
**BUSINESS SOFTWARE ALLIANCE
COMPUTER AND COMPUTER RELATED CRIMES MODEL LAW
(Based on the Council of Europe Cybercrime Convention)**

PART I

INTRODUCTION

Section

- | | |
|---|--------------|
| 1 | Short title |
| 2 | Object |
| 3 | Definitions |
| 4 | Jurisdiction |

PART II

OFFENCES

- | | |
|----|-----------------------------------|
| 5 | Illegal access |
| 6 | Interfering with data |
| 7 | Interfering with computer system |
| 8 | Illegal interception of data, etc |
| 9 | Illegal devices |
| 10 | Computer Forgery |
| 11 | Computer Fraud |
| 12 | Child pornography |

PART III

PROCEDURAL POWERS

- | | |
|----|---|
| 13 | Definitions for this Part |
| 14 | Search and seizure warrants |
| 15 | Assisting police |
| 16 | Record of and access to seized data |
| 17 | Production of data |
| 18 | Disclosure of stored traffic data |
| 19 | Preservation of data |
| 20 | Interception of electronic communications |
| 21 | Interception of traffic data |
| 22 | Evidence |
| 23 | Confidentiality and limitation of liability |

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. **[COE Preamble]**
- 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; **[COE Article 1.b.]**
- “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; **[Model Commonwealth Law]**
- “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; **[COE Article 1.a.]**
- “service provider” means:
- [COE Article 1.c.]**
- (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.
- [COE Article 1.d.]**
- “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 **[COE Article 22.1.a-d]** 4. This Act applies to an act done or an omission made:
- (a) in the territory of [enacting country]; or
 - (b) on a ship or aircraft registered in [enacting country]; or

- (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
[COE Article 2]

5. A person who, without lawful excuse or justification, accesses the whole or any part of a computer system with the intent of obtaining computer data or other dishonest intent 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
[COE Article 4]

6.(1) A person who, intentionally and without right, does any of the following acts:

- (a) destroys or alters data; or
- (b) renders data meaningless, useless or ineffective; or
- (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
[COE Article 5]

7.(1) A person who :

- (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;

when committed intentionally and without lawful excuse or justification, commits an offence punishable, on conviction, by imprisonment for a period not exceeding **[period]**, or a fine not exceeding **[amount]**, or both.

**[Model
Common-
wealth law]**

In subsection (1) "hinder", in relation to a computer system, includes but is not limited to: [why this list of activities rather than those cited in the COE Convention Explanatory Report?]

- (a) cutting the electricity supply to a computer system; and
- (b) causing electromagnetic interference to a computer system; and
- (c) corrupting a computer system by any means; and
- (d) inputting, deleting or altering computer data;

Illegal
interception
of data etc.
**[COE Article
3]**

8. A person who, intentionally intercepts by technical means, any non-public transmission to, from or within a computer system, with dishonest intent, commits an offence punishable, on conviction, by imprisonment for a period not exceeding **[period]**, or a fine not exceeding **[amount]**, or both.

Illegal
devices
**[COE Article
6]**

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

- (a) intentionally without right, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:
 - (i) a device, including a computer program, that is designed or adapted primarily for the purpose of committing an offence under this Act ; 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 under this Act; or
- (b) has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence under this Act.

(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) A person does not commit an offence under this section if the production, procurement for use, import, export, distribution, otherwise making available or possession is not for the purpose of committing an offence under this Act, such as for the authorised testing or protection of a computer system.

[(4) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (a) (i) or (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 under this Act.]

NOTE: *Subsection 4 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.*

Computer Related Forgery
[COE Article 7]

10. A person who, intentionally and without right, , inputs, alters, deletes, or suppresses computer data with intent to defraud, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Computer Related Fraud
[COE Article 8]

11. A person who, intentionally and without right causes the loss of property to another by :

- (a) inputting, altering, deleting or suppressing computer data or
- (b) interfering with the functioning of a computer system

with the fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or another, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

Child pornography
[COE Article 9]

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

- (a) publishes child pornography through a computer system; or
- (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 world. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in most 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.*

[Model
Common-
wealth law]

(3) In this section:

“child pornography” includes material that visually depicts:

- (a) a minor engaged in sexually explicit conduct; or
- (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; or
- (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

Scope of Procedural Provisions [COE Article 14]

Sec. __. The powers and procedures set forth in this Part shall apply to specific investigations or proceedings involving:

- (a) the criminal offenses established in Part II
- (b) other criminal offenses committed by means of a computer system; and
- (c) the collection of evidence in electronic form of a criminal offense

Conditions and Safeguards [COE Article 15]

Sec. __. (1) The establishment, implementation and application of the powers and procedures of this Part shall:

- (a) be subject to conditions and safeguards provided for under domestic law;
- (b) incorporate the principle of proportionality;
- (c) include grounds justifying application, and be limited in scope and duration; and
- (d) to the extent that it is consistent with the public interest, in particular the sound administration of justice, consider the impact upon the rights, responsibilities and legitimate interests of third parties.

Definitions
for this Part

NOTE: *As most jurisdictions already have legislative or common law search powers, the purpose of sections 13 and 14 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 bold and italics.

[COE Article 13. In this Part:
19.1-2]

"thing" includes:

- (a) a computer system or part of a computer system; and
- (b) another computer system, if:
 - (i) computer data from that computer system is available to the first computer system being searched; and
 - (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

[COE Article 19.3]

"seize" includes:

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

- (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
[Model Common-wealth law]

14.(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* 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. Standards for seizing computer evidence should parallel those of seizing physical evidence. The above text is illustrative only.*

Assisting Police
[Model Common-wealth law]

15.(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 this Act must permit, 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; and
- (b) obtain and copy that computer data; and
- (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 intentionally 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: *This section would need to be drafted in accordance with a country's constitutional or common law protections against self-incrimination.*

Record of and access to seized data
[Model Common-wealth law]

16.(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; or
 - (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 [COE Article 18.1] 17. 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) A 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: *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**

[COE Article 17, and Model Common-wealth law] 18. 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

18. 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
[COE Article 16]

19.(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 [number of days][90?] as specified in the notice.

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

Interception of electronic communications
[COE Article 21]

20.(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*:

- (a) order a service provider whose service is available in [enacting country] through application of technical means, within its existing technical capability, 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
[COE Article 20]

21.(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 „within its existing technical capability, to:

- (a) To collect or record traffic data associated with a specified subscriber account during a specified period; and

- (b) To preserve that information pending receipt of an order under subsection 21(2).

[Model
Common-
wealth law]

(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 subscriber account during a specified period through application of technical means.

Evidence
[Model
Common-
wealth law]

22. 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.

Confidential
ity
and
limitation of
liability
[Model
Common-
wealth law]

23.(1) A service provider who without lawful authority discloses:

- (a) the fact that an order under this Act has been made; or
- (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) A 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 this Act.