Workshop on effective cybercrime legislation in Eastern Africa

Dar es Salaam, TANZANIA
22 -24 August 2013,
The Peacock Hotel,
Dr Mohamed Chawki , Dr Maicibi Alhas and Attorney Sizwe Lindelo Snail Ka Mtuze
TABLE OF CONTENTS

Part 1: Council of Europe response to cybercrime

Part 2: African response to cyberlaw

Part 3: South Africa’s response to cybercrime

Part 4: Tanzanian response to cybercrime

Part 5: Concluding remarks
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.
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.
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.
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.
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.
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.
Part Two: African responses to cyberlaw
Economic Community of West African States (ECOWAS)

The Supplementary Act on Cyber Crime

DIRECTIVE CIDIR. 1/08/11 ON FIGHTING CYBER CRIME WITHIN 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
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
* 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

• SUBSTANTIVE AND PROCEDURAL RULES on CYBER CRIMES ENFORCEMENT AND PROSECUTION

* ONLINE MARKETING

* INTERMEDIARIES

• 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.

- “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 of regional 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
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 injuria (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 its immaterial form) and forgery to the online forms of these offences.
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.
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)
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.
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).

The 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.
Although *S v Ndiki [2007] 2 All SA 185 (Ck)* dealt with the admissibility of computer print-outs before the ECT Act, Van Zyl J made many relevant remarks pertaining to the admissibility of electronic evidence. The following remark was made by Van Zyl J in *S v Ndiki*:

‘It seems that it is often too readily assumed that, because the computer and the technology it represents is a relatively recent invention and subject to continuous development, the law of evidence is incapable or inadequate to allow for evidence associated with this technology to be admissible in legal proceedings. A preferable point of departure in my view is to rather closely examine the evidence in issue and to determine what kind of evidence it is that one is dealing with and what the requirements for its admissibility are’ [53].
Watney submits against the background of the Ndiki-case, one will have to look at the facts of a particular case and determine what type of evidence the data message represents.

Once the type of evidence has been determined, a two-phased procedure will be applicable namely:

(i) to determine the admissibility of the electronic evidence during a trial-within-a-trial and if the evidence is found to be admissible

(ii) the evidential weight of the evidence has to be determined.

Watney citing Hoffman states that questions relating to admissibility of electronic evidence must be decided in a ‘trial within a trial’. ‘A trial within a trial’ (Hoffman (2006) 1).
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,
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 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)
Part Three: South African response to e-commerce –
The Electronic Communications and Transactions Act,
Act 25 Of 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.
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).

- 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.
In the case of *R v Douvena (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported)* the Court had to decide whether an accused employee GM Douvena of Rentmeester Assurance Limited (Rentmeester) **was guilty of a contravention of section 86(1)** (read with sections 1, 51 and 85) of the ECT Act.

It was alleged in this case that the accused, on or about 21 January 2003, in or near Pretoria and in the district of the Northern Transvaal, intentionally and without permission to do so, gained entry to data which she knew was contained in confidential databases and/or contravened the provision by sending this data per e-mail to her fiancée (as he then was) to ‘hou’ (keep).

**The accused was found guilty of contravening section 86(1) of the ECT Act and sentenced to a R1 000 fine or imprisonment for a period of three months.**


**Hacking has now been entrenched in our law in s86 (1) of the ECT which makes any unlawful access and interception of data a criminal offence.** This also applies to unauthorized interference with data as contained in s86 (2) of the ECT.
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 guilty 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 guilty 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).
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)
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)
Legal Aspects impacting on Law enforcement of Cyber crimes
(Procedural aspects of Cyber crimes)

Admissibility and Evidential Weight of data Messages (ECT Act S 15)

- After much legal uncertainly as to the admissibility of a printout in Court in terms of the Old Computer Evidence Act, Section 15 of the ECT, now states that the rules of evidence must not be used to deny admissibility of data messages on grounds that it’s not in original form. A data message made in the ordinary course of business, or a printout correctly certified to be correct is admissible evidence. It constitutes rebuttable proof of its contents when it is produced in the form of a print-out.\[1\]

- The Act now states that Data messages shall be admissible giving due regard to reliability of manner of storage, generation and communication, reliability of admission manner of maintenance of message, manner in which originator is identified, and any other relevant factor. In other words the Act creates a rebuttable presumption of that data messages and or printouts thereof are admissible in evidence.\[2\]

\[1\] Also see the case of S B Jafta v Ezemvelo KZN Wildlife (Case D204/07) where a e-mail used to accept an employment contract was regarded as conclusive proof that the said employment had been accepted.

\[2\] also see the controversial case of S v Motata where electronic information (data in the form of images and sound) from cell phone was admitted into evidence in a trial within a trial (the case has yet to be concluded)
The Act now states that Data messages shall be admissible giving due regard to reliability of manner of storage, generation and communication, reliability of admission manner of maintenance of message, manner in which originator is identified, and any other relevant factor. **Section 15(4) of the ECT Act** provides that data message made by a person in the ordinary course of business, or a certified copy, printout or extract from such data message “is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.”

The copy, printout or extract is to be certified to be correct by an officer in the service of the person making the data message. In other words the Act creates a **rebuttable presumption** of that data messages and or printouts thereof are admissible in evidence. (See also the controversial case of *S v Motata Johannesburg District Court case number 63/968/07 (unreported) at 622*, where electronic information (data in the form of images and sound) from a cellphone was admitted into evidence in a trial within a trial)).
Lessons learnt from Counsel of Europe Convention on Cybercrime and the AU Convention

Counsel of Europe Convention on Cyber Crime

The Council of Europe’s Convention on Cyber crime (November 2001) which South Africa has signed but did not ratify the Convention has influenced the drafting. 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.”  

Lessons learnt from Counsel of Europe Convention on Cybercrime and the AU Convention cont.

**AU Convention**

- Attempt to develop an “African” all-round Cyber security, E-commerce and Cyber Cybercrime framework for “African” states
- No real added value to Cybercrime legislation in Africa but Ideal of African Convention is a steps in the right direction for the African Continent
- Council of Europe’s Convention on Cyber crime (November 2001) is often if not sole source of Cybercrime soft law for most African states
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.
Regulation of Interception of Communications and Provision of Communication-related Information Act - RICA cont.

This means in simple terms that it is unlawful and therefore prohibited to:

1. **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

2. **Intentionally monitor any conversations or communications by means of a monitoring device** so as to gather confidential information concerning any person, body or organisation (Cohen 2001: 2–4).

• One must note that the attempt is as unlawful as the actual act of actually intercepting and monitoring a data communication

• Section 5(1) of RICA provides that any person may authorise or give anyone else “written” permission to monitor or intercept any data communication unless it is for the purposes of unlawful conduct.

Modiba (2003: 366) suggests that if the employer in the workplace wants prior written consent to intercept and monitor communication devices at the workplace he should insist that the employee sign a document confirming such consent.
Protection of Personal Information Bill – POPI

- The proposed Act applies to personal information collected, stored and disseminated by automated and non-automated processes. It generally applies to South African businesses processing personal information in the context of their trade activities.

- The proposed Act will for instance not apply to the processing of personal information in the course of a purely personal or household activity. It further applies to the processing of personal information by/for businesses established outside South Africa using automated or non-automated means situated in South Africa. The proposed Act binds the State.

- The Act will also establish a body known as the Information Protection Commission, of which the chairperson and two ordinary members will be appointed by the State President. The duties of the Commission will include education, monitoring compliance and dealing with complaints.

- (a) Principle 1: Processing limitation:
- (b) Principle 2: Purpose specific:
- (c) Principle 3: Further process limitation:
- (d) Principle 4: Information quality:
- (e) Principle 5: Openness:
- (f) Principle 6: Security safeguards:
- (g) Principle 7: Individual participation:
- (h) Principle 8: Accountability:

• Chapter 3, Part B deals with the prohibition on the processing of “special personal information”. In this regard, in principle, it is prohibited to process personal information concerning a person’s religion or philosophy of life, political persuasion, health or sexual life etc, except where the data subject has given his/her explicit consent to the processing of the information. However, Part B further sets out various exemptions to this general prohibition on the processing of special personal information as described. For instance, the prohibition on processing of personal information relating to a person’s health or sex life will not apply where the processing is carried out by medical professionals and it is necessary for proper treatment.

• Chapter 4 provides for exemptions from the 8 information protection principles referred to above, and set out fully Chapter 3, Part A. In this regard, the Commission may authorise a responsible party (data collector) to process personal information, even though that processing would otherwise be in breach of an information protection principle, if the Commission is satisfied that, in the special circumstances of the case:

• (a) the public interest in that processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from that processing; or

• (b) that processing involves a clear benefit to the data subject or a third party that outweighs any interference with the privacy of the data subject or third party that could result from that processing.

• Any person may submit a complaint to the Commission alleging that any action is, or appears to be, for instance, a breach of any information protection principle. A complaint may be made either orally or in writing. A complaint made orally must be put in writing as soon as reasonably practicable.

Part 4: 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)
Part 4 : Tanzanian responses to cybercrime ( cont. )


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 cybercrime 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 )
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.
Part 4: 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.
Part 4: 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
Part 4: 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
Part 4: Tanzanian responses to cybercrime (cont.)

Overview of the Bill

Aspects of Jurisdiction

• 25. Jurisdiction
• 26. Extradition

Electronic Evidence

• 27. Admissibility of Electronic Evidence
Part 4: 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
Part 4: 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 5: Concluding remarks

Q & A