



SENATE LEGAL AND CONSTITUTIONAL COMMITTEE Inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

The amendments proposed in the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 are intended to clarify what is presently an unclear area of the law. The amendments will provide certainty for Australian Federal Police investigations by ensuring that telephone interception warrants will continue to be required where law enforcement agencies intercept real time communications, and that access to records and communications that are stored electronically may be obtained under other lawful authority such as a search warrant or with consent.

The AFP supports the proposed amendments. The amendments clarify an ambiguous area of law that has restricted effective investigations into serious Commonwealth offences. They also ensure that the AFP may conduct protective corporate governance.

The proposed amendments will not give the AFP new or greater powers. Importantly, the amendments preserve both existing safeguards that apply to accessing information under the telecommunications regime, and the restrictions and protections applicable when access is undertaken with consent or under another form of lawful authority.

The Bill imposes a sunset clause of twelve months. The Attorney-General has directed that a full review of the *Telecommunications (Interception) Act 1979* be undertaken and reported during this time. The AFP supports a comprehensive review as the appropriate mechanism to deal with the impact of technological developments that have emerged since the TI Act was enacted in the 1970s. Provisions in the Stored Communications Bill are required as a priority in order for the AFP to meet urgent operational needs.

In its submission to the Committee's previous inquiry, the AFP raised serious concerns about:

- potential inability to adequately detect and investigate serious criminal conduct.

The proposed amendments address the AFP's operational concerns.

- Inability for the AFP to conduct protective corporate governance, particularly in relation to monitoring improper content in compliance with the AFP's 'acceptable use' policy, and protecting AFP information systems from viruses.

The proposed amendments address corporate governance concerns in relation to employee conduct, and provide comfort in relation to human intervention required to make a final determination following machine reading or viewing.

Retrieval of stored communications

Search and entry powers assist agencies such as the AFP to gather important evidence in order to expeditiously and effectively carry out their statutory functions. The amendments ensure that the search warrant regime applies unambiguously in circumstances where, for example, an email message has been downloaded by the intended recipient but not opened, or when an email message is held at an ISP before the intended recipient has downloaded it.

The Commonwealth Director of Public Prosecutions has advised that the practical effect of the amendments will be that the *Telecommunications (Interception) Act 1979* will apply where a communication is moving over the telecommunications system but the general law will apply if the communication comes to rest. At that stage, the communication will be subject to the restrictions and protections that apply to other forms of communication.

The proposed amendments will not remove protection from a stored communication. Federal police officers will still need to hold an appropriate search warrant or other form of lawful authority. However, the amendments will ensure that important evidence is not put at risk. Without the amendment allowing expeditious access to stored communications, highly disposable and easily destroyed forms of evidence will be placed at risk.

Transparency

The day-to-day practices of the AFP in relation to search warrants are governed by the *Crimes Act 1914*, CDDP Search Warrant Manual and AFP National Guidelines. The occupier is entitled to be present at all times during the search. Occupiers are entitled to a receipt for all things that are copied, seized or moved. The TI warrant regime places no such requirements on evidence obtained.

Safeguards and protections

Australian Federal Police officers are bound by the Information Privacy Principles in the *Privacy Act 1988*, and may be subject to criminal sanctions relating to the unlawful disclosure of information (eg, section 60A of the *Australian Federal Police Act 1979* and section 70 of the *Crimes Act 1914*).

All conduct undertaken by AFP members, including application and execution of search warrants, is subject to internal and external scrutiny. Complaints about an officer's conduct may be referred to AFP Professional Standards and independently to

the Commonwealth Ombudsman. Depending on the outcome, dismissal or disciplinary action may ensue. Civil remedies and criminal action are also available.

Any evidence that is determined by a court to be seized unlawfully or unfairly may be rendered inadmissible in evidence.

International conventions

The amendments are consistent with the *Cybercrime Act 2001* which allows investigating officers acting under authority of a search warrant the power to operate equipment at the premises to access data held remotely. The Committee inquired into the provisions of the *Cybercrime* legislation in 2001 and made no adverse recommendations in respect of remote access powers.

The proposed amendments are consistent with Australia's obligations under Article 19 of the European Convention of Cybercrime. Article 19 requires that participating nations:

*'adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, in accordance with paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system, or part of it is in its territory, and as such that it is lawfully accessible from or available to the initial system, the authorities be able to **expeditiously** extend the search or similar accessing to the other system.'*

Commonwealth principles for appropriate powers and accountabilities

The Senate Scrutiny of Bills Committee Report of its Inquiry into Entry and Search Provisions in Commonwealth Legislation (2000) stated that existing search warrant accountabilities in Commonwealth legislation (that is, application to an independent issuing officer, notification, statutory thresholds such as a reasonable suspicion that evidential material is located at a premises), and the need for law enforcement to effectively investigate serious criminal activity (through retrieval of stored communications held remotely and to access information held by local ISPs) satisfy that Committee's principles regarding appropriate powers and accountabilities.

Conclusion

The AFP supports the proposed amendments to exempt stored communications from the TI regime and for those stored communications to be accessed by other lawful means. The amendments balance privacy and operational factors, and take into consideration the technical and practical realities of communications in the Twenty-First Century. The proposed amendments will ensure law enforcement effectiveness in respect of the investigation and prosecution of serious offences within existing accountability frameworks.