Cyber laws in Uganda
Implementaiton challenges
“Uganda Cyber Laws” are three currently:

2. Electronic Transactions Act, 2011
3. Electronic Signatures Act, 2011
Are you safe online..

If your privacy was breached, do you have the tools and expertise to prove it?

Photo credit: UNCTAD photo
The need for cyber laws:

1. Tackling cyber crimes
2. Intellectual property rights and copyrights protection
3. Enable e-commerce and facilitate trade
4. Regulate the use of electronic signatures
“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 classified data or other material to outside organizations... etc... any crime involving a computer.”
“Computer Misuse” includes the ‘access, downloading, displaying, viewing and manipulation of offensive or obscene materials’.

This would include pornography or scenes of violence. In extreme cases this may include the criminal act of downloading or displaying indecent photographs of children.
“Computer Misuse” includes the ‘access, downloading, displaying, viewing and manipulation of offensive or obscene materials’.

This would include pornography or scenes of violence. In extreme cases this may include the criminal act of downloading or displaying indecent photographs of children.
“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.
The definition of “Computer Misuse” includes the ‘downloading, displaying, viewing and manipulation of offensive or obscene material’. This would include pornography or scenes of violence. In extreme cases this may include the criminal act of downloading or displaying indecent photographs of children.
Computer Misuse Act, 2011

• Provides for the safety and security of electronic transactions and information systems;
• Prevents unauthorized access, abuse or misuse of information systems, including computers
• Prevents unauthorized modification and e-crime
• Preservation orders... etc
“Electronic Signature” means data in electronic form, affixed thereto or logically associated with, a message, which may be used to identify the signatory in relation to the data message and indicate the signatory’s approval of the information contained in the data message.
“Digital Signature” means a transformation of a message using an cryptography such that a person having the initial message and the signer’s public key can accurately determine:

i. whether the transformation was created using the private key that corresponds to the signer’s public key; and

ii. whether the message has been altered since the transformation was made.
The Electronic Signatures Act provides for:

- use of electronic signatures, and regulation
- criminalization of unauthorized access and modification of electronic signatures,
- determination of minimum requirements for functional equivalence of electronic signatures
Electronic signature...

Object ctd...

• modernization and harmonization of the laws relating to computer generated evidence, and

• amendments of the current laws to provide for admissibility and evidential weight of electronic communications.
“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.
Electronic Transactions Act, 2011

• 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.
Electronic Transactions

• 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.
Electronic transactions...

- 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.
Implementation of cyber laws and challenges in Uganda
• The PS, MoICT constituted a Team of Experts for the operationalization of the three Cyber laws.
• The composition of the ToE was drawn from: MoICT, MoJCA, NITA-U, URA, ULRC, UPF & MoIA
Cyber laws implementation

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 has been on-going – stakeholder consultation.

*The Computer Misuse Act was found ‘self-prosecuting’ and no attendant regulations were considered.
Cyber laws implementation...

• 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.)
Cyber laws implementation...

• Developing a national information security strategy to:
  o Establish Computer Incident Response Team (CIRT)
  o Creation of Directorate of IT security within NITA-U – already created
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
   - You need inter-agency corporation to strengthen capabilities
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
Challenges...

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.’
Challenges...

5. Lack of harmonization of laws

<table>
<thead>
<tr>
<th>Electronic transactions and signatures</th>
<th>Data protection and privacy</th>
<th>Consumer protection</th>
<th>Computer crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burundi</td>
<td>None</td>
<td>Draft</td>
<td>None</td>
</tr>
<tr>
<td>Kenya</td>
<td>Draft</td>
<td>Enacted</td>
<td>Draft</td>
</tr>
<tr>
<td>Rwanda</td>
<td>Draft</td>
<td>Enacted</td>
<td>Partial</td>
</tr>
<tr>
<td>United Republic of Tanzania</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Uganda</td>
<td>Draft</td>
<td>Enacted</td>
<td>None</td>
</tr>
</tbody>
</table>

Source: UNCTAD

Data protection is a critical law for all of us! Where is it?
Challenges...

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

Involvement of the private sector is inadequate.
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

People are still looking at small things, yet things have changed.
Challenges...

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

We must be in this together all the way. We need to empower local capacity to offer the solutions. That is sustainable model in any country.
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.
Our values for your success

We take pride in doing the **right** thing, rather than what is **right for the profitability** of SCL.

Thank you!
Summit Consulting
[www.summitcl.com](http://www.summitcl.com)
0414231136
premium@summitcl.com