Workshop on Harmonizing Cyberlaw in the ECOWAS region

African Perspectives to cyber crime

Ghana, Accra
17 – 21 March 2014,
Kofi Annan International Peacekeeping Training Centre

Attorney Sizwe Lindelo Snail Ka Mtuze

TABLE OF CONTENTS

Part One : African response to e-commerce and cyber cirme

EAST AFRICAN COMMUNITY

SOUTHERN AFRICAN DEVELOPMENT COMMUNITY
TOWARDS A COMMON FUTURE

African Union
a United and Strong Africa

Economic Community of West African States (ECOWAS)

The Supplementary Act on Cyber Crime

DIRECTIVE CIDIR. 1/08/11 ON FIGHTING CYBER CRIMEWITHIN ECOWAS

In 2009 ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states

Focus more on ***Cyber Crime , Search and Procedure*** *and* ***Data Protection***

EAST AFRICAN COMMUNITY

EAC LEGAL FRAMEWORK FOR CYBERLAWS
EAC 1 and EAC 2

Legal Framework and Recommendations

Electronic transactions and Issues of validity

Electronic Evidence

Electronic signatures and authentication

Computer crime

*Substantive offences
*Criminal procedure

Consumer protection

Data protection and privacy

SOUTHERN AFRICAN DEVELOPMENT COMMUNITY
TOWARDS A COMMON FUTURE

SADC E-COMMERCE MODEL LAW (2012)

* LEGAL RECOGNITION OF ELECTRONIC COMMUNICATIONS and LEGAL EFFECT OF ELECTRONIC COMMUNICATIONS

* TIME AND PLACE OF DISPATCH AND RECEIPT OF ELECTRONIC COMMUNICATIONS

* THE PROTECTION OF ONLINE CONSUMERS

* EVIDENTIARY ISSUES AND VALUES OF ELECTRONIC EVIDENCE

* ONLINE MARKETING

* INTERMEDIARIES

African Union
a United and Strong Africa

Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (2012)

•Unlike the UNCITRAL Model Law for E-commerce Article I-1 of the Convention has interestingly omitted definitions such as **"data", "writing " , "electronic signature" and "original"** which give effect to the functional equivalence approach.

•They have been substituted with wide definitions for the terms **"electronic commerce" , "electronic mail " and "information" .**

•Articles I-23 confirms the **"party autonomy"** principle in that its states that***, "no person shall be compelled to take a legal action by electronic means."*** as well as the right not to choose technology.

SNAIL
ATTORNEYS AT LAW

African Union
a United and Strong Africa

Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (2012) cont.

•Article I-24 furthermore confirms the **"functional equivalence principle "** in that**, "where a written matter is required to validate a legal act such maybe established and conserved in electronic form"** under the conditions of the said domestic law applicable.

•Article I-25 excludes the following acts from being perfumed electronically in terms of the AUCLCS namely the **signature of a private individual relating to family law or law of succession and acts of a civil or commercial nature under the signature of a private individual relating to real security or personal security**.

The convention also guarantees the **validity of electronic signatures and gives the definition for electronic signatures** in Article I – 32 as,

" data in electronic form attached to or logically subjoined to a data message and which can be used to identify the data message signatory and indicate consent for the information contained in the said message."

SNAIL
ATTORNEYS AT LAW

The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (2011)

- **Article III – 1 – 1: Laws against cyber crime**

Each Member State shall adopt such legislative measures as it deems effective to set up material criminal offenses as acts which affect the confidentiality, integrity, availability and survivability of ICT systems and related infrastructure networks; as well as effective procedural measures for the arrest and prosecution of offenders. Member States shall take into account the approved language choice in international cyber crime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations where necessary.

- "**Article III – 1 – 5: Harmonization "**

Each Member State shall ensure that the legislative measures adopted in respect of substantive and procedural provisions on cyber crime reflect international best practices and integrate the minimum standards contained in extant legislations in the region at large so as to enhance the possibility of regional harmonization of the said legal measures.

SNAIL
ATTORNEYS AT LAW

The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (2012) (cont.)

- **"Article III – 1 – 19: Harmonization"**

Each Member State shall ensure that the legislative measures adopted in respect of material and procedural provisions on cyber security reflect international best practices and integrate the minimum standards contained in extant legislations in the region at large so as to enhance the possibility ofregional harmonization of the said legal measures."

The convention differentiates and proposes amendment to existing law with regards to :

- Attack on computer systems
- Procedural Law
- Attack on computerized data
- Content related offenses
- Proposes adapting certain sanctions to the Information and Communication Technologies
- Offenses relating to electronic message security measures
- Offenses specific to Information and Communication Technologies
- Proposes adapting certain information and communication technologies offenses

SNAIL
ATTORNEYS AT LAW

BURUNDI

•On 29 April 2009, Burundi adopted a new account the new criminal phenomenon of cybercrime. Previously, the Criminal Code of 1981 did not punish intrusive behaviors in computer systems and data such as cases of forgery and use of forged material through computer including the modification or destruction of stored data, treated or transmitted by a computer system, and the unauthorised access to a computer system (hacking).

•Burundi's criminal law was amended in 2010 by this Bill in areas such as cybercrime (computer-related crimes). Cybercrime includes common law offenses to which IT (information technology) is a simple tool. Criminal Code does not provide for offences that may be committed using the internet such as theft, fraud, slander, blackmail and harassment, racial aversion, sabotage, and the dissemination of child pornography, the general principles of criminal law are applied. Now the Burundian Penal Code states :

"Whoever commits forgery, introducing a computer system, modifying or deleting data that is stored, treated or transmitted by a computer system, or changing by any technological means possible use of data in a computer system and thereby alters the legal implications of such data, shall be punished by imprisonment of five to twenty years and a fine of fifty thousand to one hundred thousand francs. Whoever makes use of data obtained, knowing that it is false shall be punished as if he were the author of the falsity "

SNAIL
ATTORNEYS AT LAW

KENYA

•The Kenya Information and Communications Act hosts the electronics communication law and cyber crimelaw. The Act complies with the regional AU Draft Convention on Cybercrime. The provisions under the part of the Act on electronic transactions include—

•Unauthorized access to computer data and access with intent to commit offences;
•Unauthorized access to and interception of computer service;
•Unauthorized modification of computer material;
•Damaging or denying access to computer system;
•Unauthorized disclosure of password;
•Unlawful possession of devices and data;
•Electronic fraud;
•Tampering with computer source documents;
•Publishing of obscene information in electronic form;
•Publication for fraudulent purposes; and
•Unauthorized access to protected systems.

Significantly, the Evidence Act also introduced amendments which allow for admissibility of electronic evidence and the conditions for storing, preservation and presentation of electronic evidence.

SNAIL
ATTORNEYS AT LAW

RWANDA

•Cyber law (in particular provision on cyber crime) have been included in Rwanda's Organic law. Under the Penal Code, section 5 refers to computer related crimes.

•The penalties include the payment of fines of between 5 to 7 million Rwandese Francs. Recidivists are also punished with the same penalties. Tere are no specific legislations to deal with cyber crimes, but these will be developed in due course.

TANZANIA

•There is no specific law on e-commerce in Tanzania as yet.

•Even electronic evidence was not admissible in court until fairly recently when the High Court in an unprecendented move, admitted electronic evidence for the first time in the case of Trust Bank Tanzania Ltd V Le Marsh and Others (Commercial Case No 4 of 2000) This subsequently triggered the amendment of our Evidence Act (TEA) to permit admissibility of electronic evidence. (see Section 40A of Tanzania Evidence Act Chapter 6 of Tanzanian Laws.)

•However, there is a draft bill on cybercrime control which is being discussed by a variety of stakeholders. The legislation is expected to be comprehensive and effective. The draft bill will be discussed later in this presentation in detail.

SNAIL
ATTORNEYS AT LAW

UGANDA

•**The Computer Misuse Act , 2011**is the principal legislation covering cyber crime. It provides for the safety and security of electronic transactions and information systems, the prevention of unlawful access, abuse or misuse of information systems including computers and for securing the conduct of electronic transactions in a trustworthy environment.

•The act creates offences with respect to the unauthorised use, access, abuse of computers or data. It also has provisions on electronic fraud, child pornography, cyber harassment, cyber-stalking. The Uganda Communications Commission (UCC) has set up its own CERT to compliment the national team and this was set up on the 6th of June 2013.

•The CERT prowls the Internet to monitor and report hi-tech crime including cyber terrorism, computer intrusion,online sexual exploitation and cyber fraud. The team also coordinates all other multi sectoral agencies in this fight against cyber crime; liaises with other law enforcement agencies in the prosecution of cyber related crimes and collaborates with other regional and international agencies with similar remits.

•There is a general lack of capacity among the police and other law enforcement agencies to detect, investigate and assist in prosecution under the Computer Misuse Act 2011. This has been a challenge in the prosecution of some high profile cases in the country like *Uganda Vs Kato Kajubi* and *Uganda Vs Dr. Aggrey Kiyingi* cases that relied on electornic evidence. In *Kato Kajubi* following a retrial, the accused was convicted. Following the terrorist attack on Kampala on 11th July 2010, the police with the help of the FBI were able to uncover emails linking the bombings to the suspects.

NORTH SUDAN

•North Sudan adopted the Cyber Crime Law of 2007 and in addition thereto promulgated the Informatics Crimes Law 2007 as well as CERT Sudan.

• North Sudan then had identified the following challenges against the fight against cyber crime

1- The development of communication speed which helps to speedup the electronic crime.
2. Local internet providers do not have log files for internet utilize for their customers.
3. Using unlicensed programs.
4. Lack of sufficient awareness about the electronic crimes.
5. The spread of Internet cafes , without making laws for
their work.

SNAIL
ATTORNEYS AT LAW

Part 2 : Tanzanian responses to cybercrime

- Tanzania does not have specific legislations dealing with cyber security, prevention, detection and enforcement of cyber crimes.
- Currently the laws which are in place were made before cyber security was an issue. While cyber crimes pose a significant threat to the development of electronic transactions
- Tanzanian Laws do not recognize criminal activities on the internet. For example illegal intrusion into a computer system cannot be prosecuted with the current legislations which require physical presence. (Asherry Magalla 2013)

SNAIL
ATTORNEYS AT LAW

Part 2 : Tanzanian responses to cybercrime (cont .)

Draft Computer Crime and Cybercrime Bill Tanzania (2013)

Objectives and Provisions

- Act provides a legal framework for the criminalization of computer and network related offences.
- Principal aims are to criminalize certain illegal content in line with regional and international best practices, provide the necessary specific procedural instruments for the investigation of such offences and define the liability of service providers.
- Draft Bill divided into nine parts – All provisions of Model law on cybercerime transposed and expanded as appropriate to suit Tanzania situation.
- The Proposed Bills have been drafted using technology neutral language in line with the UNCITRAL Model Law

(Judith M.C.Tembo – 2013)

SNAIL
ATTORNEYS AT LAW

Part 2 : Tanzanian responses to cybercrime (cont .)

• The Bill provides Substantive criminal law provisions in Sections 5-26 of the Bill to address computer and network-related crime by defining a common minimum standard of relevant offences based on international best practise as guided by (EAC 1 and EAC 2) and (SADC Cybercrime Model Law) as well as international standards (COE- Cybercrime Convention) and (The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa and the Commonwealth Cybercrime Initiative).

•Section 27 of the Bill creates the principle of "Territorial Jurisdiction" in the event that :

- both the person attacking a computer system and the victim system are located within the same territory or country **and** the computer system attacked is within its territory, even if the attacker is not.

SNAIL
ATTORNEYS AT LAW

Part 2 : Tanzanian responses to cybercrime (cont .)

- Sections 28-35 of the Bill intend to amend any procedural law and to cure any *lacunae* in the Tanzanian Law by defining common minimum standards based on best practices within the region (EAC 1 and EAC 2) and (SADC Cybercrime Model Law) as well as international standards (COE- Cybercrime Convention) and (The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa and the Commonwealth Cybercrime Initiative).

- Section 36 -41 define the different types of cyber criminal liability of service providers and search engines.

SNAIL
ATTORNEYS AT LAW

Part 2 : Tanzanian responses to cybercrime (cont .)

Overview of the Bill

Substantive Offences

5.Illegal Access
6.Illegal Remaining
7.Illegal Interception
8.Illegal Data Interference
9..Data Espionage
10.Illegal System Interference
11..Illegal Devices
12.Computer-related Forgery
13.Computer-related Fraud

SNAIL
ATTORNEYS AT LAW

Part 2 : Tanzanian responses to cybercrime (cont .)

Overview of the Bill

14. Child Pornography
15. Pornography
16. Identity-related crimes
17. Racist and Xenophobic Material
18. Racist and Xenophobic Motivated Insult
19. Denial of Genocide and Crimes Again Humanity
20. SPAM
21. Illegal Commerce and Trade
22. Disclosure of details of an investigation
23. Failure to permit assistance
24. Harassment utilizing means of electronic communication

SNAIL
ATTORNEYS AT LAW

Part 2 : Tanzanian responses to cybercrime (cont .)

Overview of the Bill

Aspects of Jurisdiction

- 25.Jurisdiction
- 26. Extradition

Electronic Evidence

- 27.Admissibility of Electronic Evidence

SNAIL
ATTORNEYS AT LAW

Part 2 : Tanzanian responses to cybercrime (cont .)

Overview of the Bill

Procedural Law

28.Search and Seizure
29.Assistance
30.Production Order
31.Expedited preservation
32.Partial Disclosure of traffic data
33.Collection of traffic data
34.Interception of content data
35.Forensic Tool

SNAIL
ATTORNEYS AT LAW

Part 2: Tanzanian responses to cybercrime (cont .)

Overview of the Bill

36.No Monitoring Obligation

37.Access Provider

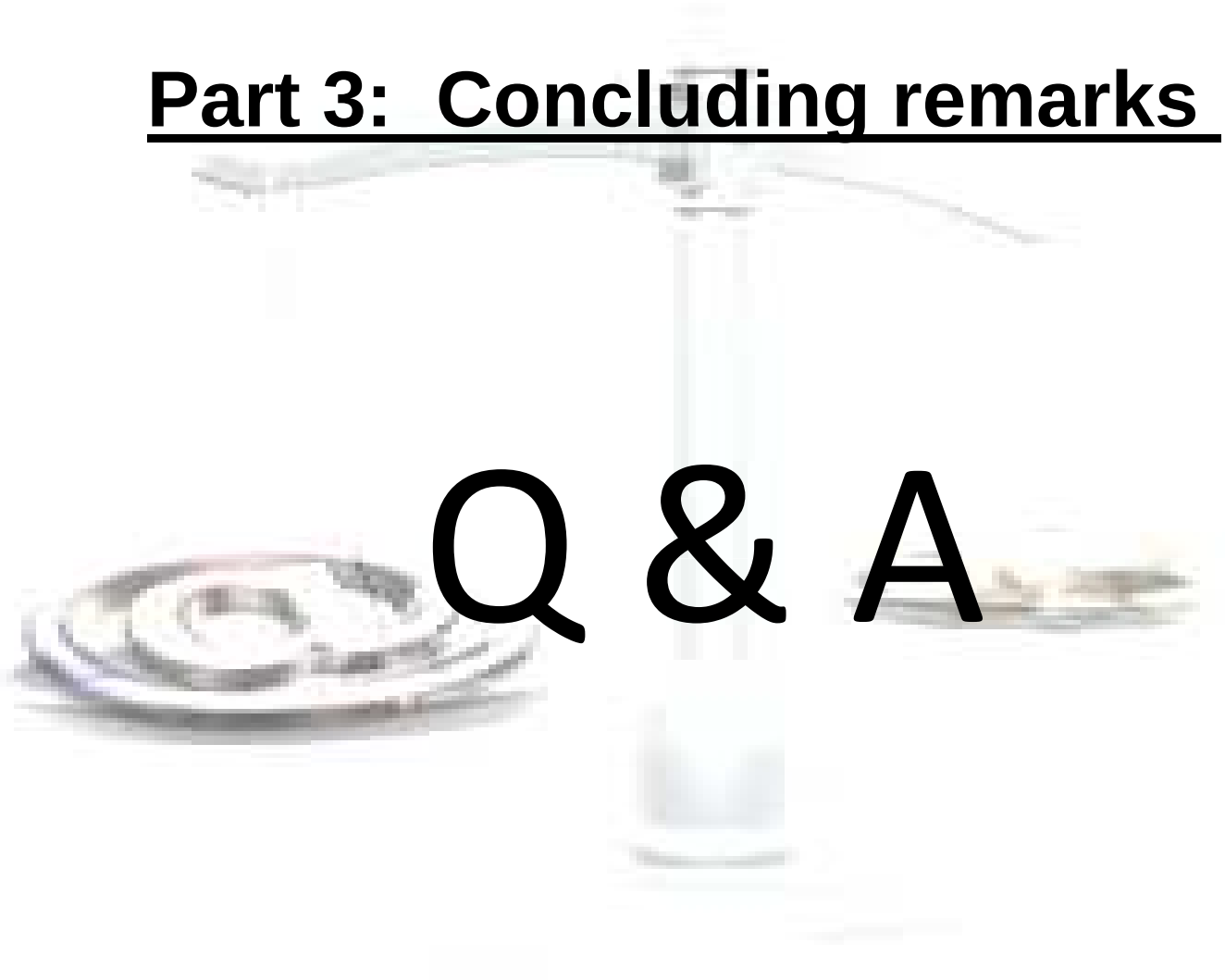
38.Hosting Provider

39.Caching Provider

40.Hyperlinks Provider

41.Search Engine Provider

Part 3: 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