Australian Government
Australian Customs Service

SUBMISSION TO THE

SENATE LEGAL & CONSTITUTIONAL LEGISLATION COMMITTEE

INQUIRY INTO THE

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL

MARCH 2006

Introduction

On 16 February 2006 the Telecommunications (Interception) Amendment Bill 2006 was introduced into the Commonwealth Parliament. This Bill makes certain amendments to the *Telecommunications (Interception) Act 1979* in relation to stored communications including a warrant regime for law enforcement access to stored communications through a telecommunications carrier.

On 1 March 2006 the Senate referred the Bill to the Senate Legal & Constitutional Legislation committee for inquiry and report by 27 March 2006. The Committee has invited the Australian Customs Service to make a written submission.

Customs supports the approach taken in the Bill and considers that the proposed amendments would preserve existing law enforcement powers involving the use of search warrants and other lawful means of accessing stored communications while recognising the need for safeguards where stored communications are to be accessed via a telecommunications carrier.

Customs powers to access stored communications

As a law enforcement agency investigating a range of offences, Customs considers that there is significant evidential value in being able to access stored communications wherever these may be located. These may be found on home and business computers, laptops, mobile telephones as well as stored remotely via the internet.

The existing Customs powers to access stored communications provide the capability of accessing stored communications from individuals. These powers do not involve accessing emails via the telecommunications carrier and concern communications that have been received i.e., ceased to travel over the telecommunications system. Where access is obtained using these powers, the person concerned would be aware at the time or made aware later by notification.

Customs primary concern in considering the Bill has been to ensure the preservation of its existing powers to conduct investigations and to access stored communications.

The following powers may involve accessing stored communications:

(a) Entry to premises under a search warrant issued by a judicial officer (ordinarily a magistrate within the State and Territory court system) pursuant to s. 198 of the Customs Act.

> That officer must be satisfied by information given under oath that there are reasonable grounds for suspecting evidence of particular offences is at the premises, or will be in the next 72 hours. A separate seizure

warrant is needed to take goods forfeited under the Customs Act from such premises (s.203). There are also certain requirements that must be met during the execution of a warrant including announcing before entry, making available a copy of the warrant, taking photographs or videos etc which may be found at Part XII Division 1 Subdivision E of the Customs Act.

Under s. 200, the executing officer or person assisting may bring to the premises equipment reasonably necessary for the examination of a thing found there in order to determine whether it may be seized under the warrant. Various provisions deal with the use of electronic equipment at the premises (ss. 200, 201, 201A, 201B, 202). Parallel provisions exist in the *Crimes Act 1914* relating to the exercise of a search warrant (see ss. 3K, 3L, 3LA, 3LB, 3M) used by the AFP.[1]

The development of a Computer Forensics Team within Customs has provided real advantages in locating and extracting evidence in electronic form found on or accessible from, computers at premises where a search warrant has been executed.

Under s. 201(1) of the Customs Act (or s. 3L of the Crimes Act) a computer found at premises at which a search warrant is being executed may be used to access data at the premises or data stored elsewhere i.e., beyond the warrant premises. This involves accessing the internet at the warrant premises and using equipment located there. If remote access occurs then a notification (s. 201B) must be sent to that other premises.

(b) Entry to premises using monitoring powers under s. 214AB of the Customs Act to ensure compliance with Customs-related law and record keeping requirements.

Entry occurs with the consent of the occupier of premises, but if consent is not given or is withdrawn after initially being given, monitoring powers may be exercised under a warrant obtained from a magistrate (see s.214AF).

The monitoring powers (s. 214AB) not only include power to inspect documents and take extracts or copies but to operate equipment at the premises.[2] While the exercise of the powers is limited to the purposes previously mentioned, they would extend to examining records accessible from computers at the premises relevant to obligations under the Customs Act. Forensic examination of documents or equipment

[1] The parallel provisions in the Customs Act and Crimes Act were introduced by the *Cybercrime Act 2001* (No. 161/2001).

[2] Under section 240 of the Customs Act certain persons are required to retain relevant commercial documents for five years. Also, under section 240AB anyone who communicates information to Customs must retain records verifying the contents of that communication for one year. Such documentation and records may be viewed in the general course of exercising monitoring powers.

would not occur under these powers as they substantially concern auditing. Any matter needing further investigation would be referred to investigators who could seek search warrants and use forensic services as necessary.

A related power to monitoring arrangements concerns the examination powers contained in Part VI (Division 3A) of the Customs Act, which allow Customs to enter premises and examine goods for export that are not yet under Customs control. Although these powers can only be exercised with the consent of the occupier (i.e., warrants are not available in the event that consent is refused), similar to the monitoring powers, they include the power to examine documents.

(c) Document examination powers at the border under ss. 186 and 186A of the Customs Act. These powers enable the detection of illicit material such as pornography as well as evidence of offences generally.

Customs has a general examination power under s. 186 of the Customs Act in which Customs officers at the border may seek to access electronic documents (including stored communications) on mobile telephones (including satellite telephones), handheld and laptop computers. This power applies to both import and export goods when they are subject to the control of Customs[3] and includes reading the electronic document directly or using an electronic device to do so (s. 186(3)(e)). Officers may then in certain circumstances, seek to copy or take extracts from these messages as electronic documents under s.186A.

Following the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* and *Telecommunications (Interception) Amendment (Stored Communications & Other Measures) Act 2005* the concept of stored communications that was adopted ensured the preservation of the existing arrangements Customs had to access stored communications that had reached the recipient.

Given the significance of investigative and monitoring powers to Customs enforcement capability, Customs welcomes the assurance within the Explanatory Memorandum that the Telecommunications (Interception) Amendment Bill 2006 will not interfere with existing lawful means of access. This means that the exercise of Customs powers in relation to search warrants, monitoring powers and the general examination power at the border will not be affected.

Access to stored communications held by a telecommunications carrier

Under the Bill, Customs is an enforcement agency that may apply for the issue of a stored communications warrant. Customs considers that the proposed mechanism will improve the existing arrangements by ensuring that access can

[3] See section 30(1) of the *Customs Act 1901*.

be made to communications via the telecommunications carrier when other means of seeking access may be impractical.

It is noted that the issuing authority must have regard to the extent to which other methods have been used or are available to the agency and whether their use would be likely to assist or prejudice an investigation (see s.116). This means that the practicality of a particular method is a factor to be considered by the issuing authority and balanced against other matters in deciding whether to issue a warrant.

Customs recognises that appropriate safeguards balancing personal privacy and the need to properly investigate offences are necessary in this area and considers that these have been included in the Bill. The jurisdiction of the Ombudsman and reporting requirements also ensure a means of properly oversighting the administrative arrangements.

The proposed mechanism involves stored communications that have ceased moving over the telecommunications system. Customs considers that this approach has value in being consistent with existing approaches regarding accessing stored communications. Additionally, that approach means that no telecommunications interception warrants would be required for those messages. This is appropriate, as a number of enforcement agencies (including Customs) cannot seek telecommunications interception warrants and it remains important to ensure their continued access to stored communications.

AUSTRALIAN CUSTOMS SERVICE

MARCH 2006