Workshop on Harmonizing Cyberlaw in the ECOWAS region

(Substantive Law in the Budapest Convention)

Ghana, Accra

17 – 21 March 2014,

Kofi Annan International Peacekeeping Training Centre

Attorney Sizwe Lindelo Snail Ka Mtuze

TABLE OF CONTENTS

SNAIL
ATTORNEYS AT LAW

Part 1: Council of Europe response to cybercrime

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.

SNAIL
ATTORNEYS AT LAW

Part 1: Council of Europe response to cybercrime cont.

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.

SNAIL
ATTORNEYS AT LAW

Part 1: Council of Europe response to cybercrime cont.

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 above, 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.

SNAIL
ATTORNEYS AT LAW

Part 1: Council of Europe response to cybercrime cont.

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.

SNAIL
ATTORNEYS AT LAW

Part 1: Council of Europe response to cybercrime cont.

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 above, 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 2 above, 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.

SNAIL
ATTORNEYS AT LAW

Part 1: Council of Europe response to cybercrime cont.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

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, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;
b an authority to take decisions on behalf of the legal person;
c an authority to exercise control within the legal person.

Lessons learnt from Counsel of Europe Convention on Cybercrime

Counsel of Europe Convention on Cyber Crime

The **Council of Europe's Convention on Cyber crime (November 2001)** has influenced the drafting of several Cybercrime legislations around the world and in Africa. Under the convention, member states are obliged to:

- criminalise the illegal access to computer system,
- illegal interception of data to a computer system,
- interfering with computer system without right, intentional interference with computer data without right,
- use of inauthentic data with intend to put it across as authentic (data forgery),
- infringement of copyright related rights online,
- interference with data or functioning of computer system,
- child pornography related offences (possession/distribution/procuring/producing of child pornography).
- The Convention's broad coverage of offences has drawn extensive criticism. Critics argue that it should limit itself to protecting the global information infrastructure by criminalizing "pure" cyber crimes. Fraud and forgery, they argue, are already covered in existing international agreements and should not be included in the Convention as "computer-related fraud" and "computer-related forgery."[1]
-

([1] Convention on Cybercrime: "Themes and Critiques" By Calvert Jones, Berkeley University http://www.cyberlawenforcement.com/)

SNAIL
ATTORNEYS AT LAW

Part Two: South African response to e-commerce and cybercrime –The Electronic Communications and Transactions Act, Act 25 0f 2002

Common law position: Prior to the ECT Act

Introduction

Prior to ECT, the common and statutory law at that time could be extended as widely as possible

One can easily apply the common law crimes of defamation, indecency (Online child pornography, decimation of child porn), crimen iniuria (also known as Cyber-smearing) fraud (Cyber fraud) (see the case of *S v Van den Berg 1991 (1) SACR 104 (T)*), defeating the ends of justice, contempt of court (in the form of publishing any court proceedings without the courts permission online or by other electronic means), theft (see the cases of *S v Harper 1981 (2) SA 638 (D)* and *S v Manuel 1953 (4) SA 523 (A) 526* where the court came to the conclusion that money which had been dematerialized could be stolen in it immaterial form) and forgery to the online forms of these offences.

SNAIL
ATTORNEYS AT LAW

The applicability of the common law however has its own limitations and narrows significantly when dealing with online crimes involving assault, theft, extortion, spamming, phishing, treason, murder, breaking and entering into premises with the intent to steal and malicious damage to property.

When looking at the crimes of breaking and entering with intent to steal as well as the crimes of malicious damage to property two commonly known categories of Computer crimes come to mind. On the one hand, hacking and cracking and on the other hand the production and distribution of malicious code known as viruses, worms and Trojan Horses.

SNAIL
ATTORNEYS AT LAW

In S v Howard (unreported Case no. 41/ 258 / 02, Johannesburg regional magistrates court) as discussed by Van der Merwe, the court had no doubt whether the crime of malicious damage to property could apply to causing an entire information system to breakdown.

The Court also mentioned further that the crime no longer needed to be committed to “physical property” but could also apply to data messages of data information.

(D van der Merwe (2008) 70)

SNAIL

ATTORNEYS AT LAW

Child Pornography

Crimes such as possession and distribution of child pornography can be prosecuted in terms of the Films and Publications Act, Act 65 of 1996 which provided in its definition of publication that a publication is:

"(i) any message or communication, including visual presentation, placed on any distributed network including, but not confined to, to the internet. "

In terms of section 27 (1) and section 28 of the said legislation if anyone creates, produces , imports or is in possession of a publication or film which contains scenes of child pornography, he shall be guilty of an offence. Gordon also notes that the act may also extend to "pseudo-pornography" as found in animated pornography. (Barrie Gordon (2000) 439).Section 25 and section 26 also prohibit the decimation of child pornography in films or publications respectively.

SNAIL
ATTORNEYS AT LAW

Evaluation of e-Evidence at Common Law

Watney states that section 35(5) of the Constitution of South Africa finds application. Section 35(5) states that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence render the trial unfair or will otherwise be detrimental to the administration of justice. (M Watney (2008) 2).

I

he constitutional court confirmed in the matter of *Key v Attorney-General, Cape Provincial Division (1996 (6) BCLR 788 (CC))* '(b)ut there will be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted.'

Issues of proof are traditionally classified under three headings namely: witnesses, objects (real evidence) and documents.

SNAIL
ATTORNEYS AT LAW

Interception and Monitoring Prohibition Act

The Interception and Monitoring Prohibition Act specifically governs the monitoring of transmissions including e-mail.

Section 2 states that: no person shall –

"intentionally intercept or attempt to intercept or authorize, or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission "

This means in simple terms that conduct that:

(a) Intentionally and without the knowledge or permission of the dispatcher to intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or
(b) Intentionally monitor any conversations or communications by means of a monitoring device so as to gather confidential information concerning any person, body or organization,

SNAIL
ATTORNEYS AT LAW

Regulation of Interception of Communications and Provision of Communication-related Information Act - RICA

The Interception and Monitoring Prohibition Act 127 of 1992 was repealed by the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (hereafter referred to as RICA). RICA, the Electronic Communications Act 25 of 2002 and the Promotion of Access to Information Act 2 of 2000 (PROATIA) generally prohibit the unlawful interception or monitoring of any data message (Cohen 2001: 2–4).

RICA specifically governs the monitoring and/or interception of transmissions including e-mail. In Section 2 it states that:

" No person shall Intentionally intercept or attempt to intercept or authorize, or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."

This is subject to the legally accepted **"grounds of justification "** in case of an **emergency** , **serious criminal offence** , **necessity** , if **authorised by interception order** and **interest of state security .**

.

SNAIL
ATTORNEYS AT LAW

Part Three: South African response to e-commerce and cybercrime –The Electronic Communications and Transactions Act, Act 25 0f 2002

In *Narlis v South African Bank of Athens 1976 (2) SA 573 (A),* the Court held that a computer printout was inadmissible in terms of the Civil Procedure and Evidence Act 25 of 1965. It was also held that a computer is not a person. It was clear that the law regarding value of electronic data in legal proceedings required urgent redress.

This resulted in the premature birth of the Computer Evidence Act 57 of 1983. Section 142 of the said act made provision for an authentication affidavit in order to authenticate to authenticate a computer printout. The Computer Evidence Act seemed to make more provision for civil matters than criminal ones. It created substantial doubts and failed the mark for complimenting existing statues and expansion of common principles. (M Kufa (2008) 18 -19)

SNAIL
ATTORNEYS AT LAW

Part Three: South African response to e-commerce – The Electronic Communications and Transactions Act, Act 25 0f 2002 cont

- After many years of legal uncertainty, Parliament enacted the Electronic Communications and Transactions Act, Act 25 of 2002 (ECT) which comprehensively deals with E-commerce as aspects and Cyber-crimes

- One must however, **note section 3** of the ECT (its interpretation clause) which does not exclude any statutory or common law from being applied to, recognizing or accommodating electronic transactions – in other words the common law or other statues in place wherever applicable is still in force and binding which has the result that wherever the ECT has not made specific provisions such law will be applicable.

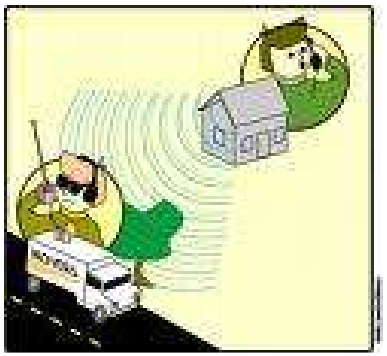
SNAIL
ATTORNEYS AT LAW

Cyber Crime

- **Section 85 defines 'unlawful access' as the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorized to access that data and still continues to access that data (S L. Geredal (2006) 282).**

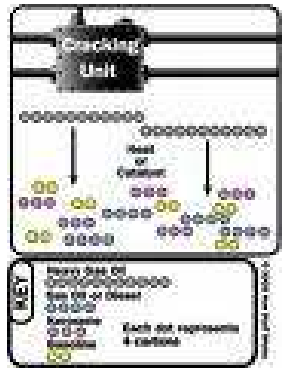
"Someone's been using my computer, too!"

- **Section 86(1) provides that, subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.**



SNAIL
ATTORNEYS AT LAW

Section 86(2) states that anyone who intentionally and without authority to do so interferes with data in a way which causes such data to be modified , destroyed or otherwise rendered ineffective is guilt of an offence.



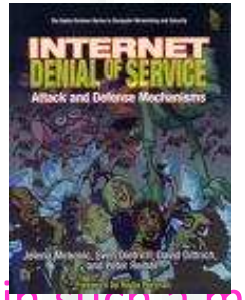
Section 86 (4) and 86(3) introduces a new form of crime known as the anti-cracking (or anti-thwarting) and hacking law. In terms of Section 86 (3) the provision and, or selling and, or designing and, or producing of anti-security circumventing (technology will be a punishable offence. (GJ Ebersoehn (2003) 16)

In terms of section 86(4) it is requirement to be guilt of this offence if the offender uses and designs a programme to overcome copyright protection, with direct intent to overcome a specific protection data protection programme (GJ Ebersoehn (2003) 17).

SNAIL
ATTORNEYS AT LAW

Denial of service (DOS) attacks also popularly known as Disk Operating System attacks, are attacks that cause a computer system to be inaccessible to legitimate users.

Section 86(5) states that, "any person who commits any act described in **Section 86** with the intent to interfere with access to an information system so as to constitute a denial , including a partial denial of services to legitimate users is guilt of an offence ".



The act or conduct is fashioned in such a manner that it is widely defined and consist of any of the action criminalized in **Sections 86(1) – Section 86 (4).** The actions include unauthorized access, unauthorized modification or utilizing of a program or device to overcome security measures. (M Kufa (2008) 20)

SNAIL
ATTORNEYS AT LAW

Similarly one can deduce that e-mail bombing and spamming is now also a criminal offence as contained in the wide definition of s86 (5) and s45 of the ECT respectively.

Section 87 of the ECT also has introduced the Cyber crimes of E-Extortion as per section 87(1), E-Fraud as section 87(2) and E-Forgery as section 87(2). Section 87(1) provides an alternative to the common law crime of extortion. Kufa states that pressure is therefore exerted by threatening to perform any of the acts criminalized in section 86.

Kufa also criticizes this section as “wet behind the ears“as its common law equivalent applies to both forms of advantage of a propriety and non-propriety form. He suggests that this proviso is wanting and will require redress. (M Kufa (2008) 21)

SNAIL
ATTORNEYS AT LAW

Part 4: Legislative response to Cyber Crime in Ghana

Electronic Transactions Act, 2008 – Act 772

Cyber offences

107. Stealing
108. Appropriation
109. Representation
110. Charlatanic advertisement
111. Attempt to commit crimes
112. Aiding and abetting
113. Duty to prevent felony
114. Conspiracy
115. Forgery
116. Intent

SNAIL
ATTORNEYS AT LAW

Electronic Transactions Act, 2008 – Act 772

Cyber Offences (continued)

117. Criminal negligence
118. Access to protected computer
119. Obtaining electronic payment medium falsely
120. Electronic trafficking
121. Possession of electronic counterfeit-making equipment
122. General offence for fraudulent electronic fund transfer
123. General provision for cyber offences
124. Unauthorised access or interception
125. Unauthorised interference with electronic record
126. Unauthorised access to devices
127. Unauthorised circumvention
128. Denial of service
129. Unlawful access to stored communications

SNAIL
ATTORNEYS AT LAW

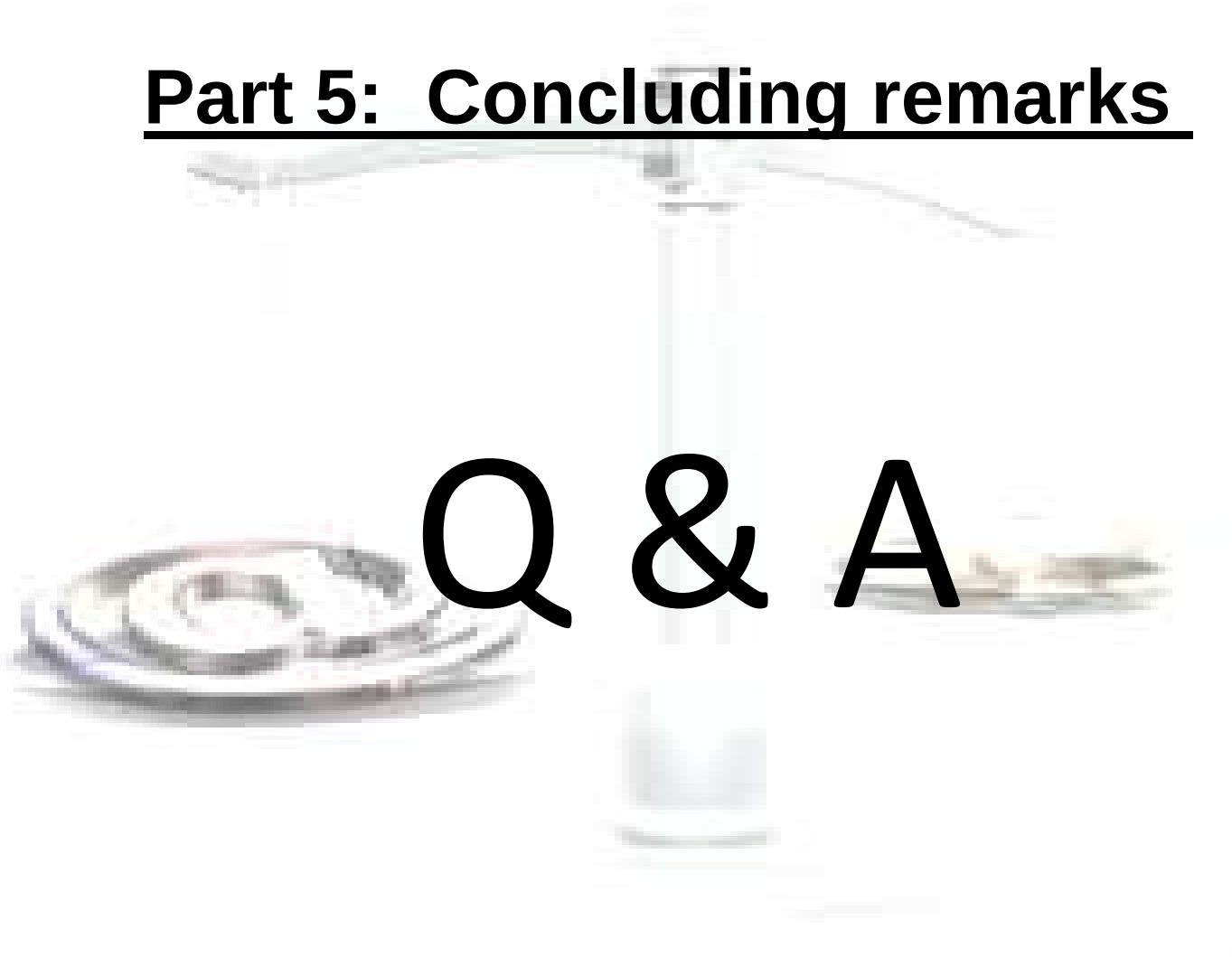
Electronic Transactions Act, 2008 – Act 772

Cyber Offences (continued)

130. Unauthorised access to computer programme or electronic record
131. Unauthorised modification of computer programme or electronic record
132. Unauthorised disclosure of access code
133. Offence relating to national interest and security
134. Causing a computer to cease to function
135. Illegal devices
136. Child pornography
137. Confiscation of assets
138. Order for compensation
139. Ownership of programme or electronic record
140. Conviction and civil claims

SNAIL
ATTORNEYS AT LAW

Part 5: Concluding remarks



Q & A

Contact Us:

SNAIL
ATTORNEYS AT LAW

Attorney : Sizwe Lindelo Snail Ka Mtuze
Director - Snail Attorneys @ Law Inc.

E-mail : ssnail@Snailattorneys.com
www : www.snailattorneys.com
Tel / Fax : +27 (012) 362 8939
Fax : +27 (086) 617 5721
Cell : +27 (083) 477 4377