

## **Legislating Cybercrimes in Jamaica: Issues of Public and Corporate Liability**

### **Introduction**

This chapter will focus on the Jamaican Cybercrimes Act 2010 (the Act) which was passed into law on March 17, 2010. It regulates internet and computer crimes. The regulation of computer or internet and computer crimes has been slow to come to the Caribbean region<sup>1</sup> including Jamaica. By August of 2009 everyone felt that the Act was an imperative for Jamaica. Institutionally, the police were somewhat equipped to deal with cybercrimes and had by then set up the Cybercrimes Investigation and Research Unit (CIRU), but there was no legislative support for their investigations. This meant that crimes committed on or using computers or computer networks went unpunished. Those crimes included instances of corporate espionage. The instances of corporate espionage were found in the course of an unrelated investigation by the CIRU. The results of that discovery was that corporate entities were either engaging computer hackers or buying information from them which was stolen from competing businesses in order to gain market advantage.<sup>2</sup> In addition to this there was a proliferation of obscene publications whereby sexually explicit photographs were being maliciously circulated for example when relationships came to an end. At the same time, about December of 2009, one large telecommunications company was hit hard when a 26 year old computer science student hacked into its computer system and stole approximately \$10, 000, 000.00 in call credit. His lawyer when interviewed, asked which legislation his client going to be prosecuted under. All of this signalled that the time for the regulation of computer and cybercrimes was more than overdue.

---

<sup>1</sup> Trinidad & Tobago – Computer Misuse Act 2000, Computer Misuse Act 2005 – Barbados and Antigua & Barbuda – Computer Misuse Act 2006

<sup>2</sup> “Senate Passes Cybercrimes Bill”, Jamaica Observer Sunday the 20<sup>th</sup> December 2009  
<[www.jamaicaobserver.com](http://www.jamaicaobserver.com)> (date accessed: 15 August 2010)

Cyber is an internet related prefix that was allegedly popularised in the 1980's by William Gibson in his book *Neuromancer*. It is used to describe internet or computer equivalents of existing products, services or things such as crime. Advances in technology and moreover the development of the internet in the 1990's caused a migration of commerce into cyberspace. Historically, the development of commerce is accompanied by criminality in its various manifestations whereby persons attempt to rob or steal from legitimate businesses. In real space this is evidenced by breaking and entering to steal either products, goods, trade secrets or other information. Trade secrets were also stolen by industrial espionage where persons impersonated legitimate employment seekers and obtained employment with the sole intention of passing trade secrets onto the unsuspecting "employer's competitors. Cyberspace is no different in terms of the migration of crime as there is evidence that the criminals have moved their activities into that medium. Of course the same crimes have different names so that breaking and entering is a regular feature online. Breaking and entering a house or shop is either shop breaking and larceny or burglary, in the online or computer environment it is called hacking. The need for in-person contact to perpetrate these crimes diminished. Thieves break and enter online stores or systems but there was, in most Caribbean jurisdictions, no regulation for punishing hacking (breaking and entering) into the online store and stealing information, cash or identities. It was therefore long recognised worldwide that cybercrimes should be regulated and this led to the creation of model laws by the Council of Europe,<sup>3</sup> UNCITRAL<sup>4</sup> and the ITU.<sup>5</sup> This paved the way for countries worldwide to adapt the various model laws to their jurisdiction.

---

<sup>3</sup> One of the first organisations in Europe to seeking to integrate or harmonise cybercrime on that Continent - 2001 Budapest (26 European countries).

<sup>4</sup> United Nations Commission on International Trade Law

<sup>5</sup> International Telecommunications Union

Cybercrimes legislation is only one, albeit an important, aspect of the regulation of life in cyberspace.

### **The Cybercrimes Act 2010 – An Overview**

The Cybercrimes Act was passed into law three years after its civil rights and remedies counterpart, The Electronic Transaction Act (the ETA), was passed on the 2<sup>nd</sup> April 2007. The ETA created an environment in which persons could lawfully transact business in cyberspace and enforce those rights in the civil courts if necessary. There was no corresponding means of regulating illegality as it relates to crimes committed against those either participating in or facilitating those transactions until the Cybercrimes Act 2010 was passed. This Act did not define cybercrime. It appears that this was a good decision because it is difficult to craft a compendious definition for cybercrime. There are varying approaches to the issue of whether the term should be defined:

Most reports, guides or publications on cybercrime begin by defining the term “cybercrime”. One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity. One example for an international approach is Art. 1.1 of the Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (CISAC) that points out that cybercrime refers to acts in respect to cyber systems. Some definitions try to take the objectives or intentions into account and define cybercrime more precisely, defining cybercrime as “computer-mediated activities which are either *illegal or considered illicit* by certain parties and which can be conducted *through global electronic networks*”. These more refined descriptions exclude cases where physical hardware is used to commit regular crimes, but they risk excluding crimes that are considered as cybercrime in international agreements such as the “Convention on Cybercrime”. For example, a person who produces USB-devices containing malicious software that destroy data on computers when the device is connected commits a crime as defined by Art. 4 Council of Europe Convention on Cybercrime. However, the act of deleting data using a physical device to copy malicious code has not been committed through global electronic networks and would not qualify as cybercrime under the narrow definition above. This act would only qualify as cybercrime under a definition based on a broader description, including acts such as illegal data interference. This demonstrates that there are considerable difficulties in defining the term “cybercrime”. The term “cybercrime” is used to describe a range of offences including traditional computer crimes, as well as network crimes. As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the Stanford Draft Convention and the Convention on Cybercrime, whilst excluding traditional crimes that are just committed using hardware. The fact that there is

no single definition of “cybercrime” need not be important, as long as the term is not used as a legal term.<sup>6</sup>

The uncertainty or confusion suggested by this extract seems to cast some doubt on the decision not to define “cybercrime”. However, the definition of computer in the Act compensates for the seeming uncertainty or confusion caused by the absence of a definition of “cybercrime”. Computer is defined as:

*“any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and –*

*(a) includes any data storage facility or electronic communications system directly connected to or operating in conjunction with such device or group of such interconnected or related devices...”*<sup>7</sup>

This definition is wide enough to incorporate all known and it appears future forms of electronic means of access to computers, data, information or networks as well as non-traditional devices that would not ordinarily be considered computers. The critical qualifier in relation to these devices and non-traditional devices is that it has to be a device *“which pursuant to a programme performs the automatic processing of data.”* This definition focuses on the “function” or “purpose” of the physical device or media in or with which the activity must take place to constitute a crime within the meaning of the Cybercrimes Act. It is also of wide application because it expands the class of devices. The result is that the drafters were able to minimise or eliminate the weaknesses associated with defining “cybercrime” by reference to the tools, target or place of criminal activity. Part II of the Act is therefore sufficiently broad to cover a wide range of offences.

---

<sup>6</sup> International Telecommunications Union Cybercrime Legislation Resources, Understanding Cybercrime: A Guide for Developing Countries (Draft 2009) at Page 17 – Paragraph 2.1. [Underlining not in original]

<sup>7</sup> s. 2(1)(a)

This means that liability for prosecution under the Act can arise where any prohibited activity takes place on or using not only a desktop computer (PC) or a laptop but also on smart phones such as a blackberry, iPhone or Palm or even ipods which are used primarily for music. The key is that it must be working and capable of automatically processing data. The idea that the Act focuses on incorporating all known forms of devices or future devices is confirmed by its treatment of flash drives or other data storage facility. A flash drive or other data storage facility does not automatically fall within the definition of a “computer” for the purpose of committing a prohibited offence under the Act. This is because these are not ordinarily connected to a computer or perform “*automatic processing of data.*” However, in order to incorporate these devices the Act provides that “[a] reference in (the) Act to any “*any program or data held in a computer*” includes a reference to any program or data held in any removable data storage medium which is for the time being in the computer.”<sup>8</sup> Additional devices would include optical discs such as compact disc, digital versatile data (digital video disc) or blu ray “held” in a “computer”.

Further guidance as to the scope of the Act is provided by an examination of its objects. The object of the Cybercrime’s Act is to “[p]rovide criminal sanctions for the misuse of computer systems or data and the abuse of electronic means of completing transactions and to facilitate the investigation and prosecution of cybercrimes.” These objects, apart from the definition of “computer”, add further certainty to an understanding of the offences that are covered by the Act. The objects define the purpose of the Act by reference to three categories which cover the substantive and procedural regulation of cybercrimes. The first and second categories covers the substantive regulation of cybercrimes by criminalising certain acts that

---

<sup>8</sup> s. 2(5)

takes place on computers and networks as defined in the Act. The third category covers the procedural regulation of the same offences. The *first* category of crimes being regulated is associated with unauthorised access to program or data on a computer or on computer systems similar to breaking and entering or with inappropriate escalation of access to a program or data by those who have been authorised to use it. The latter would be persons who would have been granted access to programs or data on a computer with, one would hope restrictions on rights and privileges. On this interpretation mere access or use is not enough to constitute an offence under the Act. It has to be in the nature of unauthorised access and unauthorised escalation of access and privileges provided the requisite intention is present. The *second* category, the abuse of electronic means of completing transactions would cover offences relating to the interception of electronic transactions, communications or a denial of service attacks. An example of interception of a transaction would be one that involves *website defacement*. This occurs where a hacker changes the appearance of a legitimate website and then redirects the user to the hacker's server to complete a transaction instead of the legitimate website. The more recognisable form of interception would be the interception of communications without authorisation.<sup>9</sup> This would include "listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices...includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications."<sup>10</sup> A denial of service attack may occur when a code or virus is released and directed at the target system flooding it with requests or information thereby preventing legitimate users from having access to the system or eventually causing the target

---

<sup>9</sup> The Interception of Communications Act

<sup>10</sup> International Telecommunications Union, Understanding Cybercrime: A Guide for Developing Countries (Draft 2009); See also the Interception of Communications Act

system to crash. The *third* category covers the procedural framework by making specific provision for the gathering, collecting and preserving of the evidence for presentation in court.<sup>11</sup>

## Substantive Offences Regulation

There are six offences and these are set out in Part II of the Act. The offences are made up of different elements which have been defined in the Act and an important element in four of the offences is intention to access or modify without authority.

### The Offences

The offences that have an unauthorised act as an essential element relate to access, modification, interception or obstruction of a program or data and are as follows:

1. A person who knowingly obtains, for himself or another person, any unauthorised access to any program or data held in a computer commits an offence.<sup>12</sup>
2. A person who does any act which that person knows is likely to cause any unauthorised modification of the contents of any computer commits an offence.<sup>13</sup>
3. A person commits an offence if that person knowingly<sup>14</sup> –
  - a. secures unauthorised access to any computer for the purpose of obtaining, directly, or indirectly, any computer service; or
  - b. without authorisation, directly or indirectly intercepts or causes to be intercepted any function of a computer
4. A person commits an offence if that person, without authorisation or without lawful justification or excuse, wilfully causes, directly or indirectly<sup>15</sup> –

---

<sup>11</sup> Part III – s. 13 – s. 17 of the Cybercrimes Act

<sup>12</sup> s. 3(1) this offence is said to be subject to subsection 3(4). However, there is no subsection 4 under section 3.

<sup>13</sup> s. 5(1)

<sup>14</sup> s. 6(1)

<sup>15</sup> s. 7(1)

- a. A degradation, failure, interruption or obstruction of the operation of a computer; or
- b. A denial of access to, or impairment of, any program or data stored in a computer.

The other two offences do not require an unauthorised act. The first of the two is broad. It is also difficult to determine the scope of this section in terms of width. Section 4(1) of the Act makes it an offence for a person to “*access any program or data held in a computer with intent to – (a) commit any offence punishable by imprisonment for a term not exceeding one year; or (b) facilitate the commission of an offence referred to in paragraph (a), whether by himself or any other person...*” The offence under s. 4(1) is committed even if the facts “*are such that the commission of the offence referred to in subsection 1(a) are impossible.*” In other words, it is the intent that offends.<sup>16</sup> Examples of this include an offence under The Obscene Publications (Suppression of) Act<sup>17</sup> and the malicious publication of a defamatory libel (criminal libel).<sup>18</sup>

The second offence that does not require an unauthorised act is the offence created by s. 8 which makes it unlawful for a person, “*for the purpose of committing or facilitating the commission of an offence under any of sections 3 to 7*”, to possess, receive, manufacture, sell, import, distribute, disclose or otherwise make available “*(a) a computer; (b) any access code or password; or (c) any other data or device designed or adapted primarily for the purpose of committing an offence under any of sections 3 to 7.*” In this context, the mental element is intent to facilitate the committing a prohibited offence. It is immaterial whether any offence is actually committed under sections 3 to 7.. It is therefore important to recommend and encourage a

<sup>16</sup> Digital Evidence and Computer Crime (below) at Page 75

<sup>17</sup> s. 2

<sup>18</sup> s. 6 of the Libel and Slander Act

culture of certification because legitimate holders of computers, access codes or passwords that are capable of enabling the commission of an offence within the relevant sections will be put to proving their innocence by being made to show that they are not holding the prohibited items with the intent or purpose stipulated in the section 8.

The provisions in the Cybercrimes Act are similar to those in the *Computer Misuse Act 1990* (England). There are three offences that are readily identifiable as being similar to the ones under the Cybercrimes Act. These offences are *unauthorized access to a computer*, *authorised access with intent to commit or facilitate the commission of further offences*<sup>19</sup> and *unauthorised modification of computer material*.<sup>20</sup> Some of these provisions have been subject to judicial interpretation and are of some assistance in interpreting the provisions of the Cybercrimes Act.

### **Unauthorised Access as an Offence**<sup>21</sup>

In order to succeed, the prosecution must prove that the accused knew that he did not have authority to access the “program or data held in a computer”<sup>22</sup> “of the kind in question” and intended to access without that authority. The *actus reus* is, of course, the act of breaking into the computer, that is *causing it to perform a function that*:–<sup>23</sup>

- a. alters or erases the program or data;
- b. copies or moves the program or data to any storage medium other than that in which the program is held or to a different location in the storage medium in which the program or data is held;
- c. causes the program or data to be executed;
- d. is itself a function of the program or data; or

<sup>19</sup> Similar to s. 4 of the Cybercrimes Act except that s. 4 is more limited in scope to offences punishable by a term of imprisonment not exceeding one year...

<sup>20</sup> ss. 1, 2 and 3

<sup>21</sup> s. 3

<sup>22</sup> *Ibid*

<sup>23</sup> s. 2(2)

e. causes the program or data to be output from the computer in which it is held, whether by having the program or data displayed in any other manner,

and references to accessing, or an intent to obtain access to, a computer shall be construed accordingly.

On this definition, it can be seen that access is not by itself an offence. The access must be unauthorised. Offences relating to unauthorised access are defined by reference to persons who access, modify or use “*any program or data held in a computer to perform any function...*”<sup>24</sup> and who are not “*entitled to control access, modification, use or the function in question*” or “*he does not have the consent for access modification use of function of the kind in question from any person who is so entitled...*”<sup>25</sup> The equivalent provision in England’s Computer Misuse Act 1990, that is ss. 17(5) was considered and refined in the case of **R. v. Bow Street Magistrate**:<sup>26</sup>

The United States Government sought to the extradition of the accused from England. The allegation was that he had obtained account information from an employee of a charge card company, who was authorised to access its computer records solely for the purposes of her employment, and had used that information to encode forged credit cards and obtain fresh personal identification numbers so as to draw money from automatic teller machines.<sup>27</sup>

The issue was whether *unauthorised access* as defined in s. 17(5) the Computer Misuse Act<sup>28</sup> extended “*to a person who was authorised to control the computer in question but misused the information thereby obtained.*”<sup>29</sup> The case was appealed to the House of Lords on a certified question of law of general public importance. Their lordships found the question to be “unhappily drafted” but went on to consider it with a view to clearing up the confusion in the interpretation of s. 17(5) of the Act. The question was:

---

<sup>24</sup> s. 2(4)

<sup>25</sup> *ibid*

<sup>26</sup> R. v. Bow Street Metropolitan Stipendiary Magistrate and Another 2000 2 A. C. 216

<sup>27</sup> *ibid* (headnotes)

<sup>28</sup> s. 2(4) of the Cybercrimes Act

<sup>29</sup> *ibid*

Whether, on a true construction of section 1<sup>30</sup> (and thereafter s. 2)<sup>31</sup> of the Computer Misuse Act 1990, a person who has authority to access data of the kind in question none the less has unauthorised access if: (a) the access to the particular data in question was intentional; (b) the access in question was unauthorised by a person entitled to authorise access to that particular data; (c) knowing that the access to that particular data was unauthorised.<sup>32</sup>

Lord Hobhouse examined the relevant sections of the Computer Misuse Act and explained where the Divisional Court fell into error and clarified how unauthorised access was to be construed as follows:<sup>33</sup>

### **The Computer Misuse Act 1990**

Sections 1 and 2 of the 1990 Act provide:

**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 ...

**2.**—(1) A person is guilty of an offence under this section if he commits an offence under section 1 above (“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) ...’

Section 2 is thus dependent on s 1.

On the evidence before the magistrate, the conduct of Joan Ojomo came fairly and squarely within the provisions of s 1(1). She intentionally caused a computer to give her access to data which she knew she was not authorised to access. The reason why the magistrate did not commit Mr Allison on charges 1 and 2 was that he felt constrained by the provisions of s 17 and the interpretation put upon them by the Divisional Court in *DPP v Bignell* [1998] 1 Cr App R 1; the Divisional Court also followed and applied *Bignell's* case.

The relevant subsections of s 17 read:

‘(1) The following provisions of this section apply for the interpretation of this Act. (2) A person secures access to any program or data held in a computer if by causing a 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) has it output from the computer in which it is held (whether by having it

<sup>30</sup> s. 3 of the Cybercrimes Act

<sup>31</sup> s. 4

<sup>32</sup> At page 220 C

<sup>33</sup> At page 223 B – 226F

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) Access of any kind by any person to any program or data held in a computer is unauthorised if—(a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.'

Section 17 is an interpretation section. Subsection (2) defines what is meant by access and securing access to any program or data. It lists four ways in which this may occur or be achieved. Its purpose is clearly to give a specific meaning to the phrase 'to secure access'. Subsection (5) is to be read with sub-s (2). It deals with the relationship between the widened definition of securing access and the scope of the authority which the relevant person may hold. That is why the subsection refers to 'access of any kind' and 'access of the kind in question'. Authority to view data may not extend to authority to copy or alter that data. The refinement of the concept of access requires a refinement of the concept of authorisation. The authorisation must be authority to secure access of the kind in question. As part of this refinement, the subsection lays down two cumulative requirements of lack of authority. The first is the requirement that the relevant person be not the person entitled to control the relevant kind of access. The word 'control' in this context clearly means authorise and forbid. If the relevant person is so entitled, then it would be unrealistic to treat his access as being unauthorised. The second is that the relevant person does not have the consent to secure the relevant kind of access from a person entitled to control, ie authorise, that access.

Subsection (5) therefore has a plain meaning subsidiary to the other provisions of the 1990 Act. It simply identifies the two ways in which authority may be acquired—by being oneself the person entitled to authorise and by being a person who has been authorised by a person entitled to authorise. It also makes clear that **the authority must relate not simply to the data or program but also to the actual kind of access secured**. Similarly, it is plain that it is not using the word 'control' in a physical sense of the ability to operate or manipulate the computer and that it is not derogating from the requirement that **for access to be authorised it must be authorised to the relevant data or relevant program or part of a program**. It does not introduce any concept that authority to access one piece of data should be treated as authority to access other pieces of data 'of the same kind' notwithstanding that the relevant person did not in fact have authority to access that piece of data. Section 1 refers to the intent to secure unauthorised access to any program or data. These plain words leave no room for any suggestion that the relevant person may say: 'Yes, I know that I was not authorised to access that data but I was authorised to access other data of the same kind.'

### **Bignell's case**

*Director of Public Prosecutions v Bignell* [1998] 1 Cr App R 1 was decided in 1997. The leading judgment was given by Astill J with whom Pill LJ agreed. Two police officers had been convicted before the stipendiary magistrate of an offence under s 1 of the 1990 Act. They had for their own private purposes caused a police computer operator to obtain for them from the police national computer information about the ownership and registration of two cars. They had no authority to make that request or to obtain that information for that purpose. They were only permitted to make such a request for police purposes;

indeed, to obtain the information, they had to misrepresent to the computer operator the purpose of their request. The computer operator acted under an authorisation from the Commissioner of the Metropolitan Police. He was authorised to use the computer to access the data on the database at the request of police officers; he was required to ascertain and log the reason for the request.

The magistrate convicted the two officers of an offence under s 1. Their appeal to the Crown Court was allowed but the prosecution requested the Crown Court to state a case for the Divisional Court. The four stated questions of law are set out in the report ([1998] 1 Cr App R 1 at 8). They asked whether the Crown Court had been right in law to allow the appeal. The Divisional Court upheld the decision of the Crown Court.

The conclusion of the Divisional Court was probably right. It was a possible view of the facts that the role of the defendants had merely been to request another to obtain information by using the computer. The computer operator did not exceed his authority. His authority permitted him to access the data on the computer for the purpose of responding to requests made to him in proper form by police officers. No offence had been committed under s 1 of the 1990 Act. The Divisional Court rightly stated that the defendants could have been prosecuted for an offence under the Data Protection Act 1984.

However, in the course of his judgment Astill J, as he had been invited to by the Crown Court and the argument of counsel, expressed views about the purpose of the 1990 Act and the effect of s 17(5). Thus, he treated the primary issue as being 'whether a police officer who secures access to the Police National Computer for a non-police purpose secures unauthorised access' for the purposes of s 1. The submissions ([1998] 1 Cr App R 1 at 8) which he accepted were that the defendants 'were authorised to control access to the computer within the meaning of section 17(5) because they were authorised to obtain the material on the computer by causing the computer to function' and that 'controlling access is different from defining or restricting authority to access and section 17(5)(b) provides for the position of a person who enjoys a restricted level of access and is, therefore, barred from other levels of access without the consent of someone who is entitled to access at that level'. This acceptance (at 12–13) introduces a number of glosses which are not present in the 1990 Act. The concept of control is changed from that of being entitled to authorise to authorised to cause the computer to function. The concept of access to a program or data is changed to access to the computer at a particular 'level'. He also accepted the submission that the purpose of the 1990 Act was to criminalise the breaking into or hacking of computer systems which he understood to mean preserving the 'integrity of computer systems'. He accordingly characterised the defendants as persons who had 'control access' (using the word 'control' as a noun) 'of the kind in question'.

It was this use of language, departing from the language of the statute and unnecessary to the decision of that case, which misled the magistrate and the Divisional Court in the present case.

### **The decision of the Divisional Court**

My Lords, what I have already said serves to identify the points upon which the Divisional Court fell into error. The certified question refers to 'authority to access data of the kind in question'. The use of the phrase 'data of the kind in question' seems to derive from a simple misreading of s 17(5) and a confusion between kinds of access and kinds of data. Nor is s 1 of the 1990 Act

concerned with authority to access kinds of data. It is concerned with authority to access the actual data involved. Because s 1(1) creates an offence which can be committed as a result of having an intent to secure unauthorised access without in fact actually succeeding in accessing any data, s 1(2) does not require that the relevant intent relate to any specific data. But that does not mean that access to the data in question does not have to be authorised.

The key passage in the judgment of Kennedy LJ ([1999] QB 847 at 857), with which Blofeld J agreed, follows on his quotation of s 17(5):

'Miss Montgomery [for Mr Allison] submits that it is clear from the evidence that Joan Ojomo was entitled to control access of the kind in question to the program or data, just like the police officers in *Bignell's* case, so the access was not unauthorised even though she misused the information she obtained. Mr. Lewis [for the government] submits that her access was unauthorised because it was intentional, unauthorised by a person entitled to authorise access to that particular data and carried out when she knew that the access to that data was unauthorised. I confess that I found Mr. Lewis's approach to be the more attractive but at the end of the day it seems to me that it fails to do justice to the words "of the kind in question" which qualify the word access in section 17(5). Joan Ojomo was entitled to control access of the kind in question. She was operating in a regular way at her authorised level. As Astill J. said in *Bignell's* case ([1998] 1 Cr App R 1 at 12), the Act of 1990 was enacted to criminalise the "hacking" of computer systems, and the Data Protection Act 1984 was enacted to criminalise improper use of data.'

Thus, Kennedy LJ is making the same elisions as Astill J. He treats the phrase 'entitlement to control' as if it related to the control of the computer as opposed to the entitlement to authorise operators to access to programs and data. He adopts the extraneous idea of an authorised level of access without considering whether, on the facts of the case, it corresponds to the relevant person's authority to access the data in fact accessed. He confines s 1 of the 1990 Act to the 'hacking' of computer systems as opposed to the use of a computer to secure unauthorised access to programs or data. Upon a misreading of s 17(5), he fails to give effect to the plain words of s 1. The meaning of the statute is clear and unambiguous...

The decision of the Divisional Court in the present case was erroneous and the appeal fell to be allowed. As your Lordships' House has already announced the case has been remitted to the magistrate for reconsideration. Full reasons having been given for allowing the appeal, it is unnecessary separately to respond to the certified question... [bold emphasis not in original]

This case makes clearer the concept of "escalation of privileges" in that it explains the meaning of the equivalent to "*of the kind in question*" that is used in the Cybercrimes Act"<sup>34</sup>

It does not mean that it is access to data or a program of a similar kind. An accused cannot in

---

<sup>34</sup> See s. 2(4)

defence allege that the data in issue is of the same kind that he or she was authorised to access. As opined to by Lord Hobhouse, “[t]hese plain words leave no room for the suggestion that the relevant person may say: “Yes, I know that I was not authorised to access that data but I was authorised to access data of the same kind.”<sup>35</sup>

### **Unauthorised Modification as an Offence**

The Act makes it an offence for a person to modify the contents of any computer without authorisation.<sup>36</sup> Modification requires active participation by the person involved and usually involves the alteration of the nature, contents of the computer or operation of a data or program:<sup>37</sup>

*For the purposes of this Act, a modification of the contents of the computer takes place if, by the operation of any function of the computer concerned or any other computer -*

- (a) any program or data held in the computer concerned is altered or erased;*
- (b) any program or data is added to the contents of the computer concerned; or*
- (c) any act occurs which impairs the normal operation of any computer;*

*and any act which contributes toward causing such a modification shall be regarded as causing it.*

### **Unauthorised for the purposes of Modification**

The Act defines unauthorised in the context of modification. The modification is unauthorised if –

- (a) the person whose act causes the modification is not himself entitled to determine whether the modification should be made; and*
- (b) that person does not have the consent for the modification from any person who is so entitled.*

---

<sup>35</sup> At page 224 Paragraph F

<sup>36</sup> s. 5

<sup>37</sup> s. 2(6)

As with access, it is to be observed that modification is criminalised when it is unauthorised. However, it is important to note that there is no provision permitting a person will be permitted to make modifications under the *Interception of Communications Act* as allowed in relation to “access” under this Act. It means that with the exception of that omission, the definition of unauthorised in relation to modification is the same as for access. In this context, the *Bow Street (supra)* is equally applicable for the purpose of assisting with an understanding of how to interpret unauthorised for the purpose of modification. In order to prove this offence, “it is necessary to show that modification occurred as a result of the acts of the defendant.”<sup>38</sup>

### **Protected Computers**

Protected computers are computers that are used in health, education and the justice system. Harsher penalties are imposed where the offences in Part II are committed on protected computers.<sup>39</sup> The Act defines a protected computer as one that is concerned with:

1. the security or defence or international relations of Jamaica;
2. the existence or identity of a confidential source of information relating to the enforcement of the criminal law of Jamaica;
3. confidential educational material, such as examination materials;
4. the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or essential public infrastructure such as hospitals, courts, toll roads, traffic lights, bridges, airports and seaports; or

---

<sup>38</sup> Eoghan Casey, *Digital Evidence and Computer Crime* 2<sup>nd</sup> Edition (Academic Press: 2004) at page 76 (citing also *R. v. Whiteley* 1991 Cr, App Rep. 25 – note well this is case decided prior to the passing of the Computer Misuse Act 1990 but the reasoning appears to be of some relevance to proof by the prosecution.

<sup>39</sup> S. 9

5. the protection of public safety, including systems related to essential emergency services such as police, fire brigade services, defence and medical services.

These offences can only be tried in the Circuit court and the penalty on conviction is an unspecified fine or a maximum term of imprisonment for ten years or to both such fine and imprisonment. The mental element required is that the offender at the time of the offence knew or ought reasonably to know is a protected computer.<sup>40</sup>

### **Specific Liability in Relation to Corporations and Corporate Officers or Directors**

Corporations and their officers are also regulated under the Act. It recognises that corporations can only act through individuals and has made provisions for making them liable. Corporations, corporate officers and directors may be liable for offences committed by their employees or officers or by third parties. This is another legislation in recent times that has increased the corporate liability and responsibility of officers and directors. Prior to this was the Companies Act of Jamaica in 2004. Corporate officers therefore need to familiarise and apprise themselves of the provisions of this Act that relate to their operations. Section 11 of the Cybercrimes Act 2010 (the “Act”) makes “a director, manager, secretary or other similar officer, of that, body corporate – (a) *connived in the commission of the offence; or (b) failed to exercise due diligence to prevent the commission of the offence*” liable on conviction on indictment before a Circuit Court to a fine or to imprisonment for a term not exceeding five years or to both such fine or imprisonment.

The consequences in terms of process and punishment in relation to these corporate representatives are more stringent than those for individuals except where the individual is

---

<sup>40</sup> S. 9(2)

convicted in relation to a protected computer. In relation to offences other than those involving protected computers, whereas individuals can be prosecuted in either the Circuit court or in a Resident Magistrate's Court, a close reading of the Act shows that the liability of a corporate representative is only prosecutable in the Circuit court. The penalty for the corporate representative is a term of imprisonment not exceeding five years or an unspecified fine or both fine and imprisonment. The Act also confers jurisdiction on the court order civil law remedies in the nature of restitution. This is usually the domain of civil courts through the filing of a civil action.

### **Rethinking Corporate Governance in the Context of Potential Criminal Liability**

Companies must be aware that they have primary liability in which case the company itself may be subject to a fine or responsible for making restitution. In addition to this, the corporate representative can be liable because of the actions of not only employees but also of independent contractors and third parties. It is a non-delegable duty. This means that the duty to take care cannot be delegated to some functionary or employee. It is the corporate representative's duty to use *due diligence to prevent the commission of an offence*. In this regard, due diligence would take into account the security of, wireless networks, in terms of their reach and who can have access to them. In relation to wired networks, the access control protocols are equally important. These access control mechanisms should be documented, verifiable and include audit controls to ensure that they remain relevant and robust.

In summary, corporate governance and responsibility has just taken on a new meaning. Corporate actors must make corporate governance a priority. Being a director on any or many boards is no longer a matter of profile or standing. It involves a duty to know, to care and to

correct. Corporate actors should therefore take the time to consider their role seriously in the face of the possibility of personal criminal responsibility under the Act.

### **Procedural Regulation**

The Act followed the model of several international regional and sector specific conventions such as the Council of Europe Convention on Cybercrime and also made provision in Part III to regulate the procedural aspects of cybercrimes. This is a necessary inclusion because there needs to be some mechanism by which evidence is made available to a court in relation to these crimes whether they are committed through the use of a single or group of unconnected computers, a local or private network or by accessing a public network, such as the internet. Digital evidence requires different tools and techniques apart from those required for traditional forms of evidence. A warrant for search and seizure may not be enough or aptly make provision for capturing all of the evidence that is available especially when it resides on other networks. Further, digital evidence is easily destroyed or altered or can be rendered simply obsolete because of technology. In addition to this, there is no other procedure for the collection, preservation and admissibility of digital evidence because the Evidence Act has not been amended to deal with its peculiarities. This is where the Act has filled the gap in Part III.

Although Part III appears on the face of it to deal with just cyber or computer related crimes it is important to realise that it does not. It applies to all crimes that is, the offences created in the Act or traditional crimes. Support for the argument that the investigative provisions under Act are also intended to aid the investigation of traditional crimes is seen in a number of the sections under Part III which deals with the preservation and production of the evidence. An appreciation of this fact is necessary because the computer is used in different

ways in relation to the commission of crimes. It can be a cyber or computer crime as prescribed in the Act and in that sense it is the *subject* of the crime, for example where there is an escalation of access or unauthorised modification on the device that is the subject of an investigation. In other words, it is the *environment* in which the crime is committed. On the other hand, when that same device is accessed lawfully, but used to remotely gain unauthorised access to another computer on an internal network or at a remote location it is classified as the *instrument* of the crime. As an *instrument* of crime, it is not the device itself that is of interest but the evidence it contains bearing in mind that remote access is likely to have been made possible by the use of a program or code.

Provision is therefore made for the preservation of data by authorising a constable to serve notice on any person who has control or possession of any computer or data storage medium<sup>41</sup> where he “*satisfied that data stored in a computer or any data is reasonably required for the purposes of criminal investigations and there is reasonable grounds for suspecting that the data may be destroyed or rendered inaccessible.*”<sup>42</sup> The constable can only ask for data to be stored for thirty (30) days but the period may be extended by a Magistrate. There are penalties for failing to preserve data when so put on notice or ordered by a Magistrate.<sup>43</sup> Apart from observing that this provision authorises the method by which evidence may be preserved, it should also be noticed that it makes provision in relation to *criminal investigations* and not a crime committed under this Act.

Further, a Magistrate can also issue search and seizure warrants if he or she is satisfied on oath that there are reasonable grounds to suspect that “*computer material may be relevant as*

---

<sup>41</sup> s. 14

<sup>42</sup> *ibid*

<sup>43</sup> *ibid*

evidence in proving an offence; or has been acquired for, or in, the commission of an offence or as a result of the commission of an offence.”<sup>44</sup> This provision also has an expanded scope; its application is not limited to offences committed under the Act but to *an offence*. This section also demonstrates the uniqueness of the investigative techniques for digital evidence. It does this by providing further in s. 15(2) that the warrant under s. 15(1) “shall authorise the constable, **with the assistance of such other person as may be necessary,** to enter the place specified in the warrant to search and seize for computer material.” It is important for the police to recognise not only the existence of this provision but to utilise it. What this provision does is to accept that specialised training and equipment is necessary for the gathering, collecting and processing of digital evidence. It further recognises that the police may not have all the required training or expertise and so this provision enables them to take on board the relevant experts such as computer forensic experts who are trained to capture, analyse and present digital evidence in court. The drafters of the 2009 ITU draft report on Understanding Cybercrimes: A Guide for Developing Countries provide some useful insight into this recommendation:

The main difference between a traditional investigation and a cybercrime investigation is the fact that a cybercrime investigation does in general require specific data related investigation techniques and can be facilitated by specialised software tools. In addition to adequate procedural instruments carrying out such analysis requires the ability of the authorities to manage and analyse relevant data. Depending on the offences and the computer technology involved the requirements with regard to the procedural investigation instrument and the forensic analysis differ and go along with unique challenges. In general these two aspects of cybercrime investigations that are closely connected and often described by the term “computer forensics”, or the collection and analysis of evidence...the term computer forensics describes the application of computer investigation and analysis techniques to determine potential evidence. This covers a wide range of analysis ranging from general analysis like search for child pornography on computer hard disks, to specific investigation such as iPod forensics and accessing encrypted files. Experts in computer forensics support investigations carried out by specialised police officers and prosecutors.

It is therefore hoped that the police, the prosecution services and defence counsel will see and appreciate the need for these specialised services or experts and create a market for them.

---

<sup>44</sup> S. 15(1)

Currently, there are at least ten (10) certified computer forensics experts in Jamaica who are both not known and are not utilised. They are information technology workers in various government departments and some private entities. The science should be encouraged so as to strengthen the investigative capacity of the police and also the ability of defence lawyers to argue their cases. The passage of the Act means that the science is here to stay, the technologies are rapidly expanding and so is crime in that space and the ability to make the fruits of crime inaccessible. The police are also required to record the seized material, where it has been rendered inaccessible. This is necessary to preserve the integrity and admissibility of the evidence. This is another area in which the assistance of computer experts is likely to be necessary.

In case of inaccessible material the Magistrate also has power to make a production order. This will compel the person who has control or access to the data to produce the information in an intelligible form. The subject of the order may at their option produce the password or key to the accessing and converting the material. The production order in keeping with the wider scope of the Act is made where the information “is reasonably required for the purpose of a *criminal* investigation or *criminal* proceedings...”<sup>45</sup> However; it is of some interest that this provision does not make reference to the privilege against self-incrimination. It is difficult to see how the order could be a basis for the police to fail to “read” the accused is rights and if he does, the effect that has on the order when an accused chooses to invoke those rights. It is an interesting thought, but for another paper.

---

<sup>45</sup>

S. 17

## **Jurisdiction and Penalty**

Offences, with the exception of an offence in relation to a protected computer, may be tried in either the Resident Magistrate's court or the Circuit court. At first blush it is not clear when an offence will be tried in one or the other. However, on closer review it can be seen that it is a matter of jurisdiction. The Judicature Resident Magistrate's Court Act creates the office of The Resident Magistrate so that its jurisdiction comes from that statute. The jurisdiction of the Magistrate in criminal matters is limited to crimes committed within the parish and within a twelve (12) mile radius. It follows that crimes prosecutable under the Act that are committed within this area would be prosecuted in the Magistrate's court. This presents a small anomaly however. The anomaly is evident where an offence though confined to a parish, may include damage that far exceeds the limit that a Magistrate could award as damages. In these circumstances, there would be good reason for transferring the matter to or prosecuting it in the Circuit court. The most likely, circumstance in which a matter ought to or must be prosecuted in the Circuit court is where the offence is committed across parish borders. This would be in case where a person uses a computer in St. James to hack into a computer in Kingston.

The penalties for the offences, except for protected computers, are the same. The penalty for conviction depends on whether the offence is tried in the Resident Magistrate's Court of the Circuit Court. The trial in the former is a summary trial whereas in the Circuit Court, it is on indictment. The severity of the penalty depends on whether the offence causes damage. In the Resident Magistrate's court these matters are tried summarily that is, not on an indictment. If there is no damage, the penalty is a maximum of two years imprisonment and/or a fine of two million dollars (\$2,000,000). If there is damage, the term of imprisonment is a maximum of three years and/or a fine not exceeding three million dollars (\$3,000,000). In a trial on indictment the

penalty on conviction is imprisonment of five years or an unspecified fine or both if no damage is done. If damage is done, the term of imprisonment is seven years or an unspecified fine or to both such fine and imprisonment. The penalty in the Circuit court is a term of imprisonment of up to a maximum of five (5) years or an unspecified fine. Where damage is caused the term of imprisonment is up to a maximum of seven years and an unspecified fine.

The Act also confers jurisdiction on the judge or magistrate to order compensation “*to any person who has suffered loss as a result of the commission of the offence.*”<sup>46</sup> This does not prevent the person from seeking any other remedy to which he or she is entitled to at law. It does not mean however, that the person will be compensated twice. The application for compensation must be made before sentencing in accordance with “*rules of court.*” ‘Rules of court’ is not been defined. In the Resident Magistrate’s court it is likely that the application will be made on motion and on application in the Circuit court.

## **Conclusion**

From the foregoing, it can be seen that the Cybercrimes Act 2010 has provided a comprehensive though not exhaustive framework for prosecution and investigating of cyber, computer related and other crimes. There is provision for the offences in relation to both public and corporate liability and harsher penalties for computers that are used in the public interest that is protected computers. The Act is not only offence neutral in so far as none of the familiar names such as identity theft, hacking or denial of access appear in it even though they are covered but also covers content related offences such as criminal libel and obscene publications. Further, in a manner similar to the Proceeds of Crime Act (POCA) it provides civil procedure

---

<sup>46</sup>

s. 12

and remedies to investigate the incidents and present the evidence. These include preservation and production orders and most importantly it enables the criminal court to order damages which would ordinarily be the purview of the civil courts. In this respect it narrows the gap between existing evidence rules and the technology driven form of evidence that arise when internet crimes or crimes committed using computers. It appears to be the first statute that embraces the use of private actors as part of the investigative process. In a real way, it has been timely in coming and goes a far way in enhancing Jamaica's crime fighting capability.