



Osgoode Hall Law School of York University
Osgoode Digital Commons

Librarian Publications & Presentations


Law Library

2008

Cyberlaws and Cybercafés: Analysis of Operational Legislation in Some Commonwealth Jurisdictions and the United States

Yemisi Dina

Follow this and additional works at: <https://digitalcommons.osgoode.yorku.ca/librarians>

 Part of the [Law Commons](#), and the [Law Librarianship Commons](#)

Section III
**Cybercafés, Cyber Laws, and
 Control of Cyber Crime**

Chapter XIV
**Cyber Laws and Cybercafés:
 Analysis of Operational Legislation in
 some Commonwealth Jurisdictions
 and the United States**

Yemisi Dina
York University, Canada

ABSTRACT

This chapter will discuss the existing cyber laws in some commonwealth countries and the United States. It compares the various definitions accorded to cyber crimes in these countries. It examines and discusses when cyber crime occurs in the various jurisdictions regardless of where it originates, the laws that apply to pornography, the significance of jurisdiction for Internet criminals in all these countries, as well as when cybercafé operators are liable in cyber related crimes.

INTRODUCTION

Current developments in emerging technologies especially with the intensive consumption and distribution of information on the Internet have generated the introduction of cyber relation legislation in many parts of the world. This chapter highlights laws and treaties addressing computer related crimes in some developing and developed countries of the world, namely: Australia, Canada, India, Nigeria, Singapore, Trinidad & Tobago, the

United Kingdom, the United States, as well as the Council of Europe convention on cyber crime.

The *Internet* has been compared to an "Atlantis like continent that has arisen from the sea, been promptly populated and now needs sufficient order to ensure that its inhabitants do not hurt one another (or the people in other continents) so much." Technology through the *Internet* has created opportunities with advantages and disadvantages universally. In the last 20 years nations of the world have had to address the legal issues

especially crime related arising from the emergence of the *Internet* through *legislation*. Prior to this, courts have had to interpret laws relating to physical property whenever there is a technologically related crime. Various government departments have been established in developed countries especially the United States and the United Kingdom to assist in enforcing the various legislation. For example, there is the Internet crime complaint center which deals exclusively with criminal matters related to the Internet, while in the United Kingdom there is the computer crime unit under the Metropolitan Police which deals with offences committed under the Computer Misuse Act, 1990. This chapter identifies the laws applicable to cyber crime in a selected number of jurisdictions and the impact of these laws on cybercafé operators.

Today the *Internet* is no longer the network of computers linked together by the scientists from ARPANET, but a string of computers in different parts of the world at different time zones for various activities. It has therefore become necessary to regulate all activities taking place in *cyberspace*. And in regulating, this new technology has complicated many issues.

This chapter will discuss the existing laws in the listed *jurisdictions*. It will compare the various definitions accorded to *cyber crimes* in these countries. Some of the questions to be examined and discussed will include the following:

1. When does cyber crime occur in the various *jurisdictions* regardless of where the site is being accessed?
2. What laws apply to pornography?
3. What is the significance of *jurisdiction* for *Internet* criminals in all these countries? Can they be extradited to other jurisdictions?
4. When are cybercafé operators liable in cyber related crimes?

BACKGROUND

Computer crimes or *cyber crimes* have been variously defined; it is a criminal activity that uses the computer, its applications or data and its technology for various activities. The Black's law dictionary at page 399 defines computer crimes as "a crime involving the use of a computer such as sabotaging or stealing electronically stored data." Takach (2006), in defining computer crimes says it "involves some form of unauthorized gain, destruction, manipulation, or intrusion, or some form of illegal image or speech."

Activities of *cyber crime* include credit card fraud, pornography, *cyberspying*, *cyberstalking*, *spamming*, *hate crimes*, *solicitation*, *cyberpiracy*, money laundering, and bribery. And since the September 11, 2001 attacks in the United States, international terrorism facilitated by the use of computers has been added to the list of computer crimes. All these activities involve using the computer and the Internet to facilitate an illegal activity.

In spite of the fact that it is a criminal activity, a lot of jurisdictions have been faced with challenges in resolving litigation arising in this context because of the nature of the activities surrounding *cyber crimes*. Challenges are such as identifying the origin of the crime, location of the offender, applicable laws to be applied in trying the offender, among others. The courts and law enforcement agencies will also have to prove beyond reasonable doubt that the activities were against the law as well as provide sufficient evidence to prove their case. Over the years, providing sufficient evidence has been a challenge in so many jurisdictions and as a result many of the criminals have been acquitted for lack of evidence.

Takach (2006) identified four dynamics facing authorities in combating computer crimes as "the rapid technological changes and the law's response to it; the elusive nature of information; increasing fusion of the public and private spheres

in computer matters and blurring in computer law of the dividing line that has traditionally separated that which is national and that which is international" While many countries have laws against cyber crimes, some developing countries are yet to incorporate these crimes in their laws thus making the process of enforcing these statutes highly problematic and frustrating.

Another problem with cyber crimes has to do with identifying and locating the criminals since the *Internet* can be accessed from anywhere. Katsh (1995) was of the opinion that "...because new levels of informational interactions emerge that may not have existed before that legal questions touching on the use of space, such as jurisdiction, become more complicated." The question of jurisdiction has also been a problem in many instances. In other words, whose court or laws will prevail when an offender is eventually identified? For example, in the United States it becomes a problem since each state has its own law and therefore the enforcement ends at the geographic boundary of that state. Several suggestions have been made by jurists calling for a more global approach to address jurisdiction issues in order to allow government agents prosecute cyber criminals since they are located all over the world.

There is yet to be an internationally acceptable treaty addressing cyber crime with the exception of the Convention on Cybercrime of the Council of Europe which came into force on November 23, 2001. This convention is an "international cooperation to facilitate the detection, investigation and prosecution of criminal offences at both the domestic and international levels." To date, the Convention on Cybercrime has been ratified by 18 member states and one non-member state—the United States.

Some cyber crimes are committed mostly in cybercafés and this occurs mostly in developing countries where there is limited access to computers. A cybercafé is a commercial premises or operation which allows people to use computers with Internet access for a fee. It is of utmost

importance for the operators of such facilities to understand the impact of this crime on their businesses since such are mostly in existence strictly for financial gains. The following laws have been identified as in force in 2007, law being an ever changing institution means that new developments necessitates amendments to these laws.

CYBER CRIME LEGISLATION

The following is an outline of relevant sections of the law relating to computer crimes in the following countries: Australia, Canada, India, Nigeria, Singapore, Trinidad and Tobago, and the United Kingdom. Certain sections of the Council of Europe Convention on cyber crime are also included. In a number of jurisdictions there is a problem with the reliability of computer misuse evidence, for example, there has to be continued proof of access from a hacker's computer to the victim's. The location of a criminal is also a challenge since the Internet has no borders; the activities of a hacker can spread across continents and cause a lot of havoc, the question of which country's laws applies always raises a challenge.

Australia

Legislation against computer crimes can be found in the Cybercrime Act, 2001. Section 1 of the act defines a computer crime as follows:

computer-related act, event, circumstance, or result means an act, event, circumstance, or result involving:

- a. *the reliability, security, or operation of a computer; or*
- b. *access to, or modification of, data held in a computer or on a data storage device; or*
- c. *electronic communication to or from a computer; or*

- d. the reliability, security, or operation of any data held in or on a computer, computer disk, credit card, or other data storage device; or
- e. possession or control of data held in a computer or on a data storage device; or
- f. producing, supplying, or obtaining data held in a computer or on a data storage device.

Canada

Computer crimes legislation is found in Section 342(1) of the Criminal Code of Canada.

342.1 (1) Every one who, fraudulently and without colour of right;

- a. obtains, directly or indirectly, any computer service;
- b. by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;
- c. uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system; or
- d. uses, possesses, traffics in, or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b), or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding 10 years, or is guilty of an offence punishable on summary conviction.

Convention on Cybercrime <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

Budapest, 23.XI.2001
Preamble

The member States of the Council of Europe and the other States signatory hereto, considering that the aim of the Council of Europe is to achieve a greater unity between its members; recognising the value of fostering co-operation with the other states parties to this convention; convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against *cyber crime*, *inter alia*, by adopting appropriate legislation and fostering international co-operation; conscious of the profound changes brought about by the digitalisation, convergence, and continuing globalisation of computer networks; concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; recognising the need for co-operation between states and private industry in combating *cyber crime* and the need to protect legitimate interests in the use and development of information technologies; believing that an effective fight against *cyber crime* requires increased, rapid, and well-functioning international co-operation in criminal matters; convinced that the present convention is necessary to deter action directed against the confidentiality, integrity, and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation, and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation; mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil

and Political Rights, and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy; mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to automatic processing of personal data; considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention; taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member states and other states, and stressing that the present convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence; welcoming recent developments which further advance international understanding and co-operation in combating *cyber crime*, including action taken by the United Nations, the OECD, the European Union and the G8; recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning

the definition of certain computer crimes, and No. R (95) 13 concerning problems of criminal procedural law connected with information technology; having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 10-11, 1997), which recommended that the Committee of Ministers support the work on *cyber crime* carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, June 9-10, 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of states to become parties to the convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against *cyber crime*; having also regard to the Action Plan adopted by the heads of state and government of the Council of Europe on the occasion of their Second Summit (Strasbourg, October 10-11, 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe; have agreed as follows:

Chapter I—Use of terms

Article 1—Definitions

For the purposes of this Convention:

- a. “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- b. “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;

- c. "service provider" means:
 - i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
 - ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.
- d. "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II—Measures to be taken at the national level

Section 1—Substantive criminal law

Title 1—Offences against the confidentiality, integrity, and availability of computer data and systems

Article 2—Illegal access

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3—Illegal interception

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public

transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4—Data interference

1. Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration, or suppression of computer data without right.
2. A party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5—System interference

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.

Article 6—Misuse of devices

1. Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
 - a. the production, sale, procurement for use, import, distribution, or otherwise making available of:
 - i. a device, including a computer program, designed or adapted

primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

- 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 intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
 - b. the possession of an item referred to in paragraphs a.i or ii e, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A party may require by law that a number of such items be possessed before criminal liability attaches.
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution, or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this convention, such as for the authorised testing or protection of a computer system.
 3. Each party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution, or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2—Computer-related offences

Article 7—Computer-related forgery

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the

input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8—Computer-related fraud

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- a. any input, alteration, deletion, or suppression of computer data,
- b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3—Content-related offences

Article 9—Offences related to child pornography

1. Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - a. producing child pornography for the purpose of its distribution through a computer system;
 - b. offering or making available child pornography through a computer system;
 - c. distributing or transmitting child pornography through a computer system;

- d. procuring child pornography through a computer system for oneself or for another person;
 - e. possessing child pornography in a computer system or on a computer-data storage medium.
2. For the purpose of paragraph 1, the term "child pornography" shall include pornographic material that visually depicts:
 - a. a minor engaged in sexually explicit conduct;
 - b. a person appearing to be a minor engaged in sexually explicit conduct;
 - c. realistic images representing a minor engaged in sexually explicit conduct.
 3. For the purpose of paragraph 2e, the term "minor" shall include all persons under 18 years of age. A party may, however, require a lower age-limit, which shall be not less than 16 years.
 4. Each party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

India

India's legislation can be found in the Information Technology Act No. 21 of 2000, Sections 65, 66 and 67.

65. Tampering with computer source documents—Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system, or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to 3 years, or with fine which may extend up to two lakh rupees, or with both.

Explanation—For the purposes of this section, "computer source code" means the listing

of programmes, computer commands, design and layout, and programme analysis of computer resource in any form.

66. Hacking with computer system—(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. (2) Whoever commits hacking shall be punished with imprisonment up to 3 years, or with fine which may extend up to two lakh rupees, or with both.

67. Publishing of information which is obscene in electronic form—Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see, or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to 5 years and with fine which may extend to one lakh rupees, and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to 10 years and also with fine which may extend to two lakh rupees.

Nigeria

Cyber crime legislation in Nigeria is incorporated in the Advance Fee Fraud and other Fraud Related Offences Act, 2006. The legislation does not address cyber crime per se as in other jurisdictions where there are separate laws. The provision of this legislation is just a penalty or requirement for operators of cybercafés and not cyber crime offenders.

Electronic telecommunication offences, and so forth.

12. (1) Any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form shall be required to obtain from the customer or subscriber:

- a. full names
 - b. residential address, in the case of an individual
 - c. corporate address, in the case of corporate bodies
2. Any customer or subscriber who:
 - a. fails to furnish the information specified in subsection (1) of this section; or
 - b. with the intent to deceive, supplies false information or conceals or disguises the information required under this section, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or a fine of ₦ 100,000.
 3. Any person or entity providing the electronic communication service or remote computing service either by e-mail or any other form, who fails to comply with the provisions of subsection (1) of this section, commits an offence and is liable on conviction to a fine of ₦ 100,000 and forfeiture of the equipment or facility used in providing the service.

13. (1) Notwithstanding the provisions of the Nigerian Communications Commission Act, 2003 or the provisions of any other law or enactment, any person or entity who in the normal course of business provides telecommunications or Internet services or is the owner or person in the management of any premises being used as a telephone or internet cafe or by whatever name called shall:

- a. be registered with the Economic and Financial Crimes Commission (in this Act referred to as "the Commission");
- b. maintain a register of all fixed line customers which shall be liable to inspection by any authorized officer of the commission; and

submit returns to the commission on demand on the use of its facilities.

(2) Any person whose normal course of business involves the provision of non-fixed line or global system of mobile communications (GSM) or is in the management of any such services, shall submit on demand to the commission such data and information as are necessary or expedient for giving full effect to the performance of the functions of the commission under this Act.

(3) Any person specified under subsection (1) and (2) of this section shall exercise the duty of care to ensure that his services and facilities are not utilized for unlawful activities.

(4) It shall be a valid defence for any provider of wire or electronic communication service, its officers, employees, or agents or other specified persons for providing information or facilities to the commission in any cause, matter or suit that the said provider, its officers, employees, or agents or any other specified persons acted in compliance with the obligations imposed under this Act.

(5) Any person or entity who by virtue of subsections (1) and (2) of this section knows or ought to know that he should:

- a. be registered with the commission, or
- b. furnish the commission on demand, with the returns on the use of his service and facilities, or
- c. facilitate access to data and information by authorized employees or staff of the commission, and fail to do so with intent to conceal or disguise the nature of his activities or the use of his services and facilities, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years without an option of fine and in the case of a continuing offence, a fine of ₦50,000 for each day the offence persists.

(6) Any person or entity convicted more than once under this Act shall have his operational license revoked or cancelled.

Singapore

The *cyber crime* law for Singapore is as stated in the Computer Misuse Act, 2003 (CHAPTER 50A).

Unauthorised access to computer material
3. (1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at:

- a. any particular program or data;
- b. a program or data of any kind; or
- c. a program or data held in any particular computer.

Access with intent to commit or facilitate commission of offence
4. (1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

(2) This section shall apply to an offence involving property, fraud, dishonesty, or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 10 years or to both.

(4) For the purposes of this section, it is immaterial whether:

- a. the access referred to in subsection (1) is authorised or unauthorised;
- b. the offence to which this section applies is committed at the same time when the access is secured or at any other time.

Unauthorised modification of computer material

5. (1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at:

- a. any particular program or data;
- b. a program or data of any kind; or
- c. a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

Unauthorised use or interception of computer service
6. (1) Subject to subsection (2), any person who knowingly:

- a. secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;
- b. intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical, or other device; or
- c. uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at:

- a. any particular program or data;
- b. a program or data of any kind; or
- c. a program or data held in any particular computer.

Unauthorised obstruction of use of computer

7. (1) Any person who, knowingly and without authority or lawful excuse:

- a. interferes with, or interrupts, or obstructs the lawful use of a computer; or
- b. impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, shall be guilty of an offence and shall be liable on

conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

Unauthorised disclosure of access code
8. (1) Any person who, knowingly and without authority, discloses any password, access code, or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so:

- a. for any wrongful gain;
- b. for any unlawful purpose; or
- c. knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

Trinidad & Tobago

The legislation for computer related offences for this jurisdiction can be found in The Computer Misuse Act, 2000

3. (1) Subject to subsection (2), a person who knowingly and without authority causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer commits an offence and is liable on summary conviction to

a fine of fifteen thousand dollars and to imprisonment for 2 years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for 4 years.

(2) If any damage is caused as a result of an offence committed under subsection (1), the person convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for 3 years.

(3) For the purpose of this section, it is not material that the act in question is not directed at:

- a. any particular program or data;
- b. a program or data of any kind; or
- c. a program or data held in any particular computer.

(4) For the purpose of this section, a person secures or gains access to any program or data held in a computer if by causing the computer to perform any function he:

- a. alters or erases the program or data;
- b. copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
- c. uses it; or
- d. causes it to be output from the computer in which it is held, whether by having it displayed or in any other manner, and references to access to a program or data and to an intent to secure such access shall be read accordingly.

(5) For the purpose of subsection (4)(c), a person uses a program if the function he causes the computer to perform:

- a. causes the program to be executed; or
- b. is itself a function of the program.

(6) For the purpose of subsection (4)(d), the form in which any program or data is output,

and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer, is immaterial.

4. (1) A person who knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer with intent to commit an offence:

- a. involving property, fraud, dishonesty, or which causes bodily harm; and
- b. which is punishable on conviction by imprisonment for more than 1 year, commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for 2 years.

(2) For the purpose of this section, it is immaterial whether:

- a. the access referred to in subsection (1) is authorised or unauthorised;
- b. the offence to which this section applies is:
 - i. committed at the same time when the access is secured or at any other time; and
 - ii. punishable summarily or indictably.

5. (1) Subject to subsection (2), a person who does a direct or an indirect act without authority which he knows will cause an unauthorised modification of any program or data held in any computer commits an offence and is liable on summary conviction to a fine of fifteen thousand dollars and to imprisonment for 2 years and, in the case of a second or subsequent conviction, to a fine of thirty thousand dollars and to imprisonment for 4 years.

(2) If any damage is caused as a result of an offence committed under subsection (1), the per-

son convicted of the offence shall be liable to an additional fine of twenty thousand dollars and to imprisonment for 3 years.

(3) For the purpose of this section:

- a. it is immaterial that the act in question is not directed at—
 - i. any particular program or data;
 - ii. a program or data of any kind; or
 - iii. a program or data held in any particular computer;
- b. it is immaterial whether an unauthorised modification is, or is intended to be permanent or merely temporary;
- c. a modification of any program or data held in any computer takes place if, by the operation of any function of the computer concerned or any other computer:
 - i. any program or data held in any computer is altered or erased;
 - ii. any program or data is added to or removed from any program or data held in any computer.

United Kingdom

The legislation for the United Kingdom is found in the Computer Misuse Act, 1990.

Unauthorised access to computer material.

1. (1) A person is guilty of an offence if:

- a. he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
- b. the access he intends to secure is unauthorised; and
- c. he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at:

- a. any particular program or data;
- b. a program or data of any particular kind; or
- c. a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both. Unauthorised access with intent to commit or facilitate commission of further offences.

2. (1) A person is guilty of an offence under this section if he commits an offence under section 1 ("the unauthorised access offence") with intent:

- a. to commit an offence to which this section applies; or
- b. to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences:

- a. for which the sentence is fixed by law; or
- b. for which a person of 21 years of age or over (not previously convicted) may be sentenced to imprisonment for a term of 5 years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act, 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable:

- a. on summary conviction, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum or to both; and
- b. on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine or to both.

Unauthorised modification of computer material.

3. (1) A person is guilty of an offence if:

- a. he does any act which causes an unauthorised modification of the contents of any computer; and
- b. at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) the requisite intent is an intent to cause a modification of the contents of any computer and by so doing:

- a. to impair the operation of any computer;
- b. to prevent or hinder access to any program or data held in any computer; or
- c. to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at:

- a. any particular computer;
- b. any particular program or data or a program or data of any particular kind; or
- c. any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act, 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable:

- a. on summary conviction, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum or to both; and
- b. on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine or to both.

United States

In the United States there are several laws addressing cyber crimes. I have identified the following Federal laws; individual states also have their own laws:

1. Computer Fraud and Abuse Act, 1986. The provisions of this act makes it an offence to use the computer of any of its devices to defraud, receive payment, extort, access passwords without authorization among others.
2. Child Online Protection Act, 1998 (COPA). This Act makes it a criminal offence and also limits commercial websites from distributing materials that are harmful to minors. 'Material that is harmful' is defined as "any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene....."

3. Child Pornography Prevention Act, 1996 (CPPA). This Act makes it a criminal offense for anyone to possess, produce, or distribute child pornography. Child pornography as defined by this law makes the possession or production of computer-generated images unlawful, including "morphed" and computer-generated images that only appear to depict minors engaged in sexually explicit conduct.
4. Digital Millennium Copyright Act, 2000 (DMCA). This Act makes it an offense for anyone to use computers and any technological devices to infringe against copyrights of traditional works. It however, limits for research purposes the liability of non-profit libraries, archives and educational institutions for copyright infringements when they serve as service providers.
5. The Patriot Act, 2001. This is an act "To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes." It has been severally criticized by librarian and information professionals and human rights advocates as it gives a lot of authority to law enforcement agencies in producing evidence against a criminal especially in terrorist matters. One of the strengths of Patriot Act is that it has "updated" the law to modern technology. Law enforcement agencies in the U.S. are able to protect victims of hacking against digital trespassers as if it were physical.

All of the jurisdictions mentioned in this chapter except Canada and Nigeria have computer specific laws to address computer crimes. None of the jurisdictions have addressed prosecuting cyber criminals who are located outside of their jurisdictions and this has been a major challenge for law enforcement agencies. Only the U.S. Patriot Act has been able to legislate successfully against cyber criminals by providing authority for law enforcement agents' high tech means.

While the majority of these offences are committed across international borders, none of these countries have been able to successfully prosecute cyber criminals across their borders. Between January 1, 2006–December 31, 2006, a total of 207, 492 complaints were filed online to the Internet Fraud Complaint Center in the USA. A ratification of the convention on cyber crime by all nations of the world will be highly effective in curbing this endemic crime as no country is left out.

When does a Crime Take Place?

The computer according to the listed legislation becomes the object, subject, and instrument of crime. Computer crime takes place when the following occurs:

- unauthorised access;
- unauthorised destruction;
- unauthorised manipulation;
- unauthorised intrusion; or
- detection of illegal images.

All these will involve someone hacking into someone's computer or data to gather information. An increase in ecommerce has perpetrated this kind of act with hackers intercepting credit card information and using it for criminal purposes. Unauthorised use of another person's password also constitutes unauthorised access.

Destroying, intruding, and manipulating will involve modifying, altering, and adding information on a computer. In this case an individual can hack into the financial or administrative records of an institution to perform such an operation. Viruses can also be used to erase and modify information which may cause system malfunctions.

Detection of illegal images and speech will involve someone trying to access pornographic images as well as communicating these images to children or minors. In the case of adults, such

an act becomes illegal when it is communicated without their consent.

Impact on Cybercafés

It is now possible for members of the law enforcement agents to detect the location of any computer that has accessed or linked the *Internet* and this enables them to find out the place where any crime is initiated by checking the *Internet protocol (IP)* address. Hence the need for authentication of access to public computers public places such as public libraries, academic libraries, and so forth, in many developed countries. It is crucial to be able trace access at anytime.

Cybercafé operators can be likened to Internet service providers (ISP) and so they need to take the necessary precautions. From all the legislation discussed, a cybercafé operator is liable once the illegal activity originates from their computers. Cybercafé operators must note that a crime is committed once it originates from their business computers; they will have to prove this by sharing details of all their clients with law enforcement agents. The operators of cybercafés must always ensure that they have actual/genuine records of persons accessing their machines in order to be able to track down criminals. This works in most developed countries. Provisions of the relevant legislation used in this study all state that it is irrelevant whether the crime originated from another jurisdiction. Once it has been detected, charges will be laid against the person. For example, a hacker based in Nigeria accessing computer files in Port of Spain, Trinidad will be charged as if the offence was committed in Port of Spain. It is also irrelevant whether the hacker is a citizen of that country or not.

CONCLUSION

Computer related crimes are like a plague that will continue to advance with technology and so

it is difficult for the legislators and law makers to meet up with controls against it.

This chapter has identified the laws related to cyber crimes stating the offences and punishment in a selected number of jurisdictions. *Cyber space* has no geographic and political boundaries so it is an opportunity for criminals all over the world. Computer crimes are advancing with technology needless mentioning the financial losses and so the law must meet up with all these challenges and advancement. Cybercafé operators will need to endlessly and continuously educate their customers of the consequences of cyber crimes by posting caveats on log on pages or sheets. They also need to post information on bulletin boards on their premises to create awareness that certain activities on the computer constitute an offence. Government through the law enforcement agencies and with cooperation from Departments of Justice can periodically organize empowerment seminars for operators of cybercafés to educate them about developments in cyber crimes and cyber laws.

FUTURE RESEARCH DIRECTIONS

Future research will involve a study concerning the role and activities of government agencies and departments responsible for managing, monitoring and controlling computer crimes in a selected number of jurisdictions. I will compare, where available, operational statistics (where provided) of these agencies in managing and controlling this crime.

REFERENCES

- Carter, A. J., IV., Perry, A. (2004). Computer crimes. *American Criminal Law Review*, 41, 313-363.
- Federal Bureau of Investigation IC3 Annual Report (2006). Retrieved December 23, 2006, from

http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf

Garner, B. (Ed.). (2004). *Blacks law dictionary*. St. Paul, MN: West.

Geist, M. Cyberlaw 2.0. *Boston College Law Review*, 44, 323-358.

Helewitz, J. A. (2005). *Cyberlaw: Legal principles of emerging technologies*. New Jersey: Pearson Education Inc.

Hoffer, S. (2003). *World cyberspace law*. New York: Juris Publishing.

Hughes, J. The Internet and the persistence of law. *Boston College Law Review*, 44, 359-396.

Katsh, M. E. (1995). Cybertime, cyberspace and cyberlaw. *Journal of Online Law*, 25. Retrieved November 1, 2006, from http://www.wm.edu/law/publications/jol/95_96/katsh.html

Skilbell, R. (2003). Cybercrimes and misdemeanors: A reevaluation of the computer fraud and abuse act. *Berkeley Technology Law Journal*, 18, 909-944.

Takach, G. S. (2006). *Computer law*. Toronto: Irwin Law Inc.

Weber, A. M. (2003). The council of Europe's convention on cybercrime. *Berkeley Technology Law Journal*, 18, 425-446.

Highlights of the USA Patriot Act. Retrieved December 23, 2006, from <http://www.lifeandliberty.gov/highlights.htm>

Convention

Council of Europe Convention on Cybercrime 2004 CETS No.: 185 signed 23/11/2001. Retrieved March 27, 2007, from <http://conventions.coe.int/Treaty/Commun/QueVoulez-Vous.asp?NT=185&CM=8&DF=3/24/2007&CL=ENG>

Table of Statutes

Cybercrime Act (2001). Retrieved September 6, 2006, from http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001112/

Criminal Code, R.S.C. s.342(1) (1985). Retrieved January 24, 2007, from <http://www.canlii.org>

Information Technology Act, India (2000). Retrieved March 19, 2007, from <http://www.manupatra.com.ezproxy.library.yorku.ca/asp/home.asp>

Advanced Fee Fraud and other Fraud Related Offences Act, Nigeria (2006). Retrieved December 5, 2006, from <http://www.nigerialaw.org/Advance%20Fee%20Fraud%20and%20other%20Fraud%20Related%20Offences%20Act%202006.htm>

Computer Misuse Act, Singapore (1993). Retrieved February 24, 2007, from <http://agcvldb4.agc.gov.sg/>

Computer Misuse Act, Trinidad & Tobago (2000). Retrieved November 6, 2006, from <http://www.ttparliament.org/bills/acts/2000/a2000-86.pdf>

Computer Misuse Act, United Kingdom (1990). Retrieved January 22, 2007, from, http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_2.htm#mdiv1

Computer Fraud and Abuse Act 18 U.S.C §1030 (2000).

Child Online Protection Act 47 U.S.C § 231 (1998).

Child Pornography Prevention Act U.S.C § 2252 (1999).

Digital Millennium Copyright Act 17 U.S.C § 1201-1205 (2000).

Patriot Act 31 USC §1956 (2001). Retrieved December 23, 2006, from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

ADDITIONAL READING

Bellia, P. L., Berman, P. S., & Post, D.G. (2003). *Cyberlaw: problems of policy and jurisprudence in the information age*. St Paul, MN: West.

Ferrera, G. R., Lichtenstein, S. D., Reder, M. E., Bird, R. C., & Schiano, W. T. (2004). *Cyberlaw: Texts and cases*. Mason, Ohio: West.

Koops, B-J. (2006). *Cybercrime and jurisdiction: a global survey*. West Nyack, NY: Cambridge University Press.