Australian Government
Action Group into the Law Enforcement
Implications of Electronic Commerce

SENATE LEGAL AND CONSTITUTIONAL COMMITTEE

Inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

Introduction

The Action Group into the Law Enforcement Implications of Electronic Commerce (AGEC) is a Commonwealth law enforcement group comprising representatives of law enforcement, revenue and regulatory agencies, covering a wide mix of Australian Government programs. A number of AGEC members exercise statutory powers in relation to the compulsory provision of information or documents. Certain members may execute search warrants, but the majority of AGEC members[1] are not able to apply telecommunications interception (TI) powers.

AGEC members agree with the need to have the law clarified in relation to email and other forms of stored communications. Technological developments have been such that most records required by agencies to carry out their basic functions are now created, transmitted and stored electronically. Ambiguity has arisen where the records or data that are considered relevant are in the form of an email, text message, or voicemail message, or attached to an email. The convergence of records or data and the telecommunications system has given rise to questions regarding the applicability of the *Telecommunications (Interception) Act 1979* (TI Act).

The AGEC concern has always been that as these forms of communication (particularly email) are used increasingly to move data and business records, necessary information is not put beyond the reach of AGEC members search or compulsory powers.

The Proposed Amendments

AGEC members support the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004.*

Effect of Proposed Amendments

Clarify the law

The TI Act was enacted prior to many forms of communication that are now considered commonplace. Equally importantly, it was enacted prior to the

[1] AGEC comprises the following HOCOLEA agencies: Australian Crime Commission, Australian Competition and Consumer Commission, Australian Customs Service, Australian Federal Police/Australian High Tech Crime Centre, Australian Prudential Regulation Authority, Australian Securities and Investments Commission, Australian Taxation Office, Australian Transaction Reports and Analysis Centre, Commonwealth Director of Public Prosecutions, Department of Immigration and Multicultural and Indigenous Affairs.

convergence of many previously discrete technologies (for example, email or SMS messages used not only as replacement for a telephone call, but also to replace postal services). There is currently nothing in the TI Act that specifically addresses the manner in which stored communications should be dealt with. This situation has given rise to debate and various opinions on how the TI Act should apply to these newer forms of communication.

AGEC considers that through the creation, transmission and storage of records electronically, there is a real potential risk to the capacity of non-TI agencies to carry out their functions. The possibility arises that law enforcement access to a copy of a document would require a TI warrant because it happened to be sent by email and stored on a remote server, whereas without the email aspect it could otherwise be lawfully obtained by other processes. When the document or data that is subject to an agency's powers is, for example, attached to an email or stored electronically, the proposed amendment will remove such ambiguity and confirm that access to it is not an interception. The proposed amendment will provide clarity and confirm that the TI Act operates in relation to real time or 'live' interception.

Confirm that access is only available through lawful authority

The proposed amendment, whilst removing stored communications from the protections of the TI Act, will not remove protection from a stored communication. The access will be dependant on lawful authority, and if an agency does not have such authority, access will not be lawful.

If unauthorised access were to occur, there remains recourse to various legislation to address the occurrence (for example, the *Privacy Act 1988*, the Cybercrime offences within the Commonwealth Criminal Code, the *Telecommunications Act 1997*).

Do not confer fresh powers on agencies

A crucial element of any investigative capacity (whether compliance or criminal) is the ability to access relevant information. Agencies have a range of powers that can include (depending on the agency) notices to produce, rights of entry to premises, seizure powers, and limited search and seizure powers. Many agencies rely on the Australian Federal Police for more comprehensive search warrant provisions in certain circumstances. Without such abilities, agencies could not carry out their statutory functions. Agencies' statutory functions and powers were generally enacted when paper-based systems were the norm, and when corporate computer systems were usually not Internet-connected.

The proposed amendments will not change any particular agency's powers, or give agencies new or greater powers. If an agency does not have power to search or seize, the proposed amendment will not provide it.

Support corporate governance

The Government has articulated its interest in protecting the national information infrastructure and working with the private sector to create a secure and trusted electronic operating environment. Government and corporate maintenance of effective

IT security is crucial to any meaningful efforts to support e-security. Email, as evidenced by the highly successful propagation of viruses, trojans and other malicious code through email programs, is a critical vulnerability for information networks.

Both public and private sector agencies generally undertake active programs of email scanning for malicious code, inappropriate content, and anything else specified as contrary to the agency's 'acceptable use' policy. Such scanning processes generally involve machine reading or viewing, with the human element required to make a final determination in some instances.

By allowing access at the storage destination, or through permission, the proposed amendments will ensure that agencies undertaking this important e-security work will not inadvertently breach the TI Act.

Conclusion

AGEC agencies support the proposed amendments to the TI Act. The proposed amendments will clarify an ambiguous area of the law, assist the agencies in effectively applying their statutory powers, and support effective corporate governance.

Contact

Neil Jensen
Director AUSTRAC and Chair AGEC
PO Box 5516
West Chatswood NSW 1515

Tel. (02) 9950 0014
Fax. (02) 9950 0073

Action Officer

Jodie Durrant
Strategic Coordinator AGEC
GPO Box 401
Canberra ACT 2601

Tel. (02) 6246 2222
Fax. (02) 6246 2121

Liz Atkins
Deputy Director Money Laundering Deterrence
AUSTRAC
PO Box 5516
West Chatswood NSW 1515

Tel. (02) 9950 0011
Fax. (02) 9950 0073