Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:4

Ms Irene Graham
Executive Director
Electronic Frontiers Australia Inc.
PO Box 382
NORTH ADELAIDE SA 5006
☎07 3424 0201 🖹07 3424 0241
E-mail:

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

30 April 2003

The Secretary
Parliamentary Joint Committee
on the Australian Crime Commission
Suite S1 107
Parliament House
CANBERRA ACT 2600

Email: acc.committee@aph.gov.au

Dear Sir/Madam

Subject: Inquiry into recent trends in practices and methods of cybercrime

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 present oral testimony and respond to any questions Committee members may have. In the event that the Committee may wish to ask EFA to attend a hearing, with a view to assisting the Committee Secretariat in scheduling hearings, we advise that the most convenient venues for EFA are, in order of preference, Brisbane, Sydney, Canberra and Melbourne. We generally prefer an early afternoon session so that if an EFA representative needs to travel from interstate, this can be done on the day of the hearing, in order to minimise travel costs, rather than requiring an overnight stay due to airline flight schedules.

Yours faithfully

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)

Submission to the Parliamentary Joint Committee on the Australian Crime Commission

Inquiry into recent trends in practices and methods of cybercrime

30 April 2003

Contents:

Executive Summary

- Existing laws that prevent law−abiding Internet users from reporting criminal activity to law enforcement agencies for investigation, and/or can result in victims of criminal activity being prosecuted, should be amended.
- Any proposed change to the existing legislative framework should take into account the technological aspects and issues relevant to Internet access and use in order to target and punish only those who knowingly and intentionally engage in criminal activity.
- The Parliament's long−standing recognition of the need for telecommunications privacy and the rights of individuals to communicate across public networks without undue or unauthorised scrutiny should be maintained.
- Any proposed legislative amendments that would change the long−established balance between individuals' right to privacy and legitimate law enforcement needs should be carefully scrutinised with regard to clear justification of need and whether the benefits are clear and are achievable by the measures proposed.
- Any proposed measures to combat crime should discriminate effectively between criminals and honest, law abiding citizens. They should be balanced and should not, in an impetuous desire to counter crime, expose all Internet users to interference with the privacy of their communications.
- No increased surveillance or monitoring powers should be granted in the absence of amendments to the *Telecommunications Act* designed to improve privacy protections, incorporate adequate safeguards and controls and also implement a means of Parliamentary oversight.

▲ Go to Contents List

Introduction

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 1994, 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.

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 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 honest Internet users in order to isolate and identify criminal conduct by others and thereby secure the prosecution and conviction of guilty parties. Once examined, such private information about honest Internet users must be discarded in accordance with recognised privacy principles.

The Parliament has recognised the need for telecommunications privacy and the rights of individuals to communicate across public networks without undue or unauthorised scrutiny. We are concerned however by the increasing prevalence of legislative proposals and laws concerning the Internet that fail to contain an appropriate balance between individuals' privacy and the legitimate needs of law enforcement agencies.

Furthermore, it is of major concern that some existing laws prevent law−abiding Internet users from reporting criminal activity to law enforcement agencies for investigation and/or result in victims of criminal activity being prosecuted.

This submission addresses such matters as relevant to the Committee's intention to consider the adequacy of the existing legislative framework for combating cybercrime and related offences.

▲ Go to Contents List

Child Pornography − Existing and Proposed Laws

EFA wishes to draw the Committee's attention to the problem of unsolicited and unintentional receipt of material involving child pornography via the Internet. This presents serious and frightening problems for Internet users because, not only are they confronted with unwanted material, they also face the risk of criminal conviction for possession of material that came into their possession without their knowledge and intent. Generally recipients of this type of material suffer in silence because if they report the criminal activity to law enforcement agencies, they risk being prosecuted for possession.

There is an urgent need for review and reform of possession laws in a number of States and Territories to minimise the likelihood of Internet users being prosecuted for events that are beyond their control. While that is not a matter for the Federal Parliament, we note that the Minister for Justice and Customs announced on 4 April 2003 that "the Commonwealth Government will introduce new offences to target people who use the Internet to transmit or download child

pornography" which "will attract tough penalties of up to 10 years imprisonment". [1]

The Commonwealth Government and Parliament have the opportunity to enact an effective law that takes into account the nature of the technology and ensures the law only targets and punishes those who knowingly and intentionally engage in criminal activity. Moreover, if Commonwealth laws 'cover the field' in relation to transmission and downloading of child pornography via the Internet, they could provide protection for law−abiding Internet users from existing ill−considered State and Territory laws.

We submit that proposed Commonwealth laws should be carefully and thoughtfully formulated to ensure they achieve the aims of criminalising such acts as 'intentional acquisition', 'knowing possession and retention' and 'possession for illegal purposes', but do **not** in the process criminalise 'accidental or unintentional acquisition', 'possession without either action or intention' and 'unknowing possession and retention'.

Internet uses may very easily come into possession of illegal material via the Internet without any intention of doing so and also may not even know that such material is in their possession. Examples include:

- spam (unsolicited bulk email) and associated file attachments. Email is a sender−push mechanism and recipients have no means of preventing unsolicited messages being received, nor preventing the messages from being saved onto their computer disk;
    - ♦ Internet users who install spam filter software on their computer still receive the spam on their computer. Even in instances where a spam message is detected by the filter software (not all spam is) and automatically "deleted", the file may still exist on the computer. Functions such as pressing the delete button do not actually delete material from the computer disk − "deleted" files can be recovered with software tools used by law enforcement agencies. Furthermore, many Internet users do not have the technical knowledge or skills to completely delete unsolicited, or any other, material from their computer.
    - ♦ Some Internet users use spam filters provided by their Internet Service Provider ("ISP") which automatically send suspected spam to a different mail box on the ISP's server. Users of such services often only read and/or download email from the spam mail box on an occasional basis, e.g. once a week, once a month, etc. If an ISP found illegal material in such a mail box and reported it to police, the user could be charged with possession even if they had not received or read the message. They may not be able to prove they had not and/or a relevant law may regard the user as having possessed the message as a result of having custody and control of the mail box, notwithstanding that a user has no effective means of controlling what arrives in their mail boxes.
- newsgroup (Usenet) messages and associated file attachments. Depending on a user's newsreader software settings, all messages in a newsgroup may be automatically downloaded onto their computer prior to the user opening/reading any of them;
- pop−up windows that appear unbidden in a user's web browser. Depending on the browser configuration settings (which for most users remain at a default−setting of caching, because most users are unaware or barely aware that settings even exist), the material that popped up will be automatically cached, i.e. saved as a temporary file on the user's computer disk, and may remain stored in the cache for an extended period;
- a web page accessed by clicking on a link, that misrepresents the contents of the linked page, which is displayed in the web browser window but is not intentionally saved. Such material is also likely to be automatically stored in the cache;

As the Committee may be aware, the problem of spam (unsolicited bulk email) is increasing and spam includes unsolicited email containing child pornography. As reported in the April 2003 Spam Report issued by the National Office for the Information Economy ("NOIE"), spam is sent in an untargeted and indiscriminate manner, often by automated means, and rarely offers a valid and functional address to which recipients can reply to opt out of receiving further unsolicited messages. Approximately 80% of the spam received by Australian Internet users is sent by people overseas [2]. Hence, Australian laws prohibiting transmission and possession of child pornography do not reduce the risk of Internet users receiving unsolicited illegal material originating overseas.

An instance of child pornography received in spam and the associated problems for recipients was raised in the House of Representatives on 27 March 2003 [3]. Jann McFarlane MP stated:

> "Today I would like to bring to the attention of the House the issue of unsolicited child pornography by email. One of my constituents, ..., came to me late last year with a very serious problem. [She] was receiving unsolicited child pornography in her electronic mail. These emails were arriving almost daily ... Despite my constituent's efforts to unsubscribe to the self−described service, the emails continued to arrive regularly. ... [She] approached the police to complain, without success. [My constituent], a 61−year−old mother, then approached my office.
>
> Possession of child pornography is a serious crime, and rightly so. But, if a law enforcement officer assessed my constituent's computer, [she] would be charged. In Western Australia, she could be imprisoned for five years. Despite her efforts to prevent the flow of illegal material to her, [she] would still be chargeable under law. [My constituent] was worried about the situation. I wrote on her behalf to the Attorney−General's office, outlining this serious problem. This letter, dated 17 December 2002, did not receive attention from the Attorney−General's office until 22 January 2003. The letter my office received in response indicated that the matter was being forwarded to the Minister for Communications, Information Technology and the Arts. I still await a response from the minister for communications. My office has been hounding the minister's office for a reply for the past three weeks with no luck.
>
> My constituent is obviously distressed about her legal status. Five states and territories do not discriminate between possession and knowing possession of child pornography. ... Looking at her temporary Internet files, which show that these files have been opened, she would have to prove that she had not accessed this material willingly. This is a nationwide problem. Should my constituent cross the border, she would be charged immediately in South Australia, New South Wales, Tasmania and the Northern Territory. Intent does not matter there. ..."

EFA considers it of serious concern that under the laws of every State and Territory, it is irrelevant whether or not a person intended to obtain possession of material involving child pornography. Further, under the laws of five of the eight States/Territories, it is irrelevant whether or not a person even knows they possess such material. Extracts from relevant laws are provided in Appendix 1.

Moreover, the Commonwealth Government's current approach to reducing the availability of illegal material via the Internet is to encourage Internet users to invite prosecution of themselves for events beyond their control. In this regard, Internet users are encouraged to report illegal material they have received to the complaints hotline established by Australian Broadcasting Authority ("ABA") under the *Broadcasting Services Act*. However, the Act contains no indemnity from, nor defence to, a prosecution for persons who complain to the ABA that they have unintentionally come into possession of illegal material.

Although there might be questions about some particular cases, the fact that a complaint can result in a police raid of an innocent and well−intentioned individual's home is cause for grave concern.

In EFA's view, the failure to provide even a defence for persons who receive unsolicited material and report the illegal activity to law enforcement agencies undermines the policy objective of the law. People who are aware of the possession laws are most unlikely to notify illegal material to agencies for investigation because in so doing they are effectively confessing to possession.

We urge the Committee to draw the problem of unsolicited receipt of illegal material to the Government's attention and recommend that proposed laws concerning downloading or possession of child pornography be carefully formulated to ensure they:

- take into account the technological aspects and issues relevant to Internet access and use;
- recognise that Australian laws cannot remove or reduce the probability that Australian Internet users will receive unsolicited illegal material originating overseas;
- target and punish only those who knowingly and intentionally engage in criminal activity;
- achieve the policy aims of criminalising such acts as 'intentional acquisition', 'knowing possession and retention' and 'possession for illegal purposes', but do **not** in the process criminalise 'accidental or unintentional acquisition', 'possession without either action or intention' and 'unknowing possession and retention'.

▲ Go to Contents List

Proposals for Increased Surveillance of Internet Users

EFA notes that proposals for increased surveillance and monitoring of Internet users' communications and activities have been put forward in recent years, apparently without any regard for an appropriate balance between individuals' privacy and the legitimate needs of law enforcement agencies.

EFA submits that clear limits need to be imposed on powers granted to law enforcement authorities in situations where civil liberties are likely to be compromised.

Surveillance of communications is often used against dissidents, whistleblowers, political activists and human rights workers around the world. Care must be exercised to ensure that any monitoring measures introduced to assist law enforcement are proportionate to the crime involved, and respect the rights and freedoms of innocent individuals, including those who wish to exercise their right to dissent against government policy.

In particular, we submit that surveillance should only be used in the case of serious crimes, be specifically targeted against suspects, and be under judicial control. Techniques used should allow for clear prevention of self−incrimination and should not interfere with other inalienable rights, such as privacy and freedom of expression.

The methods used must separate out the communications of the specific target under investigation, gather only the legally permitted amount of data, be secure against tampering, and respect the division between content and traffic data.

Australia, along with other Western democracies, has had a strong tradition of maintaining checks and balances on police power. Telecommunications interception has been treated as a serious

matter, justified only in serious circumstances and requiring judicial oversight. However, in recent years changes to the *ASIO Act* have loosened the restrictions in this area and a number of proposals have been put forward that would further erode controls and enable a much wider group of agencies to access communications data and for an expanded range of purposes.

▲ Go to Contents List

Logging of Internet Traffic and Communications

EFA is concerned by proposals for mandatory retention of transaction log records by Internet Service Providers ("ISPs"). Such proposals were previously submitted to the Parliamentary Joint Committee on the National Crime Authority and have the potential to result in it becoming lawful for government agencies to obtain a vast wealth of communications data without a judicial warrant. Government agencies already obtain, without a warrant, an average of three quarters of a million disclosures of personal information about telecommunications users annually [4] [5].

Logging and data warehousing of Internet traffic or content on a mass scale is highly privacy−invasive. It is significantly more invasive than logging telephone call records because the information can be used, not only to determine the parties to a communication, but to develop detailed profiles of individuals' interests. It is akin to recording details of every letter or fax an individual writes or receives combined with filming individuals' activities in a manner that records every item they purchase in shops, every film they see at the cinema, every book they take out on loan from a library and so on.

Any requirement for ISP logging or monitoring would be tantamount to the sanctioning of mass surveillance and would an infringement of the fundamental human rights of Internet users. Such a measure, combined with the use of sophisticated analytical techniques such as data−mining, triangulation of data, "friendship trees", and "interest profiling", would be another large step towards a totalitarian society not dissimilar from that envisaged by George Orwell in his prophetic work *1984*.

Unlike telephone call records, most ISP logs, apart from those used to determine customer log−in durations and traffic volumes, are not intrinsic to the operation of an ISP's business. E−mail and World Wide Web proxy logs are an ephemeral by−product of server operations, useful for ISPs in the short term to diagnose technical problems, but otherwise routinely discarded. It is necessary to embark on a data−mining and data matching exercise in order to turn the raw log data into information about user behaviour. This factor increases the risk that ISPs may hand over complete logs of all user transactions to law enforcement authorities rather than undertake a costly exercise of extracting and matching information about a particular individual of interest.

The proposals also raise questions about the extent to which the needs of e−commerce, in gaining trust and confidence of Internet users, are understood. Surveys of Internet users consistently raise privacy and security concerns as the primary obstacles to uptake of online commerce. Mandatory logging and retention would increase such concerns and may also give the impression that the government's encouragement of electronic commerce and online government service delivery may be partly motivated by a desire to increase surveillance of citizens.

Privacy Act Considerations

The potential for infringement of the *Privacy Act (Cth)* (as amended 2000) must also be considered. In particular we refer to the National Privacy Principles (NPP), Section 1 − Collection, which includes the following principles [6]:

> *1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.*
> *1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.*

It is acknowledged that the Privacy Act seeks to balance the right to privacy with other public interests such as law enforcement objectives. In particular, NPP 2.1(h) allows personal information to be disclosed in defined circumstances for the secondary purpose of law enforcement.

However, EFA contends that a proposal for compulsory logging of communications traffic does not give rise to a secondary purpose within the meaning of the Act. Rather, the primary purpose of such record−keeping is the acquisition of mass surveillance data without consent, in case the data is required at some future time to incriminate a particular user. The law enforcement provisions of the Act are clearly intended only to allow law enforcement agencies to access specific records collected by an organisation for some other legitimate purpose.

Furthermore, it is questionable whether the disclosure of information from communications logs for data−matching purposes is a permitted purpose under the Act if it involves disclosure of information about large numbers of individuals who are of no interest to the relevant agency.

We contend that any requirement for collecting information concerning the communications of Internet users, without their consent and without a judicial warrant, would be contrary to the government's intent in expanding the coverage of the Privacy Act.

Justification for Mandatory Record Keeping

EFA contends that no compelling case has been made to justify mandatory record keeping by ISPs. To date, to our knowledge, proponents of this type of mass surveillance have relied on anecdotes, with no supporting data or statistics on the prospects for improvement in crime clear−up rates, the nature of any crimes likely to be detected, the additional evidence expected to be obtained, or any increased probability of successful prosecutions.

We bring to the Committee's attention that in the 2000−2001 year 773,485 disclosures of information or documents were made to law enforcement agencies under Section 282 of the Telecommunications Act by telecommunications carriers, carriage service providers (includes ISPs) or number database operators. Of the total, 71% (524,253) were disclosed without a warrant or even a certified request, as permitted by Section 282(1) and (2) [4]. In the prior year 1999−2000, the numbers were 998,548 and 865,817 (86%) [5].

However, according to the Australian Federal Police ("AFP"), "it is not feasible to attempt to measure the number of arrests or convictions that might have eventuated from the contribution of information gained [by the AFP] under [the Telecommunications Act] section 282 provisions" [7].

▲ Go to Contents List

Interception of Email, SMS and Voice Mail Messages

EFA is disturbed by recent legislative proposals seeking to remove the existing requirement that law enforcement agencies obtain an interception warrant prior to accessing the content of email, SMS and voice mail messages. Although this component of the *Telecommunications Interception Legislation Amendment Bill 2002* did not obtain passage through the Senate, the government has stated it intends to re−introduce such amendments.

To date, no information concerning any legitimate need or justification for such amendments has been made publicly available.

We urge the Committee to seek detailed information from any law enforcement agency that claims a need for legislative amendments that would change the long−established balance between individuals' right to privacy and legitimate law enforcement needs.

Clause 15 of the version of the *Telecommunications Interception Legislation Amendment Bill 2002* initially introduced into Parliament would have allowed government agencies to intercept and read the contents of communications passing over a telecommunications system, that are delayed and stored in transit, without a warrant of any type (e.g. email, voice mail and SMS messages that are stored on a service provider's equipment pending delivery to the intended recipient).

Under current law, the *Telecommunications Interception Act*, an interception warrant is required to access such messages, the same as is required to intercept a telephone call. However, after a message has been delivered to the intended recipient (i.e. has completed its passage over the telecommunications system) law enforcement agencies can lawfully access the content of the message with a search or seizure warrant. Such a warrant may cover the recipient's equipment (e.g. computer containing downloaded email) or the service provider's equipment when a copy of the delivered message remains stored on their equipment.

In EFA's analysis, the change proposed in *Telecommunications Interception Legislation Amendment Bill 2002* would have permitted agencies to access delayed/stored communications without a warrant of any type, under the existing provisions of the *Telecommunications Act* such as Section 280(1)(b) and 282(1) and (2).

For example, S282(1) and (2) of the *Telecommunications Act* permit carriers and carriage service providers (including ISPs) to disclose documents and information to agencies on request (without a warrant or even written 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 above clauses currently permit 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). However, those clauses cannot be used to access the "contents or substance" of communications delayed and stored in transit because such access is prohibited by the *Telecommunications Interception Act*. If the change to the *Telecommunications Interception Act* referred to above had been enacted, the prohibition on disclosing content of such messages (without an interception warrant) would cease.

▲ Go to Contents List

A Need for Safeguards and Parliamentary Oversight

The Parliament has recognised the need for telecommunications privacy and the rights of individuals to communicate across public networks without undue or unauthorised scrutiny. In this regard, longstanding, rigorous safeguards and controls are set out in the *Telecommunications Interception Act* to prevent misuse of the power to intercept.

Any proposal to grant increased powers to law enforcement agencies must be carefully scrutinised, not only with regard to justification of need, but also whether or not adequate safeguards and controls will be in effect.

EFA considers that access to the content of telecommunications in transit, whether or not stored during transit, should not be permitted without an interception warrant. We provide details of significant differences between interception warrants and other warrants, with regard to safeguards and controls, later herein.

Furthermore, EFA is of the view that even if a need for increased powers to access information about telecommunications users can be justified, no further powers should be granted in the absence of amendments to the *Telecommunications Act* designed to improve privacy protections, incorporate adequate safeguards and controls and also implement a means of Parliamentary oversight. This matter is discussed below.

Telecommunications Act

Part 13 of the *Telecommunications Act* allows criminal law enforcement, public revenue and civil penalty enforcement agencies (defined in subsection 282(10) of the Act) to make certified and uncertified requests to a carrier or carriage service provider (including ISPs) for the disclosure of information about telecommunications users.

In the case of a certified request, the carrier/provider is authorised to rely on written certification of a senior officer of an authorised agency 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.

In the case of an uncertified request, the carrier/provider must decide whether or not they consider the disclosure is "reasonably necessary".

As noted earlier herein, these provisions result in approximately three−quarters of a million disclosures of personal information each year, without a warrant. Over half a million of these disclosures are made, or at least authorised to be made, without even a written request.

These provisions lack adequate controls and safeguards.

Although carriers and carriage 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 this financial year his office will 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*.

Interception Warrants −v− Search Warrants

The longstanding, rigorous safeguards and controls set out in the *Telecommunications Interception Act* ("TI Act") to prevent misuse of the power to intercept do not apply to search/seizure warrants issued to various Commonwealth, State and Territory agencies. Some examples of the effects of permitting access to the content of telecommunications via warrant, instead of interception warrant, would be as follows:

- Less strict requirements would govern issue of warrants because warrants other than interception warrants could be used. The nominated members of the Administrative Appeals Tribunal who are authorised to issue interception warrants must comply with conditions of issue set out in the TI Act that are intended to ensure privacy is not unduly infringed. Applicants for interception warrants are required to demonstrate that the information likely to be obtained from the interception will materially assist the investigation, that there are no alternative methods available (or that they have been tried without significant success), and that in the case of 'Class 2' offences that the matter is sufficiently serious to justify intrusion into individuals' privacy.

  Issue of search warrants is not subject to such conditions and can be issued by less appropriately qualified persons, including some likely to be biased against giving adequate consideration to privacy issues, such as police officers, officers of government departments, justices of the peace, etc.

- Access would no longer be restricted to the investigation of serious crime. Agencies would be able to obtain access, without an interception warrant, to the content of stored communications on service providers' equipment when investigating a significantly broader range of suspected offences than is permitted under the TI Act. Interception warrants can only be issued in relation to the investigation of a "serious offence" i.e. Class 1 and Class 2 offences specified in the TI Act. In most instances it is a requirement that the offence be punishable by imprisonment for life or for a period of at least 7 years. (Class 1 offences include murder, kidnapping, narcotics offences and being a party to those offences. Class 2 offences include those which are punishable by a maximum of at least seven years imprisonment, e.g. bribery, serious fraud, drug trafficking, official bribery and corruption, money laundering and offences involving two or more offenders and substantial planning and organisation.)

  Search warrants can be issued for many other reasons and purposes than can interception warrants.

- Agencies who are not authorised to use interception warrants would be able to access the content of undelivered stored communications on service providers' equipment, i.e. access information that they presently have no power to access. Interception warrants can only be issued to agencies that are specifically authorised under the TI Act (e.g. the AFP and the ACC) and 'declared agencies' under S. 34 of the TI Act. Before the Attorney−General can declare a State agency, there must be State legislating complementing the Commonwealth *Telecommunications Interception Act*. State legislation must impose parallel supervisory and accountability provisions (including those relating to inspection and reporting requirements) on the State authority. Hence, agencies of States that are not bound by such complementary legislation are not and cannot be authorised to obtain interception warrants.

  Generally, issue of search warrants is not subject to equivalent supervisory and accountability provisions.

- Enforcement agencies other than criminal law enforcement agencies would be able to obtain access to the content of stored communications without a warrant of any description.
- Limitations set out in the TI Act on the secondary disclosure and use of information obtained from execution of an interception warrant do not apply to information obtained under a search warrant, or without a warrant of any type.

▲ Go to Contents List

A Need for Proportionality and Effectiveness

We urge that any recommendations of the Committee be consistent with international human rights instruments, namely articles 12 and 19 of the Universal Declaration of Human Rights (1948) [9] and articles 17 and 19 of the International Covenant on Civil and Political Rights (1966) [10] (refer Appendix 2).

The key principle in these articles is that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence".

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 honest Internet users in order to isolate and identify criminal conduct by others and thereby secure the prosecution and conviction of guilty parties. But in considering such action we believe that it is necessary to apply the following tests to any proposals that are made:

1. That they provide clear net benefit for society. That is, the benefits are clear and are achievable by the measures proposed, with the detrimental impact on the rights of honest citizens as small as possible and widely accepted as tolerable in the light of the gains secured.
2. That the measures proposed discriminate effectively between criminals and honest, law abiding citizens. Therefore, they should be balanced and should not, in an impetuous desire to counter crime, expose all honest Internet users to interference with the privacy of their communications.
3. That of all the options available they are optimal in the sense that they are the most effective in countering criminals while having the least impact on honest citizens and the lowest costs for taxpayers and businesses.
4. They should be based on clearly defined policy objectives which citizens understand and which command widespread public support.
5. They should be enforceable, transparent, and accountable.

In addition, any legislation permitting the collection and examination of private information held by or relating to honest Internet users in order to isolate and identify criminal conduct by others must specifically require that such information be discarded within a specified time frame in accordance with recognised privacy principles.

▲ Go to Contents List

Conclusion

Existing legislation exposes Internet users to criminal proceedings and possible conviction for events that are beyond their control. Such legislation fails to take into account the technological aspects and issues relevant to Internet access and use.

A number of proposals for combatting crime in recent years have been seriously deficient in that they would undermine important rights that exist to protect the innocent without any evidence that the measure would have the intended impact on criminal activity.

Measures proposed have been indiscriminate and not effectively targeted at criminals with the result that they would undermine the confidence of honest Internet users in the safety, security and privacy that they should have when they use the Internet.

We urge the Committee to carefully scrutinise any proposed measures for combatting crime and ensure that any recommendations of the Committee are consistent with international human rights instruments and would not, if implemented, undermine the long−established balance in Australian telecommunications interception legislation between individuals' right to privacy and legitimate law enforcement needs.

▲ Go to Contents List

References

[1] New offences to clamp down on Internet child pornography, Media Release, Chris Ellison, Minister for Justice and Customs, 4 April 2003.
http://www.law.gov.au/www/justiceministerHome.nsf/Alldocs/C79B4269BE79C65BCA256CFE00114559?OpenDocument

[2] Spam Report, National Office for the Information Economy, April 2003.
http://www.noie.gov.au/publications/NOIE/spam/final_report/index.htm

[3] Statements by Members: Child Pornography, Jann McFarlane MP, House of Representatives Hansard, 27 March 2003.

[4] Answer to Question on Notice No. 150 − Communications: Carriage Service Providers, House of Representatives Hansard, 19 March 2002.
http://www.aph.gov.au/hansard/reps/dailys/dr190302.pdf

[5] Australian Communications Authority, Answer to Question on Notice No. 57 − Managed Regulation of Telecommunications, Senate Environment Communications Information Technology &the Arts Legislation Committee, Supplementary Budget Estimates 2000−2001, 30 Nov 2000.
http://www.aph.gov.au/senate/committee/ecita_ctte/quest_answers/04aca.pdf

[6] National Privacy Principles
http://www.privacy.gov.au/publications/npps01.html

[7] Australian Federal Police, Answer to Question on Notice No. 136, Senate Legal and Constitutional Legislation Committee, Budget Estimates, 28 May 2002.

[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] Universal Declaration of Human Rights
http://www.un.org/Overview/rights.html

[10] International Covenant on Civil and Political Rights
http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

Appendix 1: Extracts from State/Territory Laws

- *N.S.W. Crimes Act* s. 578B (2): "a person who has in his or her possession any child pornography is guilty of an offence".
- *S.A. Summary Offences Act*, s.33 (3): "A person who is in possession of child pornography is guilty of an offence".
- *Tas. Classification (Publications, Films and Computer Games) Enforcement Act* s.74: "A person must not have possession of – (a) a child abuse product".
- *W.A. Censorship Act* s.60 (4): "A person who possesses or copies child pornography is guilty of a crime"
  W.A. Censorship Act s. 101 (1): "A person must not use a computer service to −− ... (b) obtain possession of an article knowing it to be objectionable material"
- *N.T. Criminal Code of the Northern Territory of Australia* s.125B (1): "A person who has in his or her possession − (a) child pornography; or ... is guilty of an offence"
  N.T. Classification (Publications, Films and Computer Games) Act s. 50Z (1): "A person shall not use a computer service to − ... (b) obtain possession of an article knowing it to be objectionable material"
- *A.C.T. Crimes Act* s.92NB (1): "A person who knowingly has in his or her possession [child pornography] is guilty of an offence".
- *Victorian Crimes Act* s.70 (1): "A person who knowingly possesses child pornography is guilty of an indictable offence."
- *Qld Classification (Publications, Films and Computer Games) Enforcement Act* s.26 (3): "A person must not knowingly have possession of a child abuse computer game." (The definition of 'computer game' includes 'a computer generated image').

Appendix 2: Extracts from relevant International Instruments

Universal Declaration of Human Rights

Article 12:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

International Covenant on Civil and Political Rights

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

Article 19

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
(a) For respect of the rights or reputations of others;
(b) For the protection of national security or of public order, or of public health or morals.

In relation to Article 17, the United Nations High Commissioner for Human Rights noted:

In the Committee's view the expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.