Cybersecurity and Privacy Governance

Pria
.za
.africa
Encoding Cybersecurity Norms and Principles - Issues, Developments, and Approaches
Cybersecurity Governance

- Political Will and Leadership
- Institutional Governance
- Infrastructure and Equipment – Capability, Interoperability, Standards, Protocols
- Skills and Training – Capability
- Incident Response – Capability and Maturity
- Resources and Budget Allocations
- International, National, Sectoral and Inter-sector co-operation
- Enforcement – Legal Frameworks that identify offences and sanctions and co-operation with justice systems
- State Powers – Surveillance, Interception, Search, Seizure
- International Powers - Surveillance, Interception, Search, Seizure
Cybersecurity Governance

- UNCITRAL
- Budapest Conv.
- EU
- ITU
- UNCTAD
- UNECA
- AU
- SADC
- EAC
- ECOWAS
- Others: OECD, WIPO
- National

Globally, there are multiple initiatives, efforts, models at international, national and regional levels. Particularly to:

- Promote harmonised, global, coherent and co-ordinated approaches;
- Address legal barriers to electronic transactions; and
- Promote trust and confidence in (international) electronic transacting methods.
Africa Acronyms

Initiatives by, for instance:

- AU (African Union)
- SADC (the Southern African Development Community)
- UNECA (Economic Commission for Africa)
- UNCTAD (Commission Trade and Development)
- ECOWAS (Economic Community of West African States),
- EAC (East African Community)
UNCITRAL (1996)

- MLEC – Model Law on Electronic Commerce
  - Promote greater consistency in national and regional approaches.
  - Create a more secure legal environment for electronic commerce for providing a model reference for legislators
- Implemented by several countries
- In Africa – implemented by South Africa, Cape Verde, Mauritius
- MLES – Model Law on Electronic Signatures
Encoding Cybersecurity Norms and Principles – African Union Convention
According to the Website:

The Draft Convention gives effect to a Resolution of the last session of the Assembly of Heads of State and Government of the African Union, and seeks to harmonize African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion and cyber crime control.

In pursuance of the principles of the **African Information Society Initiative (AISI)** and the **African Regional Action Plan for the Knowledge Economy (ARAPKE)**, the Draft Convention is intended not only to define the objectives and broad orientations for the Information Society in Africa, but also to strengthen existing legislations in Member States and the Regional Economic Communities (RECs) on the Information and Communication Technologies.

It defines the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa.

It lays the foundation for an African Union-wide cyber ethics and enunciates fundamental principles in the key areas of cyber security. It also defines the basis for electronic commerce, puts in place a mechanism for combating intrusions into private life likely to be generated by the gathering, processing, transmission, storage and use of personal data and sets broad guidelines for incrimination and repression of cyber crime. Its adoption would capitalize African and international experiences in cyber legislations and speed up relevant reforms in African States and the RECs.

Source/ Read More: [http://au.int/en/cyberlegislation](http://au.int/en/cyberlegislation)
The objective of this Convention was to propose the adoption at the level of the African Union, a Convention establishing a credible framework for cybersecurity in Africa through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime.
Information security impacts on the security of the digital and cultural heritage of individuals, organizations and nations;

The vulnerability in the normal functioning of institutions can compromise the survival and sovereignty of States;

Addressing cyber security calls for clear-sighted political will to define and implement a strategy for development of digital infrastructure and services (eservices) and articulate a coherent, effective and controllable multi-disciplinary cyber security strategy.
AU Draft Convention - Challenges

- Achieve a level of **technological security adequate enough** to prevent and effectively control technological and informational risks;
- Build an information society that respects **values**, protects **rights and freedoms**, and guarantees the security of the property of persons, organizations and nations;
- Contribute to the knowledge economy, guarantee equal access to information while stimulating the creation of **authentic knowledge**;
- Create a climate of confidence and trust, that is:
  - **Predictable** in terms of prevention and resolution of disputes; and evolving because it takes into account continued technological evolution;
  - **Organized**: covering the relevant sectors;
  - **Protective**: of consumers and intellectual property (civil and penal) of citizens, organizations and nations;
  - **Secured**: striking proper balance between legal and technological security.
Provisions relating to legality of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combatting cybercrime.
Provisions: too much power to the government, particularly in accessing private information. Processing of personal data and sensitive data without consent of the owner for the purpose of state security and public interest could be misused. Broad and unchecked powers to “investigating judges”. Such powers include the power to issue search and seizure warrants for any electronic records. Prosecution of anyone seen to promote “theories” of racism and xenophobia. Only approved e-commerce payments may be used in a country. This requirement would force popular global platforms, such as Paypal, to seek regulatory approval, considerably slowing down the rate at which they could spread their services across Africa.
Encoding Cybersecurity Norms and Principles – Regional Model Approaches
SADC Cybersecurity, 2012

- SADC Model Laws - adopted at a SADC Ministerial meeting in Botswana in 2012
  - SADC Model Law on Data Protection, 2012
  - SADC Model Law on Cybercrime, 2012
  - SADC Model Law on Electronic Transactions, 2012
- Commenced with a regional and international assessment
- Technical Assistance was offered by ITU for the drafting of the Model Laws and in-country transpositions
- SADC countries to harmonise their legislative framework with Model Laws
Establishment of Harmonized Policies for the ICT Market in the ACP

DRAFT Southern African Development Community (SADC) MODEL LAW
ON ELECTRONIC TRANSACTIONS AND ELECTRONIC COMMERCE

Support for Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA)
ECOWAS

- Directive on Fighting Cybercrime, 2009
- Incorporation of legal framework for Member States
- Emphasis on cybercrime, data protection, search and seizure
EAC

- Enabling legal framework as a critical factor: e-transactions, cybersecurity
- Harmonized regional and national legal frameworks
- Creation of an EAC Task Force (2008)
- The EAC legal framework for Cyber Laws (Phase I) covering electronic transactions; electronic signatures and authentication, cyber crime, and data protection and privacy have been adopted by the Council of Ministers (2012)
“The East African Development Strategy (2011/12 – 2015/16) proposes the key drivers for the realization of the EAC regional integration agenda in the next five years to include, among others, creation of a strong legal framework (...)

The development of cyber laws in the region is critical to underpin the realisation of full potentials in regional e-commerce, electronic financial transactions and business processes outsourcing.”

Hon. Musa Sirma, Chairperson of the Council of Ministers of the East African Community and Minister for East African Community, Republic of Kenya, at the occasion of the presentation of the budget of the EAC for the financial year 2012/2013 to the legislative assembly
<table>
<thead>
<tr>
<th>Country</th>
<th>eContracting/adm &amp; evidence</th>
<th>Data privacy</th>
<th>Consumer protection</th>
<th>Copyright</th>
<th>Domain name mechanisms</th>
<th>Internet &amp; mobile payment systems</th>
<th>Cyber crime &amp; cyber-security</th>
<th>Content control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burundi</td>
<td>Pending</td>
<td>Pending</td>
<td>Pending</td>
<td>✓ (2005 Act)</td>
<td>Not reported</td>
<td>No regulations</td>
<td>(2009 Act &amp; Bill)</td>
<td>Pending</td>
</tr>
<tr>
<td>United Republic of Tanzania</td>
<td>No regulations</td>
<td>Partial under 2010 Law</td>
<td>No regulations</td>
<td>✓ (1999 Act)</td>
<td>No regulations</td>
<td>No regulations</td>
<td>No regulations</td>
<td>Partial under 2010 Law</td>
</tr>
</tbody>
</table>

*Source: UNCTAD forthcoming study on cyber-legislation in EAC.*
ICT Ministers call for harmonized policies and cyberlegislations on Cybersecurity

Khartoum Ministerial Declaration - emphasises the need for African countries to accelerate the formulation of cyberlegislation...

ECA Press Release 144/2012

Addis Ababa, 05 September 2012 (ECA) - The fourth African Union Conference of Ministers in charge of Communications and Information Technologies opened today in Khartoum, Sudan, under the auspices of His Excellency the President of the Republic of Sudan, Field Marshal Omer Hassan Ahmed Albashir.

Addressing the Ministers and invited guests during the opening ceremony, President Albashir stated that African countries need to "enact the required legislation for ICT related investments, build the capacity of the youth and put in place incentives to promote science and technology in Africa".

During her opening remarks, Ms Aida Opoku Mensah, Director of ICT, Science and Technology Division of the United Nations Economic Commission for Africa reminded participants that "while Internet users have more than doubled to 2.5 billion worldwide since 2005, Africa which is home to 14 percent of the world’s population accounts only for 6.2 percent of the world’s internet users."

Ms Opoku-Mensah also drew the attention of delegates to the "African Union Convention on Cybersecurity developed with the technical support of ECA and which will require approval of the Ministers for further consideration by African Heads of States and Governments."

Also speaking at the opening ceremony, Ms Elham Ibrahim, Commissioner for Infrastructure and Energy at the African Union Commission reaffirmed that "ICTs will transform Africa and will drive the continent’s renaissance."

At the end of the two days Conference, ICT Ministers will adopt the Khartoum Ministerial Declaration which emphasizes among other issues, the need for African countries to accelerate the formulation of cyberlegislations; implement the recommendations of the feasibility study on the African Space Agency; proactively participate and agree on common positions on global issues related to Internet Governance as well as accelerate the transition from analogue to digital terrestrial broadcasting.
Experts adopt Declaration of Addis Ababa on harmonization of cyber legislation

ECA Press Release No. 103/2012

Addis Ababa, 22 June 2012 (ECA) - Over 80 experts from Eastern, Southern and Northern Africa regions concluded a three day consultative workshop with the adoption of the Addis Ababa Declaration on harmonization of cyber legislation in Africa. The declaration is bolstered by a series of recommendations to the African Union Commission and the United Nations Economic Commission for Africa.

The recommendations focused on taking into account the views of Member States in finalizing the draft AU Convention on Cyber Security; intensifying awareness-raising and organizing tailored capacity building programmes on cyber legislation to law enforcement institutions and agencies. Further, the experts urge Regional Economic Communities to support harmonization of cyber security policies and legislation, among others.

Speaking at the closing session, Ms. Aida Opoku-Mensah, Director of the ICT, Science and Technology Division (ISTD) lauded the participants for their “collective support and commitment to the declaration adoption process”.

Also speaking in the concluding session, Ms. Eskedar Nega, Programme Officer at the ICT, Science and Technology Division of ECA reflected on the conference discussions and highlighted how ECA will take the outcomes of the conference forward in its upcoming work and set deadlines for each activity.

Ms. Opoku Mensah emphasized that the road map would feed into that the Convention, which will be tabled at the fourth Conference of Ministers in September 2012.

The workshop was organized by the Economic Commission for Africa and the African Union Commission in collaboration with Regional Economic Communities from 20-22 June at the United Nations Conference Centre in Addis Ababa. Over 80 experts in cyber legislation from ICT, justice, interior and Commerce ministries, law enforcement agencies, policy makers, including experts from legislative bodies, courts, the United States Department of Justice, Microsoft and the academia in the sub-region were in attendance.

Issued by:
ECA Information and Communication Service
P.O. Box 3001
Addis Ababa Ethiopia

AFRIncert

- AfriCert is an organisation dedicated to promoting cyber security in Africa;
- It is a forum of computer incident response teams that aims to propose solutions to challenges within the African Internet Ecosystem;
- These task teams can be found in eleven countries, namely; Burkina Faso, Cameroon, Côte d’ivoire, Egypt, Ghana, Kenya, Mauritius, Morocco, South Africa, Sudan, and Tunisia.
INTERNET OF THINGS

HOW THE INTERNET OF THINGS IS HAVING AN IMPACT IN AFRICA

The Internet of Things has already made an impact on Africa as the emergence of connected hardware takes off. Every area of life stands to benefit from the innovations and efficiencies possible in a fully connected world.

“The IoT is a reality that cannot be ignored,” says Matthew Blewett, Chief Investment Officer at Business Connexion. “It’s changing the way companies operate, forcing them to redefine their business processes to keep up with their competitors.”

Furthermore, it will force many businesses to completely redefine their traditional value chains. “By making traditionally physical and disconnected processes digital and connected, products and services can be processed and delivered in completely new ways. This means that traditional value chains are being totally redefined.”

Andy Brauer, Chief Technology Officer at Business Connexion cites Uber as a good example of a business that recognised how an IoT world allowed them to offer a service in a completely new and optimised way. “Uber saw the gap in the personal public transport space. In a connected world with mobile applications, geo-location and GPS..."
BITCOINS

• Watch this video
https://www.youtube.com/watch?v=Um63OQz3bjo
How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers. Wallets are files that provide access to multiple Bitcoin addresses.

Creating a New Address

Each address has its own balance of bitcoins.

It’s tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice’s, her anonymity is protected.

Verifying the Transaction

The miners’ computers are set up to calculate cryptographic hash functions. Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary’s wallet with a balance of newly minted bitcoins.

Transaction Verified

As time goes on, Alice’s transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the week of all the subsequent miners. Such a feat is nearly impossible.
For Consideration

- Political will, drivers, objectives
- Budget – Implementation of cybersecurity institutions, centres and capabilities requires finances
- Impact of cybersecurity readiness on trade (and development)
- Impact on rights and freedoms – privacy, access to information, neutrality of the internet –
- Limitations of rights
- Balancing of interests
Privacy Governance–Regional Model Approaches
GLOBAL CONTEXT: Protect My Data

**IT systems and business tools** (enterprise data, (know your) customer data, profiling, analytics, relationship management, financial, health)

**Digital content ownership** *(eg. social media,)* (users: personal data and intellectual property, rights and obligations)

**Database ownership** (source of data, use of data, rights and obligations)

**Apps ownership** (generation of user data: personal data and intellectual property, rights and obligations)

**Young people** (campaigns involving young people: special treatment of young people)

**Prejudice** from disclosures of personal information: homophobia, criminal records, trade union activity, inaccurate data

**Limitations** on rights to privacy (for state security)

**Tensions** between transparency, access to information and privacy
Digital Content Ownership

• Should the subject of the digital content own the own digital content?

“What are these people going to do with that data? They’re going to target you with an ad which makes you feel a bit queasy. Targeted adverts are not the future.”

Sir Tim Berners-Lee in The Guardian

“If you give [people] the ability to see how [data is] used and you ban its misuse then people are much more happy to open up to their data being used.”

Sir Tim Berners-Lee in The Guardian

"You will not transfer your account to anyone without first getting our written permission"

Facebook's terms and condition
App Ownership

• Data Protection for Apps

• Owners of App are responsible for protection of data collected

• Think of all of the information an App can collect about you
  • Health & sport monitoring apps
  • Medical apps
  • Messaging apps
Privacy in Africa: Are we asking Questions

SIM Card Registration in Africa
Does adequate technological and policy oversight exist to prevent SIM card registries from being misused?
What evidence is there that SIM card registries are actually contributing to crime reduction?
Are law enforcement agencies already using passive surveillance technologies like IMSI catchers?
Are passive surveillance technologies covered under existing legislation concerning the interception of communication?

ENCODING PRIVACY- REGULATORY DEVELOPMENTS AND APPROACHES IN AFRICA
WSIS Principles – Security and Privacy

- The WSIS Declaration of Principles state that strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. In order to achieve this, a global culture of cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders.

Clear association between information society intent and trust imperative
Member States need to:

• Achieve a level of **technological security** adequate enough to prevent and effectively control technological and informational risks;

• Build an information society that respects **values**, protects **rights and freedoms**, and guarantees the security of the property of persons, organizations and nations;

• **Create a climate of confidence and trust**
African Declaration on Internet Rights and Freedoms

• **Concerned** at the continuing inequality in access and use of the Internet, and concerned at the increasing use of the Internet by state and non-state actors as a means of violating the individual’s rights to privacy and freedom of expression through mass surveillance and related activities;

• **Recognizing** the responsibility of States to respect, protect and fulfill human rights of all people, and the responsibility of Information and Communications Technology (ICT) companies and Internet intermediaries to respect the human rights of their users as consistent with the United Nations Guiding Principles on Business and Human Rights;
Privacy and Security

• PRIVACY
• Everyone has the right to privacy online including the right to control how their personal data is collected, used, disclosed, retained and disposed of. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication.
• The right to privacy on the Internet should not be subject to any restrictions, except those which are provided by law, for a legitimate purpose and necessary and proportionate in a democratic society, as consistent with international human rights standards.
Personal Data Protection

• Personal data or information must only be collected and/or processed by States and non-State actors such as access providers, mail providers, hosts and other intermediaries, in compliance with well-established data protection principles, including:
  • personal data or information must be processed fairly and lawfully; secondly, personal data or information must be obtained only for one or more specified and lawful purposes; thirdly, personal data or information must not be excessive in relation to the purpose or purposes for which they are processed; fourthly, personal data or information must be deleted when no longer necessary for the purposes for which they were collected.
Surveillance

- Mass or indiscriminate surveillance of the people and the monitoring of their communications constitutes a disproportionate interference, and thus a violation, of the right to privacy. Mass surveillance should be prohibited by law.
- In order to meet the requirements of international human rights law, lawful surveillance of online communications must be governed by clear and transparent laws that, at a minimum, comply with the following basic principles: first, communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of serious crime; secondly, communications surveillance must be judicially authorized and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation. Thirdly, the application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.
Access to Information

**RIGHT TO INFORMATION**

- Everyone has the right to access information on the Internet. The Internet must continue to facilitate the free flow of information.
- All information, including scientific and social research, produced with the support of public funds should be freely available to all.
Fundamental Right Accessible to Everyone. Access to information is a fundamental human right, in accordance with Article 9 of the African Charter on Human and Peoples’ Rights. It is open to everyone, and no one should be privileged or prejudiced in the exercise of this right on account of belonging to a class or group howsoever defined, and whether in terms of gender, class, race, political association, occupation, sexual orientation, age, nationality, HIV status, and other bases as cited in many African constitutions. It is not required that anyone must demonstrate a specific legal or personal interest in the information requested or sought or otherwise required to provide justification for seeking access to the information.

Privacy And AI in Africa: National Approaches

- Existence of the right to Privacy (Constitutional right?)
- Limitations on Rights
- Data Protection Principles in Law
- Right of Access to Information
- Procedures to fulfil right of access to information
- Regulatory Oversight over Privacy and Access to Information
AfriSIG 2015

- How will Africans contribute to global public policy setting and discourse?
- Lessons learnt in SA
  - In developing countries, issues of mobile uptake and mobile security and privacy are emphasised - mobile payments, spam, digital literacy
  - Accessibility of concepts of information privacy and access to information, cybercrime, e-signatures
  - End user confidence and trust in internet banking in developing countries
  - Confidence and trust in e-government services
  - Institutional effectiveness lessons learnt – resourcing, skills,
  - Developing in-country policy hubs?
Pria Chetty

THANKS, QUESTIONS?

Pria.chetty@endcode.org

EndCode
References

• http://ico.org.uk/for_organisations/data_protection/security_measures)

• http://www.theguardian.com/money/2012/sep/03/do-you-own-your-digital-content


• http://www.bizcommunity.com/Article/75/542/98352.html

• http://ico.org.uk/Youth
THANKS, QUESTIONS?