AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION

Submission to the Senate Legal and Constitutional Legislation Committee

Inquiry into the Telecommunications (Interception) Amendment Bill 2006

Introduction

ASIC does not accept that the stored communications regime sought to be established by the Bill is necessary. As we have previously commented to the Committee[1], in our view emails and SMS messages and the like should be able to be accessed by agencies using the existing powers of those agencies. These communications are analogous to forms of communications such as letters and memoranda (for which email is a common substitute). Letters and memoranda can be seized using powers under the *Australian Securities and Investments Commission Act 2001* (Cth) (ASIC Act) or under a conventional search warrant, as can emails which have been printed. A voicemail might be considered analogous to an audio tape, video tape or computer diskette which may also be seized using ASIC notice powers or under a conventional search warrant. We consider the distinction drawn between emails and SMS messages and these other forms of electronic communication to be artificial.

The sunset clause in the *Telecommunications (Interception) Act 1979* (Cth) (TI Act) relating to stored communications ends on 14 June 2006, and until this time agencies such as ASIC have been and will be able to access stored communications using their notice and search warrant powers. Given agencies were able to access stored communications in this manner before and during the period of the Review of the Regulation of Access to Communications (Review), we note the Report of the Review

[1] See our submission dated 28 June 2004 in relation to the Committee's inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004. A copy of this submission is attached for your reference.

did not identify any adverse practice or make any adverse finding about the use by agencies of their powers to access stored communications using their existing powers. In addition, we are not aware of any circumstances arising before or after the Review that militate against the permanent enactment of the stored communications provisions currently subject to the sunset clause. In these circumstances, we suggest that the current stored communications provisions should be permanently enacted.

Although ASIC does not see the need for the stored communications regime proposed by the Bill, should the enactment of the Bill be considered necessary, ASIC makes the following comments in relation to its provisions.

Circumstances in which ASIC may apply for a stored communications warrant

We are concerned about how *serious contravention* would be defined in proposed s5E of the TI Act. Many of the offences we investigate would not satisfy the requirements of the definition in proposed s5E(1)(b)(i) of the TI Act because they do not meet the proposed threshold. The majority of *Corporations Act 2001 (*Cth)(Corporations Act) offences attract a penalty below the suggested threshold, presumably because they are non-violent and do not threaten national security. But they can still be very serious, resulting in great loss to others. Having regard to this, we suggest that a more appropriate threshold for a serious contravention in proposed s5E(1)(b)(i) of the TI Act is a term of imprisonment of at least 12 months.

ASIC is also concerned that the definition of *serious contravention* does not encompass contraventions of legislation administered by ASIC which are neither offences or civil penalties (such as those provisions in Pt 2 Div 2 Subdivision D of the ASIC Act – the consumer protection provisions).

Dealing with stored communications accessed under a stored communications warrant

ASIC requests the ability to use stored communications in all types of civil penalty proceedings

We note stored communications warrant information is permitted to be used for the purposes in proposed s139 of the TI Act. These purposes include the prosecution of certain offences and proceedings for the imposition of a pecuniary penalty (proposed ss139(4)(a) and (b) of the TI Act). Proposed s139(4)(b) of the TI Act would allow stored communications warrant information to be used in civil penalty proceedings seeking the imposition of a pecuniary penalty, but not in the case of civil penalty proceedings which seek compensation or the banning of a person from managing corporations (see ss1317H, 1317HA and 206C of the Corporations Act).

ASIC seeks the ability to use stored communications warrant information in all types of civil penalty proceedings. Although proposed s139(4)(b) of the TI Act appears to have been drafted with reference to the definition of exempt proceedings in the TI Act, we are not aware of any policy reasons why stored communications warrant information could not be used for all types of civil penalty proceedings. This is especially so given that the amount of a civil penalty compensation order could well exceed that of a civil pecuniary penalty order, and that the High Court has concluded

that a civil penalty disqualification order is an order involving the imposition of a penalty or forfeiture (see *Rich v ASIC* [2004] HCA 42). ASIC does not consider it is likely that a civil penalty compensation order will be less than the equivalent of 180 penalty units.

The limited availability of stored communications warrant information in civil penalty proceedings also raises some other issues:

- Would stored communications warrant information be permitted to be used in civil penalty proceedings under the Corporations Act seeking a pecuniary penalty, compensation order and management banning order?
- What would be the consequences of using stored communications warrant information in proceedings seeking a pecuniary penalty where the remedy sought was changed to compensation orders during the proceedings, but after the stored communications warrant information had been adduced in evidence?

ASIC requests the ability to use stored communications in civil and administrative proceedings

We request ASIC be given the ability to use stored communications obtained under a stored communications warrant in civil and administrative proceedings.

Civil proceedings are important ASIC remedies. Approximately 30% of all of ASIC's enforcement litigation actions concern ASIC seeking civil remedies. ASIC will often seek urgent injunctive relief under s1324 of the Corporations Act where (*inter alia*) a person is engaging or has engaged in a contravention of the Corporations Act. ASIC will also often seen injunctive relief under s1323 of the Corporations Act where it appears that a person who has contravened the Corporations Act is about to leave or transfer monies gained from this jurisdiction.

Administrative remedies are vital to ASIC carrying out its regulatory functions and represent around 27% of ASIC enforcement remedies sought. ASIC acts to protect the financial markets from undesirable participants by disqualifying persons from managing corporations, seeking deregistration as auditors and/or liquidators and prohibiting persons from providing any financial services or specified financial services in specified circumstances or capacities.

Although proposed s145 of the TI Act would allow ASIC to use stored communications warrant information in any proceedings after that information has been used in exempt proceedings, for all practical purposes and as the TI Act currently stands, ASIC is unlikely to commence exempt proceedings. However, ASIC often takes regulatory and enforcement action against persons seeking different combinations of remedies, such as criminal and civil penalty proceedings, or urgent civil injunctive proceedings followed by criminal proceedings. The combinations of remedies used by ASIC means that the need to use stored communications in, for example, urgent interlocutory proceedings or to disqualify a defendant from managing corporations (before the conclusion of criminal proceedings) is likely to arise.

Need for different investigative teams

If the provisions of the Bill regarding the use of stored communications remain as they are, and stored communications can only be used in criminal proceedings, ASIC will be required to divide its investigation teams. This will cause difficulty for ASIC in circumstances where it is difficult to determine the additional safeguards that are derived from limiting the use of stored communications.

ASIC must currently divide its teams where investigations involve both possible criminal and civil proceedings. In *Williams v Keelty* [2001] FCA 1301, the issue of possible advertent or inadvertent use, in civil proceedings, of material obtained by search warrant was addressed. If the warrants were sought to obtain material for use by the applicant for the warrant in civil proceedings, which could not have been obtained by discovery, they would have been issued for an improper purpose. Subsequently, the decision in *ASIC v Rich* [2005] NSWSC 62 held that ASIC need not divide its investigation teams on a mixed investigation where search warrants had been executed, provided the criminal parts of the investigation were ongoing. It is not clear whether this would apply to the stored communications warrants, or whether ASIC would need to have separate investigative teams for mixed investigations where these warrants were used. However, this does cause ASIC some difficulty in that there may not be available staff to resource two separate investigations. It is difficult also to see what additional protection is gained by quarantining the use of stored communications and thus requiring the division of investigation teams.

The intended recipient of a communication

Determining the *intended recipient* of a communication is important. This is because a communication must be accessible to its intended recipient (*inter alia*) for it to be a *stored communication* (and will therefore determine, in part, whether a stored communications warrant is required to access it). We consider there are may be ambiguities in the definition of *intended recipient* in proposed s5G of the TI Act as it may be unclear how the addressee of a stored communication would be determined in some cases.

An email may be addressed to a person in an obvious manner (e.g. "john.smith@asic.gov.au"), using a selected term (e.g. "fgh888@hotmail.com") or by a particular role (e.g. "webmaster@asic.gov.au" – a "role address"). Proposed s5G of the TI Act does not indicate in all circumstances how the addressee of the email is to be determined. For example, if the email was addressed to "john.smith@asic.gov.au", but had a salutation of "Dear Mary", would that email be addressed to John Smith or Mary? Also, in the case of a role address that may be accessed by a number of persons, who is the addressee of such a stored communication? On one view, a role address could be considered to be addressed to a person (e.g. the person who is known to be the webmaster in an organisation) but this may not be the better view.

Stored communications not to be accessed

Proposed s108 of the TI Act provides that a person will commit an offence if they access stored communications "without the *knowledge* of the intended recipient of the

stored communication" (emphasis added). That the intended recipient of a stored communication *knows* of that access is therefore an important method of allowing access to a stored communication without using a stored communications warrant. However, it is not clear whether the intended recipient could be made known of that access generally (in that they are advised all their stored communications held by a carrier will be accessed) or whether advice must be given of each stored communication to be accessed. In addition, it is not clear whether the person should be advised of the access contemporaneously or otherwise.

Applications for stored communications warrants

Proposed s110 of the TI Act states that, in relevant circumstances, the "chief officer" of an agency may apply for a stored communications warrant. However, there is doubt as to whether the Chairman of ASIC could satisfy the definition of "chief officer". The *Financial Management and Accountability Regulations 1997* (Cth) specifically define the Chairperson of ASIC to be a "Chief Executive" for the purpose of the *Financial Management and Accountability Act 1997* (Cth). ASIC suggests amending the term "chief officer" in the Bill or inserting the words "(by whatever name called)" in Sch 1 Part 2 of the Bill or proposed s110(2)(b)(i) of the TI Act.

_____