Challenges of Implementing Cyber laws in Uganda

On 20th June 2013, I delivered a presentation on “challenges of implementing cyber laws in Uganda”, at the Uganda Law Society CLE seminar.

Government of Uganda passed three critical laws, namely (i) Computer Misuse Act, 2011; (2) Electronic Transactions Act, 2011; and (3) Electronic Signatures Act, 2011. Taken together, they are referred to the Uganda Cyber Laws.

According to computer misuse act’s long tittle (preamble), ‘it provides for the safety of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.”

The need for cyber laws in Uganda and elsewhere in the world is four fold:

- Tackle cyber crimes
- Address intellectual property rights and copyrights protection
- Enable e-commerce and facilitate trade
- Regulate the use of electronic signatures to ensure security (confidentiality, integrity and availability) of communication and non-repudiation

Computer Misuse refers to unauthorized access to private computers and network systems, deliberate corruption or destruction of other people’s data, disrupting the network or systems, introduction of viruses or disrupting the work of others; the creation and forwarding of defamatory material, infringement of copyright, as well as the transmission of unsolicited advertising or other material to outside organizations. It includes all the activities that undermine computer security – affect the integrity, confidentiality and availability of computer systems.

A digital signature is an electronic signature used to confirm the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate (reject) it later.

A digital signature is NOT a scanned copy of your physical signature. An electronic signature on the other hand, “is a typed name or a digitized image of a handwritten signature. Consequently, electronic signatures (signatures) are very problematic with regards to maintaining integrity and security, as nothing prevents one individual from typing another individual's name. Due to this reality, an electronic signature that does not incorporate additional measures of security (the way digital signatures do, as described above) is considered an insecure way of signing documentation.” The Electronic Signature Act, 2011 laws of Uganda is intended to address the challenges associated with electronic signatures by providing for the use of digital signatures in commercial transactions.

Electronic Transaction means a transaction of either commercial or non-commercial nature communicated electronically by means of data messages and includes the provision of information and e-government services.

- makes provision for the use, security, facilitation and regulation of electronic communications and transactions;
- encourages the use of e-Government service, and
- provides for related matters.

The Electronic Transaction Act addresses the following issues, among others:

- Enforceability and form requirements for electronic contracts.
- Regulation of domain names which are a new form of digital property.
- Privacy protection for consumers and users of electronic media.
- Establishment of a regulatory framework that is compliant with the rapid technological changes.
- Determining the levels of responsibility in tort and contract attached to enhanced abilities of machines.

- Classification of trade in information products especially where the relationship between the producer and ultimate consumer is remote.

Status of implementation of cyber laws in Uganda

The Ministry of Information and Communications Technology (MoICT) of Uganda has been at the forefront in the implementation of cyber laws. A lot has been achieved since 2011, when the cyber laws were enacted.

- The Permanent Secretary in MoICT constituted a *Team of Experts (ToE) or* Technical Task Team (TTT) for the operationalization of the three Cyber laws.
- The composition of the ToE was drawn from several government agencies including MoICT, Ministry of Justice and Constitutional Affairs (MoJCA), National Information Technology Authority of Uganda (NITA-U), Uganda Revenue Authority (URA), Uganda Law Reform Commission (ULRC), Uganda Police Force (UPF) and the Ministry of Internal Affairs (MoIA), among other institutions.
- Some of the members of the team of experts undertook benchmark studies

Scope of work for ToE:

- Drafted the Ministerial Gazette for the commencement of the Cyber Laws; and
- Oversaw and guided the process of developing attendant ***Regulations*** for the Electronic Signatures Act and the Electronic Transactions Act;
  - *process on-going* – stakeholder consultation.

**The Computer Misuse Act was found 'self-prosecuting' and no attendant regulations were considered*.

- Awareness training among all stakeholders and the general public;
- Continued engagement with private sector to identify any upcoming issues and gaps in the laws (*e.g. Data Privacy, Intellectual Property, electronic document retention, etc.)*

- Developing a national information security strategy to:
    - Establish Computer Incident Response Team (CIRT)
    - Creation of Directorate of IT security within NITA-U – already created

The challenges

1. Lack of the *right skills* and *tools* in to investigate computer crimes
    – You need a team of young experts
    – You need *powerful tools* to process evidence
    – You need on-going training to beef up capacity
    – Less bureaucracy to ensure you are up to date with new developments in IT
2. Mechanisms of control
    – There are missing mechanisms of control
    – Lots of parties and networks are involved in communication
    – Anonymous communications e.g. anonymous cloud emails involved in crime e.g. use of internet cafes, wireless networks, dynamic IPs internet access, etc…
3. New procedures
    – Need to develop procedures for digital evidence
    – Privacy vs. lawful interception and data retention. How sure are we that private data might not be abused?
    – Use of encryption technology make it difficult to investigate
4. Education & training

- Need for user awareness
- Low understanding of cyber laws among key stakeholders
- Very few cyber crime training experts – local capacity is not being developed and empowered to help government
- High levels of public ignorance
- Generally low levels of acceptability of cyber laws in courts – it is a threat to '**legal experience**.'

5. Lack of harmonization of laws
6. Lack of willingness to change the status quo
    - Stakeholder collaboration and concerted efforts is yet to be achieved
    - Implementation in highly centralized government institutions
    - Approach is lacking --- old people being trained instead of young graduates
7. Evolving and complex
    - Cyber initiatives are implemented by a single vendor, with single experts. That is bad for national security e.g. CERT
    - No capacity to establish cyber weaponry yet – a 10-20 year project
    - Formal training with low cost alternatives not yet sought, eg. EC Council
8. A catch up game; no clear strategy
    - Cyber is evolving and complex
    - It is not about few experts. Need all stakeholders aware of the challenge
    - Cyber security does not work with copy and paste – you set your own agenda

References

E-government and Cameroon cyber security legislation, 2010 by Patricia Asongwe

Ministry of ICT of Uganda; website accessed on 19th June 2013

Cyber laws of Uganda, 2011

Ministry of ICT presentations and resources.

References and further information on how digital signatures work, visit the following link.

http://www.arx.com/digital-signatures-faq; accessed on 24th June 2013.