2

Outline of the European Convention on Cybercrime and the Cybercrime Bill

Introduction

2.1 As noted in Chapter 1, the Cybercrime Legislation Amendment Bill 2011 (the Bill) contains provisions intended, among other things, to facilitate Australia's accession to the Council of Europe Convention on Cybercrime (the European Convention). In September 2010, Australia was formally invited by the Council of Europe to accede to the European Convention and, the provisions of the Bill are intended to complete the domestic legislative work required prior to acceding to binding treaty obligations.

2.2 This section outlines some of key aspects of the European Convention and the Bill.

European Convention on Cybercrime

2.3 The European Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.[1] The main objective of the European Convention, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against

1 Council of Europe, Convention on Cybercrime, ETS No. 185.

cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[2]

2.4 The European Convention was developed by Members of the Council of Europe, with the participation of both European and non-European states. At the time of writing, 30 member states of the Council of Europe and one non member state (the United States of America) have acceded to the European Convention. Another 16 nations (both Council of Europe and other) have signed but not ratified the Convention.[3]

2.5 In summary, the European Convention requires States parties to:

- create a range of computer offences (illegal access, illegal interception, data interference, system interference) and computer enabled offences relating to forgery, fraud, child pornography, and infringement of copyright and intellectual property (Chapter II, Articles 2-13);
- establish powers and procedures to allow investigation of computer offences as set out in the European Convention, other computer enabled crime, and the collection of electronic evidence of any criminal offence (Chapter II, Articles 14-21); and
- co-operate with other Convention signatory countries (States parties) in the investigation and proceedings relating to computer offences, and the collection of electronic evidence of any criminal offence (Chapter III, Articles 23-35);

2.6 The European Convention contains several express limitations and assumptions that :

- limits the scope of procedural powers by requiring that such powers are 'for the purpose of specific criminal investigations and proceedings' (Article 14.1). The Explanatory Report to the European Convention reminds States parties that the power and procedures of the European Convention are limited to use for 'an investigation in a particular case';[4]
- permits States parties to limit the range of offences for which assistance is to be given to a foreign country to ensure such measures are proportionate and do not unnecessarily intrude into personal privacy.

---

2 The Convention has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

3 Signatories to the European Convention, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>, viewed 4 August 2011.

4 *Explanatory Report, Convention on Cybercrime,* paragraph 152, p. 25.

For example, a country may limit mutual assistance to serious offences rather than all offences (Article 33);

- requires that all powers and procedures must be subject to conditions and safeguards to ensure the protection of human rights (Article 15). This includes judicial or other independent supervision, the need for grounds to justify an application under the European Convention, and a limitation of the scope and the duration of the particular power or procedure under the Convention (Article 15.1);
- requires States parties to adhere to common standards or minimum safeguards, including those pursuant to obligations under the European Convention for the Protection of Human Rights and Fundamental Freedoms. States parties from other regions of the world are to adhere to applicable human rights instruments (such as the International Covenant on Civil and Political Rights);[5] and
- requires that powers and procedures shall "incorporate the principle of proportionality", and, among other things, the right against self-incrimination, access to legal privileges, and the specificity of individuals or places which are the object of European Convention measures.[6]

Cybercrime Legislation Amendment Bill 2011

2.7 The Bill is described as a 'Bill for an Act to implement the Convention and for other purposes'. In summary, the Bill:

- requires carriers and carriage service providers to preserve the stored communications and telecommunications data for specific persons when requested by certain domestic agencies or when requested by Australian Federal Police on behalf of certain foreign countries;
- ensures Australian agencies are able to obtain and disclose telecommunications data and stored communications for the purposes of a foreign investigation;
- provides for the extraterritorial operation of certain offences in the *Telecommunications (Interception and Access) Act 1979* (TIA Act);

5 *Explanatory Report to the Convention*, paragraph 145, p. 24; see also advice Mr A Seger, Head of Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Council of Europe, *Submission 4*, p. 2.

6 *Explanatory Report to the Convention*, paragraph 146, p. 24.

- removes the constitutional restriction from the computer crime offences in the *Criminal Code Act 1995* so they have adequate scope;
- creates confidentiality requirements in relation to authorisations to disclose telecommunications data.[7]

2.8 The Bill achieves these objectives by amending the following Acts:

- *Telecommunications Act 1997*;
- *Telecommunications (Interception and Access) Act 1979*;
- *Mutual Assistance in Criminal Matters Act 1987*;
- *Criminal Code Act 1995*.

Telecommunications Act 1997

2.9 The *Telecommunications Act 1997* regulates the telecommunications industry.

2.10 Part 13 of the *Telecommunications Act 1997*, makes it an offence for a carrier or carrier service provider and its employees to use or disclose any information or document which comes into its possession in the course of its business, where the information relates to:

- the contents or substance of a communication carried by the carrier or carriage service provider, whether the communication is delivered or not; or
- carriage services supplied, or intended to be supplied, by the carrier or carriage service provider; or
- the affairs or personal particulars of another person.

2.11 The exceptions to the prohibition on disclosure of information include:

- where the disclosure is reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty, and protection of public revenue;
- where the disclosure is made to Australian Security Intelligence Organisation (ASIO) for the performance of its functions;
- where the disclosure is required or is otherwise authorised under a warrant or under law.

7 *Explanatory Memorandum,* Cybercrime Legislation Amendment Bill 2011, p. 1.

2.12 The *Telecommunications Act 1997* imposes an obligation on carriers and carriage services providers to provide reasonable assistance to enforcement agencies necessary to enforce the criminal law and intelligence agencies for security purposes.[8]

Telecommunications (Interception and Access) Act 1979

2.13 The *Telecommunications (Interception and Access) Act 1979* (TIA Act) works in conjunction with the *Telecommunications Act 1997*, to prohibit the interception, collection, or disclosure of communications unless authorised under the Act.

2.14 The TIA Act currently contains three distinct regimes that regulate the use of powers depending on the sensitivity of the data and the purpose for which it is sought:

- interception warrants allow for the real-time copying or recording of information passing over a telecommunications system (chapter 2);
- stored communications warrants allow access to communications stored on the equipment of the carrier (chapter 3); and
- non warrant based authorisations allow for the disclosure of information about communications but not the communications themselves (chapter 4).

2.15 The TIA Act created the position of the Communications Access Coordinator which is located within the Attorney-General's Department, and is the first point of contact for the telecommunications industry, law enforcement agencies and national security agencies under the Act.

Mutual Assistance in Criminal Matters Act 1987

2.16 The *Mutual Assistance in Criminal Matters Act 1987* (MA Act) regulates the granting of international assistance by Australia in relation to criminal matters in response to a request from a foreign country.[9]

2.17 Under the MA Act, the Attorney-General must refuse assistance to foreign countries in six specific circumstances. These include where the offence is a political offence, the person has already been acquitted or pardoned

8 Section 313 of the *Telecommunications Act 1997*.

9 The forms of assistance include, for example, the taking of evidence, production of documents, search and seizure orders, the forfeiture or confiscation of property, and the recovery of pecuniary penalties; see section 5, *Mutual Assistance in Criminal Matters Act 1987*, 'Objects of the Act.'

(double jeopardy) or because providing assistance would prejudice the sovereignty, security or national interest of Australia (paragraphs 8 (1) (a)–(f)).

2.18 Assistance may also be refused on a number of other grounds, including :

- where the conduct is not an offence in Australia;
- where if it occurred in Australia the offence could not be prosecuted because of lapse of time or other reasons;
- would prejudice an Australian investigation, or
- would impose an excessive burden on Commonwealth, state or territory resources (subsection 8 (2)).

Death penalty

2.19 The Attorney-General must refuse assistance to a foreign country if the offence carries the death penalty in that country, unless he or she is of the opinion that special circumstances of the case warrant the provision of assistance (section 8 (1A) of the MA Act). Under section 8(1B), the Attorney-General may also refuse assistance where the assistance may result in the death penalty being imposed, and, having regard to the interests of international cooperation decided that assistance should not be granted.

Criminal Code Act 1995

2.20 The *Criminal Code Act 1995* provides the general principles of criminal responsibility that apply in the prosecution of all offences against laws of the Commonwealth. It sets out the elements of offences and what is required to establish guilt in respect of offences, including as to the required burden of proof. Part 10.7 of the Criminal Code details computer offenses, including unauthorised modification or impairment in, to, or from a computer.