Model Law on Computer and Computer Related Crime

The Commonwealth

Office of Civil and Criminal Justice Reform

Model Law on Computer and Computer Related Crime

The Commonwealth

Wherever possible, the Commonwealth Secretariat uses paper sourced from responsible forests or from sources that minimise a destructive impact on the environment.

Printed and published by the Commonwealth Secretariat.

Introduction

Cybercrime at all levels of sophistication poses unprecedented challenges in terms of legislation, law enforcement, and policy-making. 'Cybercrime' is not a defined legal category, but includes: (a) offences aimed at computers, computer or communications systems, their users or the data they contain; and (b) more traditional offences committed using these systems, especially if technologies have significant effects on how the crime is committed or investigated.

Procedural laws must also deal with the issues raised when digital material is relied upon in court, whatever the nature of the offence. International co-operation is facilitated by common approaches to criminalisation and any cybercrime-specific investigative or procedural rules.

Cybercrime does not respect national boundaries. That creates challenges for the public sector, in terms of legislation and investigative and prosecutorial capacity and reach, and for the private sector, which must address technical vulnerabilities in the systems it designs and operates which sometime straddle many national jurisdictions. The internet brings criminals together to share information on how to commit crimes and how to avoid detection, adding a new dimension to organised crime. Increasingly, successful attacks are founded on knowledge, co-operation and deals created and shared between networks of individuals and groups. Offenders seek out and exploit any weak links or vulnerable locations.

Fast communications mean that offences can be committed very quickly, and that digital evidence of them can be erased equally quickly. Even with the best possible legal measures, the speed of offending is a major challenge for investigators, and the practical implications of this include the need for a high degree of skill, high quality equipment and extensive training. The complexity and speed of evolution of cybercrime makes it essential that expertise in policy, law, law enforcement, prosecution and prevention not only be developed but also monitored, maintained and updated frequently. To do this efficiently it is important that all countries co-operate effectively, both within the Commonwealth and globally.

This Model Law on Computer and Computer-Related Crime aims to support Commonwealth countries in putting a place a legal framework for criminalisation and investigation of computer and computer-related crimes.

The Model Law is closely related to the Model Law on Electronic Evidence, as well as the Model Law on Electronic Transactions.

The Model Law is also closely related to amendments to the Harare Scheme relating to Mutual Legal Assistance in Criminal Matters within the Commonwealth, approved by Law Ministers in 2011. Those amendments include new provisions as to the interception of telecommunications and postal items; covert electronic surveillance; the use of live video links in the course of investigations and judicial procedures; and asset recovery.

Background

The initiative for the creation of the Model Law on Computer and Computer-Related Crime came from Commonwealth Law Ministers at their meeting held 3-7 May 1999, in Port of Spain, Trinidad and Tobago.

At that meeting, Law Ministers considered the impact of technology on various aspects of the law and highlighted the issue of computer crime for further consideration. Ministers asked that an expert group be convened to consider the content of a model law on the basis of work then under way on the Council of Europe draft Convention on Cybercrime. Topics that were specifically mentioned for consideration included criminalisation of various forms of computer abuse, admissibility of computer evidence, and investigation of computer-related crime.

An Expert Group prepared the first draft of the Model Law which was considered by Senior Officials in 2001. That draft took into account a late draft of what was to become the Council of Europe Budapest Convention on Cybercrime.

Senior Officials decided that the Expert Group should be reconvened in order to review the draft Model Law in light of developments since the original meeting of the Group, including changes made to the final Council of Europe Budapest Convention on Cybercrime.

The Expert Group reconvened in March 2002 and prepared a final draft of the Model Law. The final draft was submitted to Commonwealth Law Ministers at their meeting of 18-21 November 2002, held in Kingstown, St Vincent and the Grenadines.

Law Ministers commended the Model Law for use by those Commonwealth member countries seeking assistance in the development of an appropriate legislative framework. Law Ministers also mandated Senior Officials to keep the Model Law on Computer and Computer-Related Crime under review, to ensure that the law is kept up to date with regard to emerging technology and investigative techniques. As of July 2017, the Model Law is under consideration for review.

Summary of the Provisions of the Model Law

The Model Law is in three Parts. Part I contains in section 3 the important definitions of 'computer data', 'computer system', 'service provider' and 'traffic data' together with an additional definition of 'computer data storage medium'. Section 4 of the Model Law deals with the jurisdiction of the enacting state.

Part II of the Model Law (sections 5-10) is concerned with substantive criminal law and the creation of offences. The offences relate to illegal access, interfering with data, interfering with a computer system, the illegal interception of data, illegal devices and child pornography using a computer system or a computer data storage medium. The Model Law does not cover computer-related forgery or fraud.

Part III of the Model Law (sections 11 to 21) deals with 'procedural law'. It contains provisions as to search and seizure warrants, the obligation to assist the police, recording and access to seized data, the production of data, the disclosure of stored traffic data, the preservation of data, the interception of electronic communications and the interception of traffic data, with provisions as to evidence, confidentiality and the limitation of liability together with the necessary definitions.

Computer and Computer Related Crimes Bill

Part I

Introduction

Section

Part II

Offences

Part III

Procedural Powers

Computer and Computer Related Crimes Bill

AN ACT to combat computer and computer related crime and to facilitate the collection of electronic evidence.

Part I

Introduction

Short title

1. This Act may be cited as the *Computer and Computer Related Crimes Act*.

Object

2. The object of this Act is to protect the integrity of computer systems and the confidentiality, integrity and availability of data, prevent abuse of such systems and facilitate the gathering and use of electronic evidence.

Definitions

3. In this Act, unless the contrary intention appears:

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"computer data storage medium" means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device;

"computer system" means a device or a group of inter-connected or related devices, including the internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function;

"service provider" means:

(a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and

(b) any other entity that processes or stores computer data on behalf of that entity or those users.

"traffic data" means computer data:

(a) that relates to a communication by means of a computer system; and

(b) is generated by a computer system that is part of the chain of communication; and

(c) shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.

Jurisdiction

4. This Act applies to an act done or an omission made:

   (a) in the territory of [*enacting country*];

   (b) on a ship or aircraft registered in [*enacting country*];

   (c) by a national of [*enacting country*] outside the jurisdiction of any country; or

   (d) by a national of [*enacting country*] outside the territory of [*enacting country*], if the person's conduct would also constitute an offence under a law of the country where the offence was committed.

NOTE: *The nature of cyber crime is such that it is important to have an extended jurisdictional basis for such offences, as often acts committed in the territory of one jurisdiction may have a substantial impact on other jurisdictions. Some countries can address this issue through case law that interprets "territorial jurisdiction" broadly to include situations where there is a "real and substantial link" to that jurisdiction albeit elements of the offence may have been committed elsewhere. In other countries the legislation specifically provides that jurisdiction may be assumed where there is one substantial link to the country, which term is broadly defined. Whichever approach is adopted, it is important that countries consider the question of jurisdiction carefully and adopt provisions that will ensure no safe haven for those who commit cyber crime.*

Part II

Offences

Illegal access

5. A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [*period*], or a fine not exceeding [*amount*], or both.

Interfering with data

6. (1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts:

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data; or

(e) denies access to data to any person entitled to it;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [*period*], or a fine not exceeding [*amount*], or both.

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

Interfering with computer system

7. (1) A person who intentionally or recklessly, without lawful excuse or justification:

(a) hinders or interferes with the functioning of a computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer system;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [*period*], or a fine not exceeding [*amount*], or both.

In subsection (1) "hinder", in relation to a computer system, includes but is not limited to:

(a) cutting the electricity supply to a computer system;

(b) causing electromagnetic interference to a computer system;

(c) corrupting a computer system by any means; and

(d) inputting, deleting or altering computer data.

Illegal interception of data etc.

8. A person who, intentionally without lawful excuse or justification, intercepts by technical means:

(a) any non-public transmission to, from or within a computer system; or

(b) electromagnetic emissions from a computer system that are carrying computer data;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [*period*], or a fine not exceeding [*amount*], or both.

Illegal devices

9. (1) A person commits an offence if the person:

(a) intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence against section 5, 6, 7 or 8; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;

with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8; or

(b) has an item mentioned in subparagraph (a)(i) or (a)(ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8.

(2) A person found guilty of an offence against this section is liable to a penalty of imprisonment for a period not exceeding [*period*], or a fine not exceeding [*amount*], or both.

[(3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (1)(a)(i) or (1)(a)(ii), a court may, having regard to all the circumstances, infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8.]

NOTE: *Subsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

Child pornography

10. (1) A person who, intentionally, does any of the following acts:

(a) publishes child pornography through a computer system;

(b) produces child pornography for the purpose of its publication through a computer system; or

(c) possesses child pornography in a computer system or on a computer data storage medium;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [*period*], or a fine not exceeding [*amount*], or both.

NOTE: *The laws respecting pornography vary considerably throughout the Commonwealth. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in all member countries. However a country may wish to extend the application of this prohibition to other forms of pornography, as the concept may be defined under domestic law.*

NOTE: *The pecuniary penalty will apply to a corporation but the amount of the fine may be insufficient. If it is desired to provide a greater penalty for corporations, the last few lines of subsection (1) could read:*

"commits an offence punishable, on conviction:

(a) *in the case of an individual, by a fine not exceeding* [**amount**] *or imprisonment for a period not exceeding* [**period**]*; or*

(b) *in the case of a corporation, by a fine not exceeding* [**a greater amount**].

(2) It is a defence to a charge of an offence under paragraph (1) (a) or (1) (c) if the person establishes that the child pornography was a bona fide scientific, research, medical or law enforcement purpose.

NOTE: *Countries may wish to reduce or expand upon the available defences set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defences to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.*

(3) In this section:

"child pornography" includes material that visually depicts:

(a) a minor engaged in sexually explicit conduct;

(b) a person who appears to be a minor engaged in sexually explicit conduct; or

(c) realistic images representing a minor engaged in sexually explicit conduct.

"minor" means a person under the age of [*x*] years.

"publish" includes:

(a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or

(c) print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in paragraph (a).

Part III

Procedural Powers

Definitions for this Part

NOTE: *As most jurisdictions already have legislative or common law search powers, the purpose of sections 11 and 12 is to illustrate the amendments necessary to existing powers to ensure that such powers include search and seizure in relation to computer systems and computer data.*

The example given is of necessary amendments to a sample general search warrant provision but similar amendments would need to be made to all search powers, including powers of search on arrest, search without warrant in exigent circumstances, and plain view seizures

The general search warrant provision is provided for illustration and is not intended as a comprehensive model of general search powers. Some options have been included also where there may be differing standards as between countries. These options are bracketed in italics.

11. In this Part:

"thing" includes:

(a) a computer system or part of a computer system;

(b) another computer system, if:

i. computer data from that computer system is available to the first computer system being searched;

ii. there are reasonable grounds for believing that the computer data sought is stored in the other computer system; and

(c) a computer data storage medium.

"seize" includes:

(a) make and retain a copy of computer data, including by using on-site equipment;

(b) render inaccessible, or remove, computer data in the accessed computer system; and

(c) take a printout of output of computer data.

Search and seizure warrants

12. (1) If a magistrate is satisfied on the basis of [*information on oath*] [*affidavit*] that there are reasonable grounds [*to suspect*] [*to believe*] that there may be in a place a thing or computer data:

(a) that may be material as evidence in proving an offence; or

(b) that has been acquired by a person as a result of an offence;

the magistrate [*may*] [*shall*] issue a warrant authorising a [*law enforcement*] [*police*] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data.

NOTE: *If the existing search and seizure provisions contain a description of the content of the warrant, either in a section or by a form, it will be necessary to review those provisions to ensure that they also include any necessary reference to computer data.*

Assisting Police

13. (1) A person who is in possession or control of a computer data storage medium or computer system that is the subject of a search under section 12 must permit, and assist if required, the person making the search to:

(a) access and use a computer system or computer data storage medium to search any computer data available to or in the system;

(b) obtain and copy that computer data;

(c) use equipment to make copies; and

(d) obtain an intelligible output from a computer system in a plain text format that can be read by a person.

(2) A person who fails without lawful excuse or justification to permit or assist a person commits an offence punishable, on conviction, by imprisonment for a period not exceeding [*period*], or a fine not exceeding [*amount*], or both.

NOTE: *A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self-incrimination.*

Record of and access to seized data

14. (1) If a computer system or computer data has been removed or rendered inaccessible, following a search or a seizure under section 12, the person who made the search must, at the time of the search or as soon as practicable after the search:

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to:

i. the occupier of the premises; or

ii. the person in control of the computer system.

(2) Subject to subsection (3), on request, a police officer or another authorized person must:

(a) permit a person who had the custody or control of the computer system, or someone acting on their behalf to access and copy computer data on the system; or

(b) give the person a copy of the computer data.

(3) The police officer or another authorized person may refuse to give access or provide copies if he or she has reasonable grounds for believing that giving the access, or providing the copies:

(a) would constitute a criminal offence; or

(b) would prejudice:

i. the investigation in connection with which the search was carried out;

ii. another ongoing investigation; or

iii. any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

Production of data

15. If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that:

(a) a person in the territory of [*enacting country*] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; and

(b) an internet service provider in [*enacting country*] produce information about persons who subscribe to or otherwise use the service; and

(c) [*a person in the territory of* [enacting country] *who has access to a specified computer system process and compile specified computer data from the system and give it to a specified person.*]

NOTE: *As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.*

NOTE: *Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.*

Disclosure of stored traffic data

Option 1

16. If a police officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify:

a) the service providers; and

b) the path through which the communication was transmitted.

Option 2

16. If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

(b) the path through which the communication was transmitted.

Preservation of data

17. (1) If a police officer is satisfied that:

(a) data stored in a computer system is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk that the data may be destroyed or rendered inaccessible;

the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.

(2) The period may be extended beyond 7 days if, on an ex parte application, a [*judge*] [*magistrate*] authorizes an extension for a further specified period of time.

Interception of electronic communications

18. (1) If a [*magistrate*] [*judge*] is satisfied on the basis of [*information on oath*] [*affidavit*] that there are reasonable grounds [to suspect][*to believe*] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [*may*] [*shall*]:

(a) order an internet service provider whose service is available in [*enacting country*] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorize a police officer to collect or record that data through application of technical means.

Interception of traffic data

19. (1) If a police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request that person to:

(a) collect or record traffic data associated with a specified communication during a specified period; and

(b) permit and assist a specified police officer to collect or record that data.

(2) If a magistrate is satisfied on the basis of [*information on oath*] [*affidavit*] that there are reasonable grounds [*to suspect*] that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate [*may*] [*shall*] authorize a police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

Evidence

20. In proceedings for an offence against a law of [*enacting country*], the fact that:

(a) it is alleged that an offence of interfering with a computer system has been committed; and

(b) evidence has been generated from that computer system;

does not of itself prevent that evidence from being admitted.

Confidentiality and limitation of liability

21. (1) An internet service provider who without lawful authority discloses:

(a) the fact that an order under section 13, 15, 16, 17, 18 and 19 has been made;

(b) anything done under the order; or

(c) any data collected or recorded under the order;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [*period*], or a fine not exceeding [*amount*], or both.

(2) An internet service provider is not liable under a civil or criminal law of [*enacting country*] for the disclosure of any data or other information that he or she discloses under sections 13, 15, 16, 18 or 19.

The Commonwealth

P15370_11