LMM(02)17

MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME

BACKGROUND

1. In Port of Spain, Law Ministers considered the impact of technology on various aspects of the law. One of the issues highlighted for further consideration was computer crime. Ministers recognized the challenges for law enforcement arising from the developments in technology including the new types of criminal activity and the difficulties associated with the gathering and use of electronic evidence. Ministers asked that an expert group be convened to consider the content of a model law on the basis of the work of the Council of Europe on the Draft Convention on Cyber Crime (*COE Draft Convention*). 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.

EXPERT GROUP

2. Following the course of action identified, the Secretariat convened an expert group to address the topic of Computer Crime and related issues.

3. Working on the basis of the *COE Draft Convention*, the expert group on Computer Crime and Related Criminal Law issues made recommendations, *inter alia*, for the content of a model law. On the basis of their report a draft model law, combined with the model law on e-commerce, was prepared and submitted to Senior Officials for their consideration.

SENIOR OFFICIALS

4. At their meeting in November 2001 Senior Officials decided that the Expert Group should be reconvened to review the draft model law in light of recent developments, in particular the changes made to the Council of Europe Convention on Cyber Crime, since the original meeting of the group. They also requested that the combined model law be separated into two model laws addressing the separate subject areas of e-commerce and computer crime and related issues.

5. The Expert Group was reconvened in March 2002 and based on their report (*Annex A*) a revised Model Law on Computer and Computer Related Crime was prepared. (*Annex B*).

6. The redrafted Model Law was circulated to Senior Officials for their consideration and comment. On the basis of comments received from Senior Officials, some small drafting changes and corrections were made and additional notes were added to the model. The only substantive change is a proposal by Canada to redraft paragraph 3 of Clause 9 on illegal devices. The original text and the proposal from Canada are highlighted in bold in *Annex B.*

ACTION SOUGHT

7. The Model Law on Computer and Computer Related Crime is recommended for endorsement by Law Ministers.

Commonwealth Secretariat
Marlborough House
London SW1Y 5HX

October 2002

ANNEX A

REPORT OF 2ND MEETING OF EXPERT GROUP ON COMPUTER AND COMPUTER RELATED CRIME

I INTRODUCTION

1. In July 2000, an expert group meeting was convened by the Commonwealth Secretariat to prepare drafting instructions for a model law on computer and computer related crime. This was in response to the mandate given to the Secretariat by Law Ministers.[1] On the basis of the report of that group, a draft model law was prepared and submitted to Senior Officials of Law Ministries at their meeting in London in November 2001.

2. Senior Officials were of the opinion that the expert group should be reconvened to review the draft model law in light of recent developments, in particular the changes made to the Council of Europe Convention on Cyber Crime, since the original meeting of the group. The Government of Canada offered to fund the reconvened meeting of the group.

3. Senior Officials agreed that any interested member countries that wished to provide written submissions on the draft model law should do so by the end of December 2001. The Government of Australia submitted written comments, which were referred to the Expert Group for their consideration.

4. The 2nd meeting of the expert group on Computer and Computer Related Crime took place in London, 5-7 March 2002. A list of participants is attached as *Annex I.*

II REVIEW OF DRAFT MODEL LAW - GENERAL

5. The Group reviewed the draft model law and the written comments submitted and made recommendations for amendments to reflect recent developments and to ensure that the draft prepared was consistent with the instructions and intent of the Group as set out in the original report. A revised model law has been prepared on the basis of the recommendations arising from the second meeting of the Expert Group..

III REVIEW OF DRAFT MODEL LAW – SPECIFIC ISSUES

1. Separation of E-Commerce and Computer Crime Models

6. As recommended by Senior Officials, the Group was of the view that the original draft model, which encompassed both e-commerce and computer crime, should be separated into two model laws. As a result, only those provisions relating to computer crime were considered at this meeting. The model law in this area has been renamed accordingly - The Computer and Computer Related Crimes Act and the titles and object provisions have been redrafted to reflect this more limited subject area.

2. Definitions (Section 3)

[1] See publication Law in Cyber Space for report of the expert group.

7. In light of the separation of the model laws, the Group went on to reconsider the definition provisions, relevant to computer crimes, which in the combined draft model law had been merged with definitions for e-commerce. The Group reiterated its original recommendation for inclusion of the four definitions from the Council of Europe Convention – *computer data, computer system, service provider* and *traffic data.* On a general point, the Group noted that for some of the definitions, the Council of Europe had moved from the term "includes" to the term "means". The Group was of the view that for the purpose of legislation, the narrower more defined term "means" should be employed for all the definitions. As to the content of those definitions, each one was considered separately.

8. No changes were made to the definition of *computer data*, which had also remained the same in the Council of Europe Convention. However, there was some discussion as to whether the definition should be restricted to computer data or extend to data generally. On the basis that this model law is addressing computer and computer related issues, it was determined that the definition should relate to the narrower term "*computer data*".

9. Two issues were discussed with respect to the definition of *computer system*. The Group noted that the words "or any other function" had been deleted from the Council of Europe definition in the final version. This was apparently because the term would capture too broad a range of devices including things such as washing machines and cars that contain computer chips. However, the Group was of the opinion that it would be better to have an inclusive definition in a model law, which would allow for flexible application to developing technology. The Group noted that in the common law the tradition of prosecutorial discretion would provide a protection against inappropriate application of the offence provision.

10. The Expert Group considered it important to cover the Internet in model offence provisions. While some concerns about overreaching were considered, it was determined that the combination of prosecutorial discretion, the qualification of "without lawful justification or excuse and targeting the Internet network located in the country's territory could prevent misapplication of the offences. In order to be certain that the definition adopted would cover the Internet, the Group recommended that specific reference be made to it in the definition.

3. Offence provisions

11. The Group went on to review all of the offences individually, though only a few were the subject of discussion or recommendation for substantive amendment. Only the key points of discussion or amendment are summarized in this report below.

(a) Illegal Interception of Data (Section 8)

12. In its original report the Group had recommended against limiting the application of this offence to "non- public" transmissions because of concerns that this would unduly limit the scope of the offence. However, in light of the importance that the Council of Europe placed on this qualifying language and its inclusion in the final version of the Convention, the Group reconsidered the issue.

13. The discussion revealed that some of the problems with the qualifying language arose from wording that made it unclear whether the word "transmission" was being used as a verb to connote the medium or as a noun covering the communication itself. The Group was of the opinion that the offence provision had to be framed in sufficiently broad terms to capture

interception of any communication that was non – public, regardless of whether the medium used was public or private. Thus the Group recommended a new draft of the offence provision to reflect this principle.

14. The Group also gave consideration to the question of the appropriate *mens rea* for the offence but concluded that the original approach – intentionally or recklessly – was an appropriate standard to employ.

(b) Illegal Devices (Section 9)

15. One of the difficult issues with the offence of illegal devices is how to distinguish the use, import, production etc. of such devices for legitimate purposes, such as testing or protecting a system, as opposed to illegitimate purposes. The issue was of such significance that the final version of the Council of Europe Convention contained a new clause specifically excluding the application of this offence provision in cases of legitimate purpose.

16. There was a lengthy discussion as to whether such an exclusion clause should be similarly reflected in the model law. While the Group agreed that the section should not apply to situations of innocent purpose, they were satisfied that the combination of "without lawful excuse or justification" and the requirement for a specific intention of criminal purpose was sufficient to prevent an overly broad application of the section.

(c) Child Pornography (Section 10)

17. The possible defence to the child pornography offence was reconsidered in light of concerns that it was too broadly worded. There was particular focus on the general reference to "rehabilitation", which would allow anyone to raise a doubt on the basis that he or she was using the material to "rehabilitate" him or herself. The Group decided to remove the reference to rehabilitation and limit the defence to situations of bona fide scientific research or medical purposes. The Group was also of the view that the defence should extend to the possession of such material for law enforcement purposes, such as seizure and possession in the course of evidence gathering or court processes. On that basis law enforcement was added to the list of legitimate purposes.

4. Procedural Powers (Part 3)

18. The various procedural powers in the model law were reviewed in detail. The major issues discussed are outlined below.

(a) Search and seizure powers (Section 12)

19. The Group considered at length how best to reflect the necessary powers for search and seizure in the computer context, given that most jurisdictions will have existing general search powers that will need to be amended. As set out in the detailed note in the model law, the Group decided to provide an example of amendments to a general search power, without including a lengthy model provision for general search and seizure powers, which would be unnecessary for most jurisdictions.

20. In recognition of the vast range of approaches to search and seizure throughout Commonwealth jurisdictions, the example also uses alternative language to further illustrate that it is intended as an example only. Those alternatives are also used to highlight that there are various approaches to search and seizure in Commonwealth countries in terms of the authorities that apply for and issue the warrant, the type of material to be filed in support of applications and the threshold to be met for issuance of the warrant.

21. The example illustrates that the items to be searched for and seized should clearly include not only tangible "things" but also intangible "computer data". Thus, that specific language needs to be included throughout any search provision.

22. Another important point to consider is the definition of terms such as "thing" or "item" – the example uses "thing" and the definition of "seize". Because of the nature of computer systems and data, those definitions need to be sufficiently broad and flexible to ensure that the police can carry out a proper and thorough search and seizure within the computer context. Definitions of that nature have been included in the draft model law.

23. The Group emphasized that each jurisdiction will need to review all existing search powers, whether statutory or by common law, and adopt legislative provisions that will ensure that all such powers extend to search and seizure in the computer context.

(b) Assisting police (Section 13)

24. There was an extensive discussion of this provision (former section 14), which obligates persons in control of computer systems or storage mediums to assist law enforcement in the course of a search. As was recognized by the Group in their original report, in the computer context such assistance is critically important in order for the person making the search to obtain the computer data in an intelligible and useful form. Therefore, the Group remained convinced that a specific provision on assistance should be included in the model law, above and beyond the normal powers of the police to seek assistance during a search. The Group discussed a proposal by Australia that the offence should be limited to assistance that is reasonable and necessary. Ultimately it was decided that the qualification of without lawful excuse or justification would provide a sufficient protection against unreasonable requests and that it would be too onerous to require proof in each instance that the request was necessary and reasonable. The Group however adopted the further Australian suggestion that because this provision is framed as an obligation on persons and not a power flowing from an order of the court, a specific penalty for failure to comply with a request for assistance should also be included.

25. However, the Group recognized that, even with possible penalties attaching to non-compliance, because the assistance involves information held by a person, there were practical limits to the effectiveness of the compulsion power. As is the case with breathalyser provisions, a person could decide to refuse to provide the information and face the applicable penalties rather than giving the police access to the computer data. Countries may wish to keep this in mind in determining the applicable penalty for failure to comply with a request.

26. At the same time, the Group emphasized that within each jurisdiction careful consideration will have to be given to the interplay between this legislative provision and constitutional or common law protections against self-incrimination, given that the section requires a person to provide information that may in some circumstances be self incriminating. There were varying opinions as to the extent to which the protection against self-incrimination would preclude the use of evidence obtained as a result of the compelled disclosure of the information. It was clear that the extent of any violation of the protection and the impact on the use of the evidence would vary from country to country. In addition, there will be substantial differences as to how countries deal with this issue depending on whether there is a constitutional or common law protection against self-incrimination. It is for each jurisdiction to determine how to incorporate such an obligation in domestic law and whether or not it will need to be qualified in light of the protection against self-incrimination.

(c) Record of and access to seized data (Section 14)

27. The Group considered the practical application of this provision at length. The intent of the provision was primarily to ensure that the police keep a proper record of the items seized in the search and that the record is provided to the occupant or person in control of the computer system on a timely basis. The language of the draft was amended to make this clear. In addition, in those instances where the police decide to remove or render computer data inaccessible or physically seize a computer system, provision needs to be made for the occupant to request and obtain copies of the seized material, particularly where the records relate to an ongoing business or enterprise. At the same time, it was recognized that there would be instances where it would not be appropriate to give copies or access because of possible prejudice to an investigation or proceeding or where possession of the seized material would itself constitute an offence e.g. child pornography. The provision recommended by the Group is intended to achieve a balance between these interests.

(d) Production order power (Section 15)

28. As recommended in the original report, the model law contains a production order power that can be used as an alternative to a search warrant. The target group for such orders would be third parties unrelated to the suspects in the investigation, where there is no risk that the information or data sought will be destroyed. Under this power, the court will issue an order requiring a person to produce specified computer data within a set time period.

29. While the Group was unanimous as to the importance and usefulness of such a power, there was division as to the threshold to be met for the order to issue. For some countries, because the material to be produced may carry the same expectation of privacy as material seized by search warrant, the view was that the same standard and procedure should apply to both processes. However it was recognized that for other countries, because the production power is less intrusive in that the police do not enter and search the premises for the material, it is viewed as more analogous to a subpoena power than a search warrant. Those countries

would apply a lesser threshold for the order and a simplified process. The model law reflects this latter position. However, each country will need to carefully consider its constitutional and other requirements relating to search and seizure in order to determine what standard and process should be applicable to production orders.

(e) General

30. The Group discussed whether the model law should contain general provisions on penalties for obstruction during the course of a search or failure to comply with a court order. It was concluded that no specific provisions would be necessary as the laws of general application on these issues would be equally applicable to searches conducted or court orders issued under this statute. Countries would need to ensure that any necessary consequential amendments were made to apply such general provisions.

IV RECOMMENDATIONS REGARDING MUTUAL ASSISTANCE

31. The expert group reiterated their concern about the absence of effective provisions in the Harare scheme to deal with requests for assistance relating to computer data. In particular they noted that the absence of provisions for preservation orders, disclosure of traffic data, and assistance with collection of real time data makes the scheme of limited use in cases where computer data evidence is sought. The resulting problems are likely only to increase as more cases arise where such evidence is required.

32. The expert group recognized that Senior Officials did not recommend the inclusion of any such provisions into the Harare Scheme at their November meeting. It was noted however that given the postponement of consideration of the model law, there may not have been a sufficient opportunity to consider the specific recommendations for the Harare scheme in the area of computer evidence, within the context of the general recommendations of the expert group and the draft model law.

33. The expert group recommended that Senior Officials reconsider all of the recommendations on Mutual Assistance set out in the original report of the Expert Group and in particular those relating to amendments to the Harare Scheme, when considering the revised draft model law. A copy of the recommendations on mutual assistance from the original report of the expert group is attached as *Annex II. Annex III* to the Report contains excerpts from the Harare Scheme, with proposed revisions that reflect the expert group recommendations highlighted in bold in the text.

V ISSUES REFERRED TO E-COMMERCE GROUP

34. In the course of their discussions, the Group identified two issues which they felt the expert group on E-commerce should consider. First they noted that the term “data” was used in the definitions relating to E-commerce but the content of the definition was substantially the same as the term “computer data” in the computer crime context. For the reasons outlined in Part III, section 2 above could the term “computer data” be used in the e-commerce model law as well to make it consistent in both models?

35. Secondly, the Group noted the inconsistency between the definition of "information" in the E-commerce model law and the definition of document in the evidence model law. Given that the evidence model has been referred by Senior Officials to Law Ministers already, the Group suggested that consideration be given to amending the definition in the E-commerce model to make it consistent with the evidence model.

VI CONCLUSION

36. The Expert Group recommended that the revised model law and proposed amendments to the Harare Scheme be referred to Senior Officials.

37. The Commonwealth Secretariat expressed its thanks to the members of the expert group for their participation and to the Government of Canada for their generous support in sponsoring the reconvening of the expert group.

ANNEX I

2ND MEETING EXPERT GROUP ON COMPUTER AND COMPUTER RELATED CRIME
Marlborough House, London, 5-7 March 2002

CANADA

Ms Lucie Angers
Department of Justice
Room 5021 East Memorial Building
284 Wellington Street
Ottawa, Ontario K1A 0H8

Tel: 00 1 613 957 4750
Fax: 00 1 613 957 6374
Email: langers@justice.gc.ca

Mr Normand Wong
Department of Justice
(as above)

Tel: 00 1 613 941 4321
Fax: 00 1 613 957 6374
Email: nwong@justice.gc.ca

DOMINICA

Mr Gene Pestaina
Attorney-at-law
Chambers
3 Victoria Street
Roseau

Tel: 00 1 767 448 8687
Fax: 00 1 767 440 0076
Email: genep@cwdon.dm and and
genep@hotmail.com

MALAYSIA

Mr Shamsul Sulaiman
Senior Assistant Parliamentary Draftsman
Drafting Division
Attorney General's Chambers Malaysia
Level 5, Block C3
Federal Government Administrative Centre
62502 Putrajaya

Tel: 00 60 3 8885 5229
Fax: 00 60 3 8888 9373
Email: shamss@maxis.net.my and
shamsul@jpn.jpm.my

SOUTH AFRICA

Mr Enver Daniels
Chief State Law Adviser
Justice and Constitutional Development
Department
18th Floor, Cartwright's Corner House
Cnr of Adderley and Darling Streets
Cape Town

Tel: 00 27 21 469 9060
Fax: 00 27 21 461 8630
Email: DanielsE@justice.gov.za

UNITED KINGDOM

Ms Georgina Harrisson
Home Office
50 Queen Anne's Gate
London SW1H 9AT

Tel: 00 44 207273
Fax: 00 44 207273
Email:
georgina.harrisson@homeoffice.gsi.gov.uk

COMMONWEALTH SECRETARIAT

Ms Kimberly Prost
Deputy Director of Legal & Constitutional
Affairs Division

Tel: 44 (0)20 7747 6420
Fax: 44 (0)20 7839 3302
Email: k.prost@commonwealth.int

ANNEX II

RECOMMENDATIONS OF EXPERT GROUP ON COMPUTER AND COMPUTER RELATED CRIME REGARDING MUTUAL ASSISTANCE

1. The Harare Scheme on Mutual Assistance in Criminal Matters should permit requests between states for the preservation of specified stored computer data, in particular, but not limited to, traffic data.

2. The requirements for the content of a request for a preservation order should be less then those required for general mutual assistance, with the most essential points being:

(a) the authority seeking preservation;
(b) a brief description of the conduct under investigation;
(c) a description of the stored data to be preserved and its relationship to the investigation;
(d) a statement that the Country intends to submit a request for mutual assistance for the search or access, seizure or similar securing or disclosure of the data.

3. There should be a provision that any preservation effected in response to a request shall be for a period of not less than 40 days in order to enable the requesting Country to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request the data shall continue to be preserved pending a decision on the request.

4. The grounds of refusal applicable should be as minimal as possible, perhaps limited solely to prejudice to sovereignty, security, order public or essential interest.

5. Consideration should be given to whether an amendment is required to reflect the principle that if the requested Country considers that the preservation order will not ensure the future availability of the data or will threaten the confidentiality of, or other wise prejudice the requesting Country's investigation, it shall promptly inform the requesting Country, which shall then determine whether the request should nevertheless be executed.

6. There should be no requirement for dual criminality in relation to such requests. Countries that require dual criminality for mutual assistance requests should consider removing the requirement, at the very least for requests for preservation orders. Countries that may on a discretionary basis decline requests on the basis of an absence of dual criminality, as provided for in the Harare scheme, should not do so in the case of requests for preservation orders. As the Harare scheme does not require dual criminality as a prerequisite to mutual assistance, no amendment is necessary in that regard. However, as noted in 3 above, an amendment may be necessary to clarify that, inter alia, the dual criminality ground of refusal does not apply in the case of requests for preservation orders.

ANNEX III

EXCERPTS FROM THE HARARE SCHEME ON MUTUAL ASSISTANCE IN CRIMINAL MATTERS WITH PROPOSED REVISIONS ARISING FROM EXPERT GROUP RECOMMENDATIONS

1. (1) The purpose of this Scheme is to increase the level and scope of assistance rendered between Commonwealth Governments in criminal matters. It augments, and in no way derogates from existing forms of co-operation, both formal and informal; nor does it preclude the development of enhanced arrangements in other fora.

(2) This Scheme provides for the giving of assistance by the competent authorities of one country (the requested country) in respect of criminal matters arising in another country (the requesting country).

(3) Assistance in criminal matters under this Scheme includes assistance in

(a) identifying and locating persons;
(b) serving documents;
(c) examining witnesses;
(d) search and seizure;
(e) obtaining evidence;
(f) facilitating the personal appearance of witnesses;
(g) effecting a temporary transfer of persons in custody to appear as a witness;
(h) obtaining production of judicial or official records; and
(i) tracing, seizing and confiscating the proceeds or instrumentalities of crime.
(j) preserving data stored by means of a computer system on an interim basis;

CONTENTS OF REQUEST FOR ASSISTANCE

13. (1) **Except in the case of a request for preservation of computer data under 1(3)(j), a** request under the Scheme shall:

(a) specify the nature of the assistance requested;
(b) contain the information appropriate to the assistance sought as specified in the following provisions of this Scheme;
(c) indicate any time-limit within which compliance with the request is desired, stating reasons;
(d) contain the following information:
  (i) the identity of the agency or authority initiating the request;
  (ii) the nature of the criminal matter; and
  (iii) whether or not criminal proceedings have been instituted.
(e) where criminal proceedings have been instituted, contain the following information:
  (i) the court exercising jurisdiction in the proceedings;
  (ii) the identify of the accused person;
  (iii) the offences of which he stands accused, and a summary of the facts;
  (iv) the stage reached in the proceedings; and

(v) any date fixed for further stages in the proceedings.

(f) where criminal proceedings have not been instituted, state the offence which the Central Authority of the requesting country has reasonable cause to believe to have been committed, with a summary of known facts.

(2) A request shall normally be in writing, and if made orally in the case of urgency, shall be confirmed in writing forthwith.

PRESERVATION OF STORED COMPUTER DATA

28bis (1) A request under this Scheme may seek assistance in preserving specified stored computer data of any form, pending the submission of a request for the production of the data.

(2) "Computer data" includes 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.

(3) The request shall specify:

(a) the authority seeking preservation;

(b) a brief description of the conduct under investigation;

(c) a description of the data to be preserved and its relationship to the investigation or prosecution;

(d) a statement that the requesting country intends to submit a request for mutual assistance for the production of the data.

(4) Preservation granted in response to a request under (1) above shall be for a period of forty (40) days, in order to enable the requesting Party to submit a request for the production of the data. Following the receipt of such request, the data shall continued to be preserved pending a decision on that request and, if the request is granted, until the data is disclosed or seized for production.

(5) If the requested country considers that the preservation order will not ensure the future availability of the data or will threaten the confidentiality of, or other wise prejudice the requesting country's investigation, it shall promptly inform the requesting country, which shall then determine whether the request should nevertheless be executed.

(6) Notwithstanding Clause 7, a request for assistance under this Clause may be refused only to the extent that it appears to the Central Authority of the requested country that compliance would be contrary to the Constitution of that country, or would prejudice the security, international relations or other essential public interests of that country.

ANNEX B

COMPUTER AND COMPUTER RELATED CRIMES BILL

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	Child pornography

PART III

PROCEDURAL POWERS

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

ANNEX B

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]; 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

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; 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

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; 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.

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 (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 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.

[EXPERT GROUP TEXT OF PARAGRAPH (3)

(3) A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess 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 unless the contrary is proven.]

[ALTERNATE TEXT OF PARAGRAPH 3 PROPOSED BY CANADA

(3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (i) or (ii), a court may 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, unless the person raises a reasonable doubt as to its purpose.]

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; 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 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; 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

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 bold and italics.

11. In this Part:

"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

"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

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; 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 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; 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

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 communic - ations

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.

Confidentialit y 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; 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) 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.