28 June 2004

The Secretary
Senate Legal & Constitutional Committee
Parliament House
Canberra ACT 2600

Dear Secretary

I refer to the Committee's current inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004. Attached you will find this agency's submission to the Committee.

It is understood that the Committee intends holding public hearings on this Bill in Canberra on Thursday 1 July 2004. I would be pleased to attend the hearing and provide the Committee with additional evidence if it considered helpful.

Should you require additional information in relation to the Committee's hearing, please contact our Government Relations Adviser, Andrew Larcos, on (02) 9911 2679.

Yours sincerely

Keith Inman
Director
Enforcement

Submission by the

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION
to the Senate Legal and Constitutional Legislation Committee inquiry into the provisions of the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004*

Introduction

The Australian Securities and Investments Commission ("ASIC") is an independent Commonwealth agency which regulates corporations, financial markets and financial products. ASIC is responsible for enforcing company and financial services laws to protect consumers, investors and creditors. ASIC has responsibilities and powers under a range of legislation including:

- the *Corporations Act 2001*;
- the *Australian Securities and Investments Commission Act 2001* ("the ASIC Act");
- the *Insurance Act 1973*;
- the *Life Insurance Act 1995*;
- the *Insurance Contracts Act 1984*;
- the *Retirement Savings Account Act*; and
- the *Superannuation Industry (Supervision) Act 1993*.

ASIC is not an "agency" within the meaning of the *Telecommunications (Interception) Act 1979* ("the TI Act").

ASIC supports the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* ("the Bill"). ASIC also supports the submission of the Action Group on E-Commerce ("AGEC"), which was formed under the auspices of the Heads of Commonwealth Law Enforcement Agencies ("HOCOLEA"). ASIC is a member of both HOCOLEA and AGEC.

Submissions

The Bill represents the third attempt to reform the application of the TI Act to communications such as email and voice mail. ASIC has previously made a submission to this committee's inquiry into the Security Legislation Amendment (Terrorism) Bill 2002 and Related Bills. ASIC's submission was directed to the Telecommunications Interception Legislation Amendment Bill 2002 which constituted a previous attempt at reform in this area.

As noted above, ASIC is not an "agency" for the purposes of the TI Act. Consequently, ASIC is unable to apply for or obtain a telecommunications interception warrant. It is unable to be provided with evidence obtained under a telecommunication interception warrant by another agency. ASIC cannot use or have any access whatsoever to evidence which may only be obtained under a telecommunications interception warrant.

The use of email and voice mail is now extremely common. In ASIC's experience this is particularly the case with respect to the use of email in the financial services industry where the benefits of email are clear. Providers of financial services may well use email to correspond with their clients and with the suppliers of financial products. Similarly, other subjects of ASIC regulation, such as the officers of corporations are likely to be frequent users of email. Email has to some extent replaced other forms of office communication such as the letter and the memorandum.

ASIC is responsible for the investigation of many contraventions of the law in the financial sector. The targets of ASIC investigations are frequently well educated and well resourced. Partly for this

reason, it is generally difficult to obtain evidence of the sorts of white-collar crimes that ASIC investigates. This difficulty is recognised by Parliament in the range of powers that it has provided to ASIC to assist in the conduct of its duties. ASIC recognises that the holding of such powers is always accompanied by a serious responsibility to respect the rights of individuals who may be affected by those powers.

Emails are proving to be an important source of evidence in support of ASIC investigations. For instance, in a major investigation into the collapse of a large public company, emails sent between directors provided evidence of their knowledge of, and consent with respect to, several transactions which became the subject of criminal charges.

If ASIC were unable to access some types of email (such as emails stored in a particular way) it would be easy for wrongdoers to deliberately set up their systems so that they may use email in furtherance of a contravention of the law but email evidence of their wrongdoing could never be accessed by ASIC. In some cases, this may make investigation and prosecution of serious contraventions of financial sector laws impossible. Further, the level of evidence available to ASIC in its everyday investigations would be likely to decrease in the future with the increasing reliance on electronic communication rather than paper documents.

Where evidence may be obtained without a telecommunications interception warrant, a law enforcement agency must still have lawful means in order to obtain it, such as the consent of the owner, a conventional search warrant or a notice to produce. The use of notices to produce or conventional search warrants by enforcement agencies such as ASIC is not unlimited. It is subject to strict limitations. For instance, the things which ASIC may require for production under section 33 of the ASIC Act are limited to books relating to a limited number of matters specified in the provision (such as books relating to the affairs of a body corporate). A search warrant under the *Crimes Act 1914* ("the Crimes Act") may only be issued by a magistrate; a justice of the peace or a person employed in a State or Territory Court who is authorised to issue search warrants. It may only be issued when the issuing officer is satisfied by information on oath that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises. The execution of search warrants is subject to a number of other controls set out in the Crimes Act and is closely scrutinized by the Courts. The conduct of ASIC is generally subject to supervision or scrutiny by a number of bodies including The Administrative Appeals Tribunal, the Commonwealth Ombudsman and Parliament. ASIC is also subject to the *Freedom of Information Act 1982*.

In ASIC's view, the application of the current provisions of the TI Act to forms of communication such as email and voicemail is unclear. The TI Act is a relatively old piece of legislation (passed in 1979) and so there is some difficulty in applying its language to more recent phenomena such as email. As a consequence, a great deal of confusion throughout the internet industry as to what form of communications can be seized under a conventional search warrant or compulsory notice and what forms of communications require a telecommunications interception warrant. Understandably, some internet service providers feel it best to err on the side of caution and refuse production to a wide range of communications including some forms of communication to which ASIC believes it has a right of access. This approach has impacted on ASIC investigations.

One widely followed interpretation of the current provisions is that an telecommunications interception warrant will be required to access a communication, such as an email or a voicemail, which has not been accessed by the recipient. This leads to the practical problem that it is generally impossible for an internet service provider ("ISP") to determine whether an email has been accessed or not. Accordingly, some ISPs take the view that a telecommunications interception warrant is required for any seizure of email. Where this view is adopted, ASIC cannot obtain access to any communications stored at the ISP without resorting to litigation to seek to enforce production in

accordance with a search warrant or notice. Even then, ASIC would only be able to obtain access if the Court disagreed with the interpretation adopted by the ISP and by that time the relevant documents may have been deleted.

In ASIC's view the distinction between emails and voicemail which have been accessed or not accessed is fairly arbitrary. Such a distinction does not apply to other forms of communication which may be obtained by way of a conventional warrant or notice to produce such as letters (including draft letters), memoranda and facsimiles (other than those intercepted while passing over the telecommunications network).

The Bill will clarify the application of the TI Act to forms of communications such as email and voicemail. This is important not only because it will facilitate the legitimate investigations of agencies such as ASIC but also because it will provide certainty and protection to ISPs which are seeking to comply with the law.

The Bill distinguishes between "stored communications" such as "communications stored on equipment or any thing" and what might be referred to as "real time communications" such as voice over Internet protocol or other communications "stored on a highly transitory basis as an integral function of the technology used in transmission". In ASIC's view, this distinction is consistent with the general effect of the TI Act which is to regulate the interception, over a period of time, of real time communications. A telecommunications interception warrant permits real time listening to, or recording of, communications for a period of up to 90 days. By contrast, a search warrant or other lawful authority to obtain evidence applies for the period of time at which it is executed and is not an ongoing power. Were the Bill to be passed, real time access to the content of any communications, whether a telephone call, an email or any other form of telecommunication, will still only be available under an telecommunications interception warrant.

ASIC believes that stored communications, and particularly email, are more analogous to forms of communications, such as letters and memoranda. Indeed, to a large extent these have been replaced by email. Letters and memoranda can be seized under a conventional search warrant as indeed can emails which have been printed and (at least) emails which clearly have been read by their recipient. A voice mail might be considered as analogous to an audio tape, video tape or computer diskette which may also be seized under a conventional search warrant.

In previous community debate on this issue, it has been noted that if email may be obtained by execution of a warrant on an ISP, then the sender or recipient of an email will never know that it has been seized. This is undoubtedly true. However, this is no different to the situation where a search warrant is served, for instance, on a bank for access to a person's financial records. This may already be done by law enforcement agencies and is done by ASIC with reasonable regularity. Similarly, search warrants may be executed on Australia Post for access to letters not yet received by the addressee.

It is also true, however, that the use of a conventional search warrant or notice on an ISP differs from use on a Post Office in that an ISP (unlike a post office) is likely to have records of email which has been previously delivered. This is a unique feature of stored communications which applies neither to postal communications or telephony. It does not change the fact that stored communications are generally more analogous to the type of communications which require a conventional search warrant or other compulsory process rather than a telecommunications interception warrant.

Another advantage of the current Bill is that it clearly applies to web – based email services such as "hotmail". In ASIC's experience such services are frequently used by wrongdoers as it is much harder for law enforcement agencies to establish the identities of users of these services.

ASIC encourages the Committee to support passage of the Bill.