy of above Anton Piller orders [PDF 14Mb] contained in Sharman Networks' Application for Protective Order in U.S. litigation, 6 Feb 2004
[http://www.eff.org/IP/P2P/MGM_v_Grokster/20040206_Search_Seizure_Order.pdf] [PDF 14Mb]
[http://www.eff.org/IP/P2P/MGM_v_Grokster/#documents−relating−to−sharman−networks−kazaa−4]
30. *Application for Protective Order* [2.7Mb], made in the United States District Court Central District of California, by Attorneys for Sharman Networks Limited, 6 February 2004
[http://www.eff.org/IP/P2P/MGM_v_Grokster/20040206_Protective_Order.pdf] [2.7Mb]
31. Senate Legal & Constitutional Legislation Committee, Inquiry into the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004, Committee Hansard, 1 July 2004
[http://www.aph.gov.au/hansard/senate/commttee/S7763.pdf]
32. *Telstra perplexed by MIPI court order*, Howard Dahdah, PC World Magazine, 9 February 2004
[http://www.pcworld.idg.com.au/index.php?id=1088524116
33. *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* [2004] FCA 934 (1 July 2004)
[http://www.austlii.edu.au/au/cases/cth/federal_ct/2004/934.html]
34. *R v Evans &Doyle* [1999] VSC 486 (13 October 1999)
[http://www.austlii.edu.au/au/cases/vic/VSC/1999/486.html]
Byrne &Byrne [2002] FamCA 887 (27 September 2002)
[http://www.austlii.edu.au/au/cases/vic/VSC/1999/486.html]
Miller v. Miller (1978) 141 CLR 269
[http://www.austlii.edu.au/au/cases/cth/high_ct/141clr269.html]
Telecommunications Interception Policy Review Report − Section 5 Participant Monitoring, Attorney−General's Department, 1999
[http://www.law.gov.au/agd/Department/Publications/publications/teleintreview/teleintreview2.html#par
35. *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2004] FCA 183* (4 March 2004), para. 74, 75.
[http://www.austlii.edu.au/au/cases/cth/federal_ct/2004/183.html]
36. *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2004] FCA 183* (4 March 2004), para. 17
[http://www.austlii.edu.au/au/cases/cth/federal_ct/2004/183.html]
37. *Search 'mess' delays Kazaa case*, by Simon Hayes, The Australian IT, 23 March 2004
[http://australianit.news.com.au/articles/0,7204,9053495%5e16123%5e%5enbv%5e,00.html]
38. *Kazaa case: access to seized materials delayed*, by Sam Varghese, Sydney Morning Herald, 24 March 2004
[http://smh.com.au/articles/2004/03/24/1079939686550.html]
39. *Kazaa Wins Procedural Victory in Aussie Court*, by John P. Mello Jr., TechNewsWorld, 18 May 2004
[http://www.technewsworld.com/story/33853.html]
40. *Inside the Kazaa raid*, by Garth Montgomery and Dan Warne, Australian Personal Computer Magazine, 11 May 2004
[http://www.apcmag.com/apc/v3.nsf/0/412A621F4556A65FCA256E77001DD222]
41. *Court seeks to protect Kazaa case from media*, by Andrew Colley, ZDNet Australia, 14 May 2004
[http://www.zdnet.co.nz/news/business/0,39023166,39147577,00.htm]
42. *Kazaa's owner attacks piracy case*, ABC News, 10 February 2004, 8:57pm (AEDT)
[http://www.abc.net.au/news/newsitems/s1041680.htm]
43. *Music industry data seizures in the balance*, Julian Bajkowski, Computerworld, 25 Feb 2004
[http://www.computerworld.com.au/index.php/id;476244052;relcomp;1]

44. *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd [2004] FCA 183* (4 March 2004), para 40, 41.
[http://www.austlii.edu.au/au/cases/cth/federal_ct/2004/183.html]
45. Article 17 of Schedule 2 of the *Human Rights and Equal Opportunity Commission Act 1986* (*International Covenant on Civil and Political Rights*)
[http://www.austlii.edu.au/au/legis/cth/consol_act/hraeoca1986512/sch2.html]
and Article 12 of the Universal Declaration of Human Rights
[http://www.un.org/Overview/rights.html]

Go to Contents List