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