AfriSIG 2015

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

ENDCODE
Tech. Law. Policy. Africa.

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

ENDCODE
Tech. Law. Policy. Africa.

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)

ENDCODE
Tech. Law. Policy. Africa.

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 Si

ENDCODE
Tech. Law. Policy. Africa.

Encoding Cybersecurity Norms and Principles –African Union Convention

AU

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

AU Draft Convention

- 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

ENDCODE
Tech. Law. Policy. Africa.

AU Draft Convention - Complexities

- 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

AU Convention - Content

Article I – 29

An electronic signature on an electronic written support shall be admissible on the same terms as a signature in manuscript written on paper based matter.

The signature shall use such reliable identification procedure as guarantees its linkage with the act to which it relates.

Such procedure shall be presumed to be reliable until proved otherwise, where:
The electronic signature has been created by a security signature device,
The procedure guarantees the integrity of the act and the signature thereof has been identified.

Article I – 30

An electronic signature created by a security device which the signatory is able to keep under his/her exclusive control and is appended to a digital certificate shall be admissible as signature on the same terms as a signature in manuscript.

ICT - AU Commission

PART II: PERSONAL DATA PROTECTION

Section 1: Terminology

Article II – 1: Definition

For the purpose of this Convention:

1) **Code of conduct** means set of rules formulated by the processing official with a view to regulate the correct use of computer resources, networks and the electronic communication of the structure concerned, and approved by the protection authority.

2) **Consent of data subject** means any manifestation of express, unequivocal, free, specific and informed will by which the person concerned or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing.

3) **Recipient of data** means any person entitled to receive communication of such data other than the person concerned, the data processing official, the sub-contractor and persons who, for reasons of their functions, have the responsibility to process the data.

Provisions relating to legality of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combatting cybercrime

ENDCODE
Tech. Law. Policy. Africa.

AU Convention - Criticism

Africa Needs A Cybersecurity Law But AU's Proposal is Flawed, Advocates Say

BY JOEL MACHARIA | Friday, January 31 2014

ABOVE: The AU may soon pass a cybersecurity bill that advocates say will not offer enough protections (EmbassyEquatorialGuinea/flickr)

Kariuki Kaboro is the co-founder of a local cloud services start-up in Nairobi. He does not use ATM cards as frequently as he used to. In fact, he avoids using them at all when he can. He does not have a fear of technology; as the co-founder of a cloud computing services company, he is more at home with technology than most people would be. His aversion for ATM cards stems from a different source.

Source/ Read More: http://techpresident.com/r

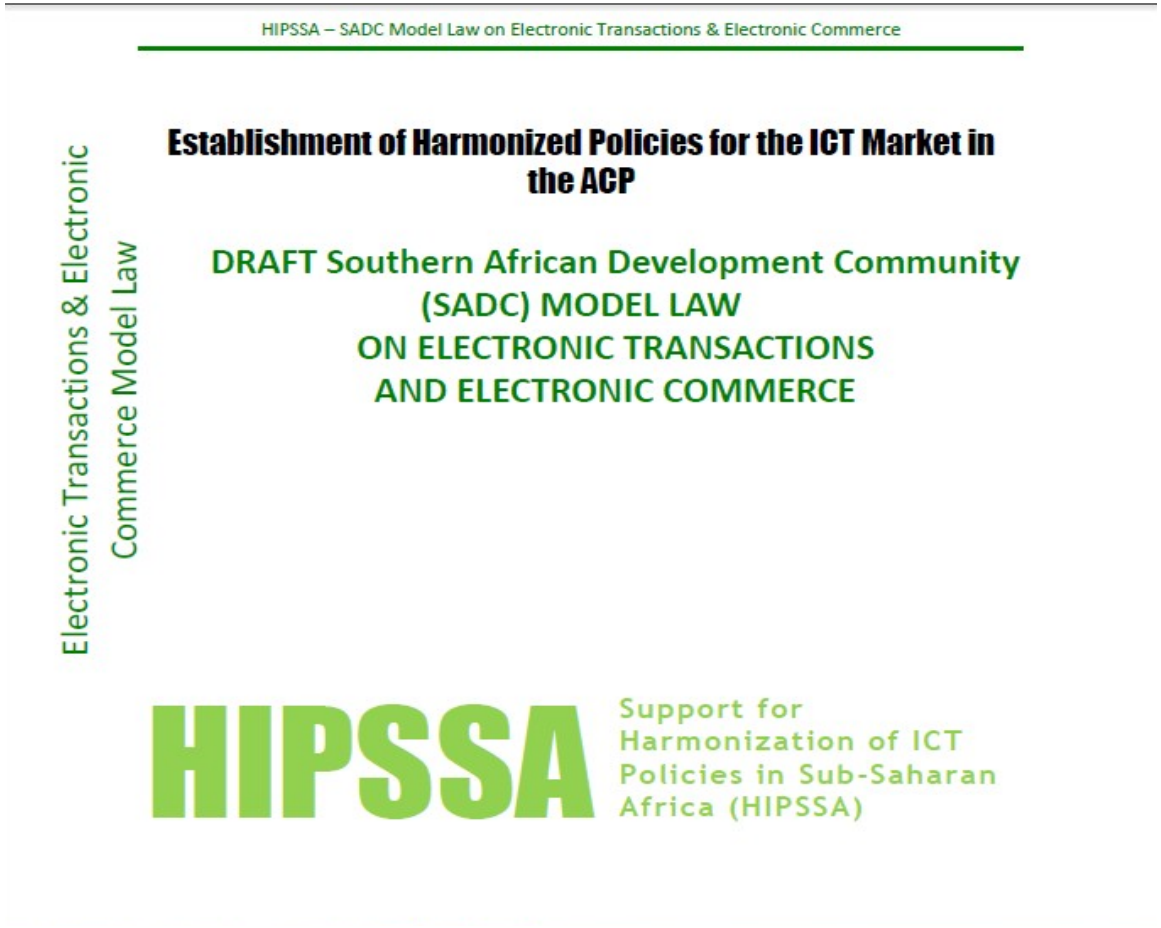
Provisions: too much power to the government, particularly in accessing private information. processing of personal data and sensitive data without consent of the owner for the purpose of state security and public interest could be misused. broad and unchecked powers to "investigating judges". Such powers 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

SADC Model Law on E-Transactions and E-Commerce, 2012



HIPSSA – SADC Model Law on Electronic Transactions & Electronic Commerce

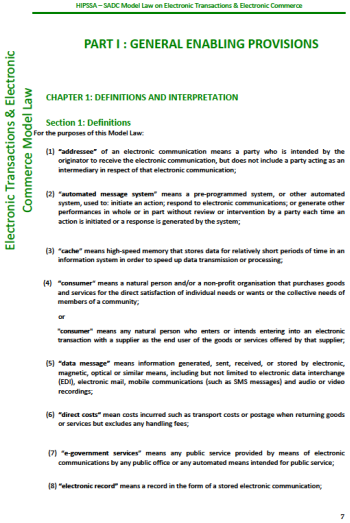
Electronic Transactions & Electronic Commerce Model Law

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

HIPSSA

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



HIPSSA – SADC Model Law on Electronic Transactions & Electronic Commerce

Electronic Transactions & Electronic Commerce Model Law

PART I : GENERAL ENABLING PROVISIONS

CHAPTER 1: DEFINITIONS AND INTERPRETATION

Section 1: Definitions

For the purposes of this Model Law:

(1) **"addressee"** of an electronic communication means a party who is intended by the originator to receive the electronic communication, but does not include a party acting as an intermediary in respect of that electronic communication;

(2) **"automated message system"** means a pre-programmed system, or other automated system, used to: initiate an action; respond to electronic communications; or generate other performances in whole or in part without review or intervention by a party each time an action is initiated or a response is generated by the system;

(3) **"cache"** means high-speed memory that stores data for relatively short periods of time in an information system in order to speed up data transmission or processing;

(4) **"consumer"** means a natural person and/or a non-profit organisation that purchases goods and services for the direct satisfaction of individual needs or wants or the collective needs of members of a community;

or

"consumer" means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

(5) **"data message"** means information generated, sent, received, or stored by electronic, magnetic, optical or similar means, including but not limited to electronic data interchange (EDI), electronic mail, mobile communications (such as SMS messages) and audio or video recordings;

(6) **"direct costs"** mean costs incurred such as transport costs or postage when returning goods or services but excludes any handling fees;

(7) **"e-government services"** means any public service provided by means of electronic communications by any public office or any automated means intended for public service;

(8) **"electronic record"** means a record in the form of a stored electronic communication;

7

ECOWAS

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

EAC

- Regional e-Government Programme adopted by the EAC Council of Ministers (2006)
- Enabling legal framework as a critical factor: e-transactions, cybersecurity
- Harmonized regional and national legal frameworks
- Creation of an EAC Task Force (2008)
- Background: East African Community Secretariat, 'Report of the 2nd EAC Regional Taskforce Meeting on Cyber Laws' (2008) http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf
- 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)

ENDCODE
Tech. Law. Policy. Africa.

EAC

"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

	eContracting/ administration & evidence	Data privacy	Consumer protection	Copyright	Domain name mechanisms	Internet & mobile payment systems	Cyber crime & cyber-security	Content control
Burundi	Pending	Pending	Pending	✓ (2005 Act)	Not reported	No regulations	✓ (2009 Act & Bill)	Pending
Kenya	✓ (2009 Act)	No regulations	✓ (2010 Regulations & proposed Bill)	✓ (2009 Act)	Not reported	No regulations	✓ (2009 Act)	✓ (2010 Regulations)
Rwanda	✓ (2010 Act)	No regulations	✓ (2010 Act)	✓ (2009 Act)	Pending	No regulations	✓ (2010 Law)	✓ (2010 Law)
United Republic of Tanzania	No regulations	Partial under 2010 Law	No regulations	✓ (1999 Act)	No regulations	No regulations	No regulations	Partial under 2010 Law
Uganda	✓ (2011 Act)	Partial	✓ (2011 Act)	✓ (2006 Act)	Pending	No regulations	✓ (2011 Act)	✓ (2011 Act)

Source: UNCTAD forthcoming study on cyber-legislation in EAC.

ENDCODE
Tech. Law. Policy. Africa.

ICT Ministers call for harmonized policies and cyberlegislations on Cybersecurity

Khartoum Ministerial Declaration – emphasises the need for African countries to accelerate the formulation of cyberlegilsation...

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.

Source/ Read More: http://www1.uneca.org/ArticleDetail/tabid/3018/ArticleId/1934/ICT-Ministers-call-for-harmonized-policies-and-cyberlegislations-on-Cybersecurity.aspx

Experts adopt Declaration of Addis Ababa on harmonization of cyber legislation

Print Return

Share / Save

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

Source/ Read More: http://www1.uneca.org/ArticleDetail/tabid/3018/ArticleId/1430/Experts-adopt-Declaration-of-Addis-Ababa-on-harmonization-of-cyber-legislation.aspx

AFRIcert

- 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

13
AUG 2015

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."

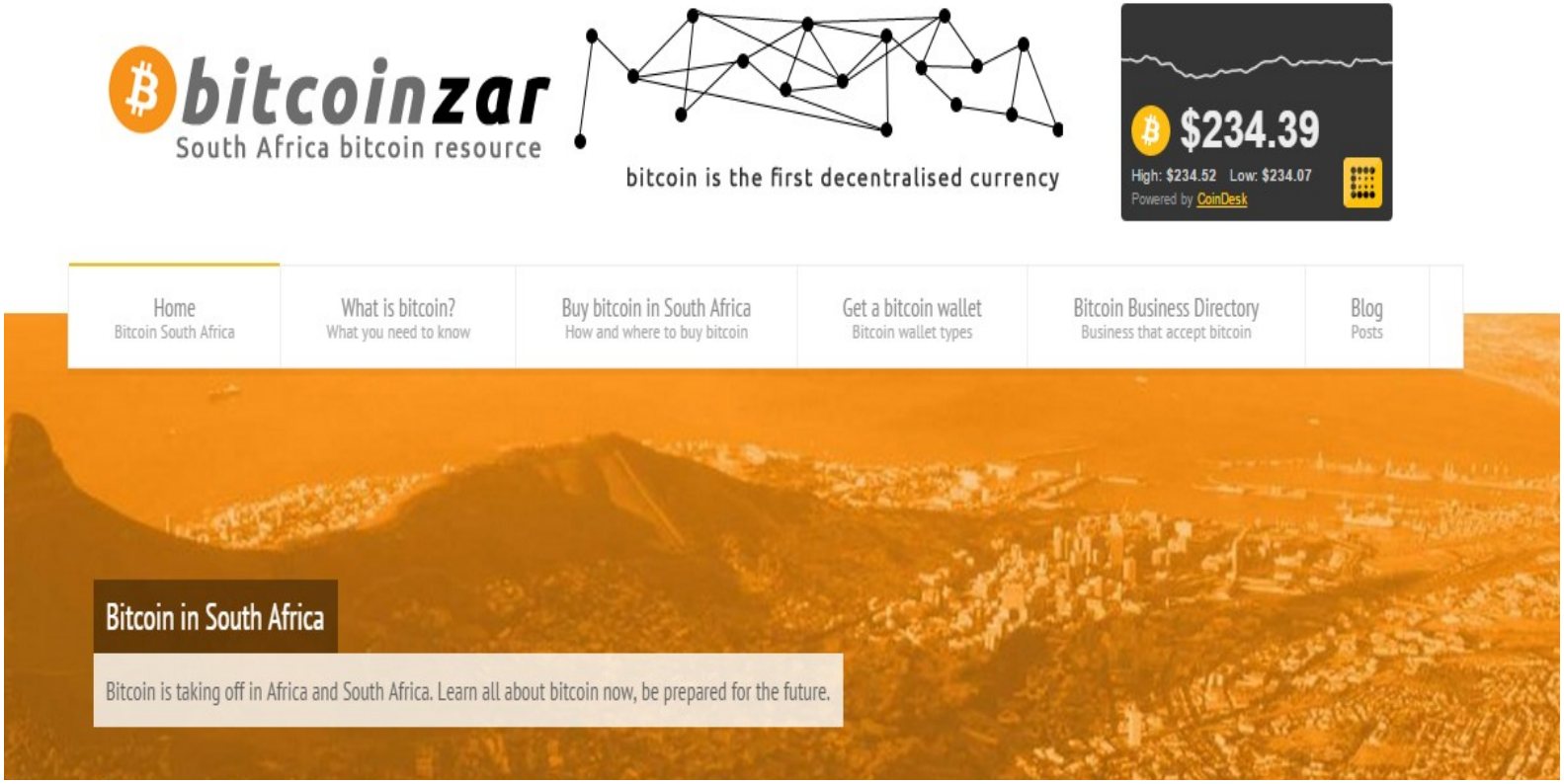
Furthermore, it will force many businesses to completely redefine their traditional value chains. "By making traditionally physical and disconnected processes digital and connected, products and services can be processed and delivered in completely new ways. This means that traditional value chains are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

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

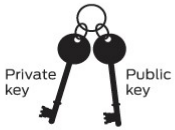
CREATING A NEW ADDRESS

Each address has its own balance of bitcoins.

Bob creates a new Bitcoin address for Alice to send her payment to.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

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.

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

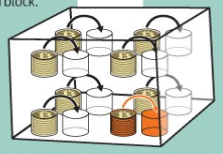
Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

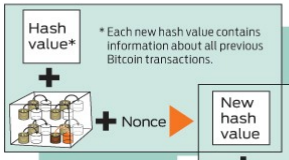
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

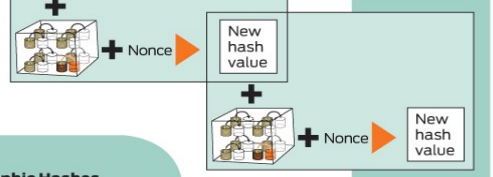
Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.





The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.



Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

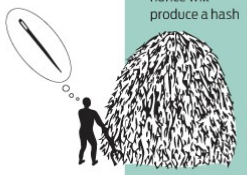
The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all euil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ???	0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

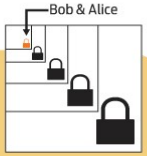
The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.



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 work of all the subsequent miners. Such a feat is nearly impossible.



JOSHUA J. ROMERO, BRANDON PALACIO & KARLSSONWILKER INC.

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 conditions

Sir Tim Berners-Lee speaks out on data ownership

The inventor of the web says data must be owned by its subject, rather than corporations, advertisers, and analysts

Alex Hern
theguardian.com, Wednesday 8 October 2014 13.23 BST
Jump to comments (148)

Sir Tim Berners-Lee says users must reclaim data rights Photograph: Peter Macdiarmid/Getty Images

The data we create about ourselves should be owned by each of us, not by the large companies that harvest it, the Tim Berners-Lee, the inventor of the world wide web, said today.

Berners-Lee told the IPExpo Europe in London’s Excel Centre that the

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

No data protection on up 50% of apps

more options

14 AUG 2013 10:00

SUBMIT A COMMENT BIZLIKE

PARIS, FRANCE: At least 20% of the world's websites and mobile telephone applications provide no information on how, or if, they protect users' personal data, a French watchdog company said on Tuesday (13 August).

CNIL

In collaboration with 19 other countries, France's national data protection agency CNIL in May conducted an audit of more than 2,000 of the world's most popular websites and apps to evaluate how they inform users of their data collection practices.

"More than 20% of the websites and mobile applications audited supply no information to their visitors with regard to their policies on data protection even though these sites or applications collect personal information.

For mobile applications alone, this number even reached 50%," it said.

"In cases when such policies are not communicated, users do not have the means to control their data", CNIL said, adding that even when such policies are available, they are often too general or too focused on specific technical aspects such as cookies.

Internet services routinely install small bits of software, called "cookies", on users' computers to store identifying information and to track Internet behaviour.

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 that 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?

https://manypossibilities.net/2012/09/35-reasons-to-worry-about-privacy-in-africa/

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 al[illegible]s.

Clear association between information society intent and trust imperative

AU Convention

- 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

APAI – African Platform for Access to Information Declaration, 2011

- 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.

- http://www.africanplatform.org/fileadmin/user_upload/pdf/APAI-Declaration/APAI-Declaration-English.pdf

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

Tech. Law. Policy. Africa.

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.theguardian.com/technology/2014/oct/08/sir-tim-berners-lee-speaks-out-on-data-ownership?CMP=ema_827
- http://www.bizcommunity.com/Article/75/542/98352.html
- http://ico.org.uk/Youth

Pria Chetty

Pria.chetty@endcode.org

endcode.org

THANKS, QUESTIONS?

ENDCODE

Tech. Law. Policy. Africa.