# AFRICAN INTERNET GOVERNANCE AND SOCIAL ISSUES: HUMAN RIGHTS AND DEVELOPMENT

AfriSIG 2017- Egypt

Ephraim Percy Kenyanito
(Digital Programme Officer- ARTICLE 19 Eastern Africa Office)
www.article19.org
Legal Researcher and Policy Analyst
www.ephraimkenyanito.com
ekenyanito@gmail.com
Twitter: @ekenyanito

ARTICLE 19

**ARTICLE 19 works so that people everywhere can express themselves freely, access information and enjoy freedom of the press. We understand freedom of expression as three things:**

## 1. Freedom of expression is the right to speak

It is the right to voice political, cultural, social and economic opinions

It is the right to dissent

It makes electoral democracy meaningful and builds public trust in administration.

## 2. Freedom of expression is freedom of the press

It is the right of a free and independent media to report without fear, interference, persecution or discrimination

It is the right to provide knowledge, give voice to the marginalised and to highlight corruption

It creates an environment where people feel safe to question government action and to hold power accountable.

## 3. Freedom of expression is the right to know

It is the right to access all media, internet, art, academic writings, and information held by government

It is the right to use when demanding rights to health, to a clean environment, to truth and to justice

It holds governments accountable for their promises, obligations and actions, preventing corruption which thrives on secrecy.

# Activities

**We design and promote laws and policies** that protect free expression, holding abusers and governments to account, and advocate for legal reforms. We also respond to urgent requests from activists needing support and expert advice worldwide.

**We assist the media in its professional development with a range of training and capacity-building resources** on freedom of the press, journalists' rights, defamation, public interest broadcasting, media pluralism, and reporting diversity

**We defend victims** by monitoring and analysing abuses, publicising the plight of individuals under attack**, providing security training** and security measures for journalists and human rights defenders, and **litigating** on their behalf**.**

**We also actively demand transparency and accountability** by testing governments' transparency practices and access to information provisions, and by campaigning for the disclosure of information of public interest.

# Session One: Internet governance and human rights

# Internet governance and human rights

1)**Fundamental rights** and what they mean on the internet.
2)**Freedom of expression and opinion.**
3)**Freedom of association.**
4)**Privacy.**
5)**Social, economic and cultural rights.**
6)**Women's rights:** Is the internet and enabler of women's human rights? How, and what is needed to guarantee this.

# Fundamental rights and what they mean on the internet.

**Frank La Rue (UN Special Rapporteur) stated in his seminal commentary:**

"...the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet..."

**UN HRC Resolution- Online- Offline**

**Joint Declaration on Freedom of Expression and the Internet-** "...c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting off the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet..."

# Intersections between FoE & Privacy,association, Social, economic and cultural rights

**Privacy as a prerequisite/necessary component of FoE-** ***Sconlen & Holderness/Zimbabwe*** (African Court on Human and Peoples'Rights) "...restrictions that are imposed on dissemination represent, in equal measure, a direct limitation on the right to express oneself freely..."

**Privacy in contest with FoE: investigative journalism, papparazzi**

**FOE & Social, economic and cultural rights-** Google in .za and Facebook in Asia; censorship & economic rights e.g. internet shutdowns- Burundi, Uganda, Egypt etc

**National security & law enforcement**

**Corporate accountability**

# Limitations

**Legitimacy, Neccessity and Propotionality**
limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including-
(a) the nature of the right;
(b) the importance of the purpose of the limitation;
(c) the nature and extent of the limitation;
(d) the relation between the limitation and its purpose; and
(e) less restrictive means to achieve the purpose.

# Women's Rights- Class Discussion- What are the issues, Why engage etc

- **ARTICLE 19 Eastern Africa Research Findings-**
- Most female journalists rely on Facebook (53.7 per cent), WhatsApp (86.4 per cent), e-mail (61.5 per cent) and mobile voice (96.2 per cent) for their day-to-day work.
- 75 per cent of the journalists interviewed have experienced online harassment in the course of their work.
- 36 per cent of the respondents preferred to ignore the attacks and took no action against the posts or the perpetrators.
- Digital harassment leads to women withdrawing from the use of the Internet and in many cases they have stopped working for some time. It has also changed the patterns of online interaction by women.
- Hacking, stalking and threats appear to be the most common forms of digital harassment of women. Most of these attacks have lasted a day.
- 54 per cent of the respondents rate their knowledge of digital security tools and practices as good and 29 per cent as workable. Most of these tools are inbuilt in the devices that women journalists use and include simple practices like passwords and screen locks.

# Session Two: Policy and regulation that impacts on development and internet-related human rights

# Policy and regulation that impacts on development and internet-related human rights

**The session will cover the following topics:**

1)Data retention
2)Internet intermediary liability
3)Filtering and blocking
4)Surveillance
5)Interception
6)Personal data protection
7)

**Key users:** Women's rights, LGBT rights and protection of journalistic sources and whistle blowers.

# Right to Privacy (in the digital age)

**Rights Framework:**

**UDHR, Article 12** (unlawful or arbitrary interference with his privacy, family, home or correspondence, unlawful attacks on his honour & reputation)

**ICCPR, Article 17**

**ACHPR, Article 3** (equality before the law)**, Article 4** (right to life and integrity of the person)**, Article 5** (right to dignity)**, Article 6** (right to liberty and security of the person)**, Article 9** (RTI and FoE)***, Article 10** (FoAssociation)***, Article 11** (FoAssembly)***, Article 13** (participation)***, Article 19** (equality of all peoples)

**ACHPR Resolution on FOE on the Internet**

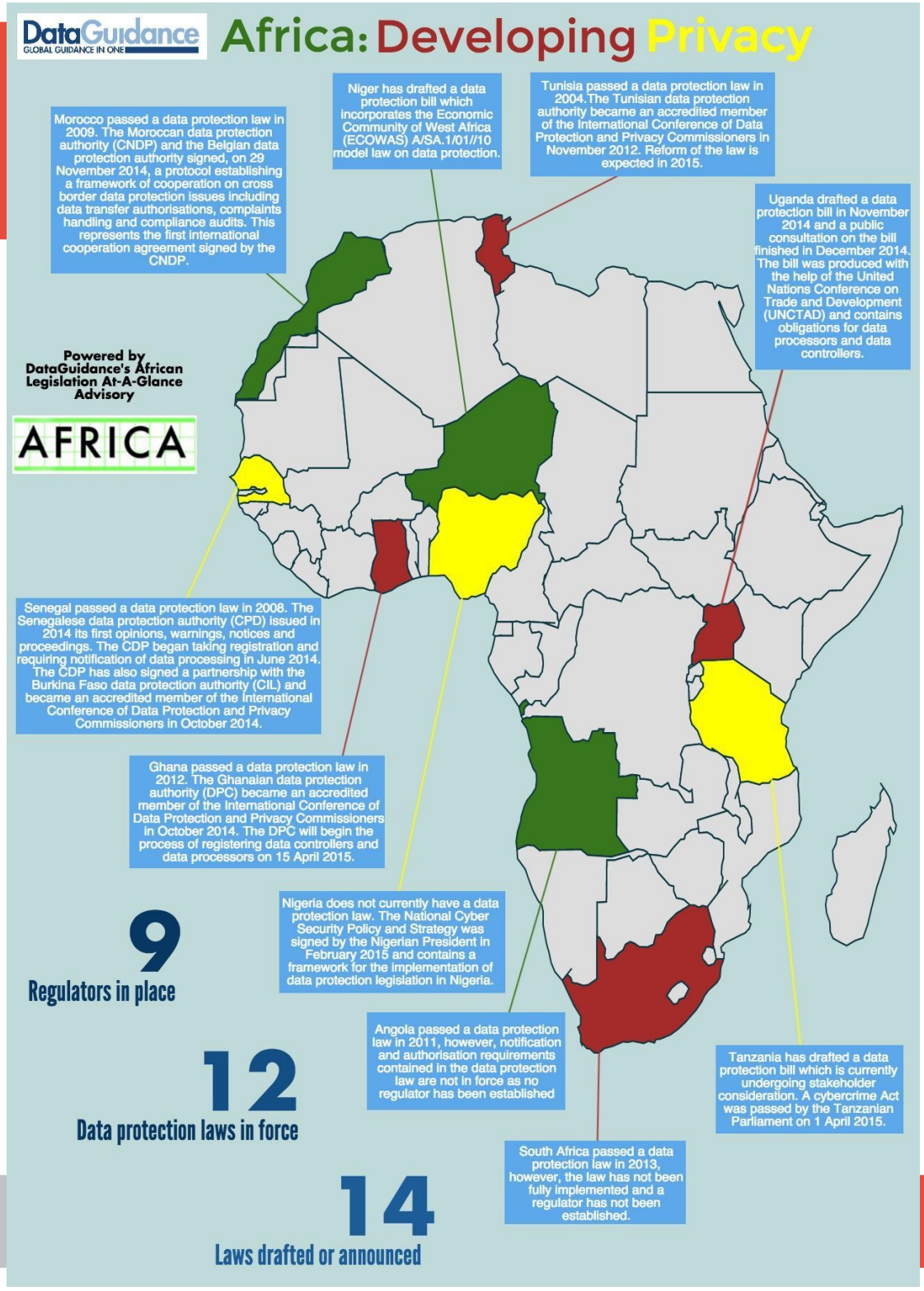
**ECOWAS-** Supplementary Act on Personal Data Protection within ECOWAS (2010)

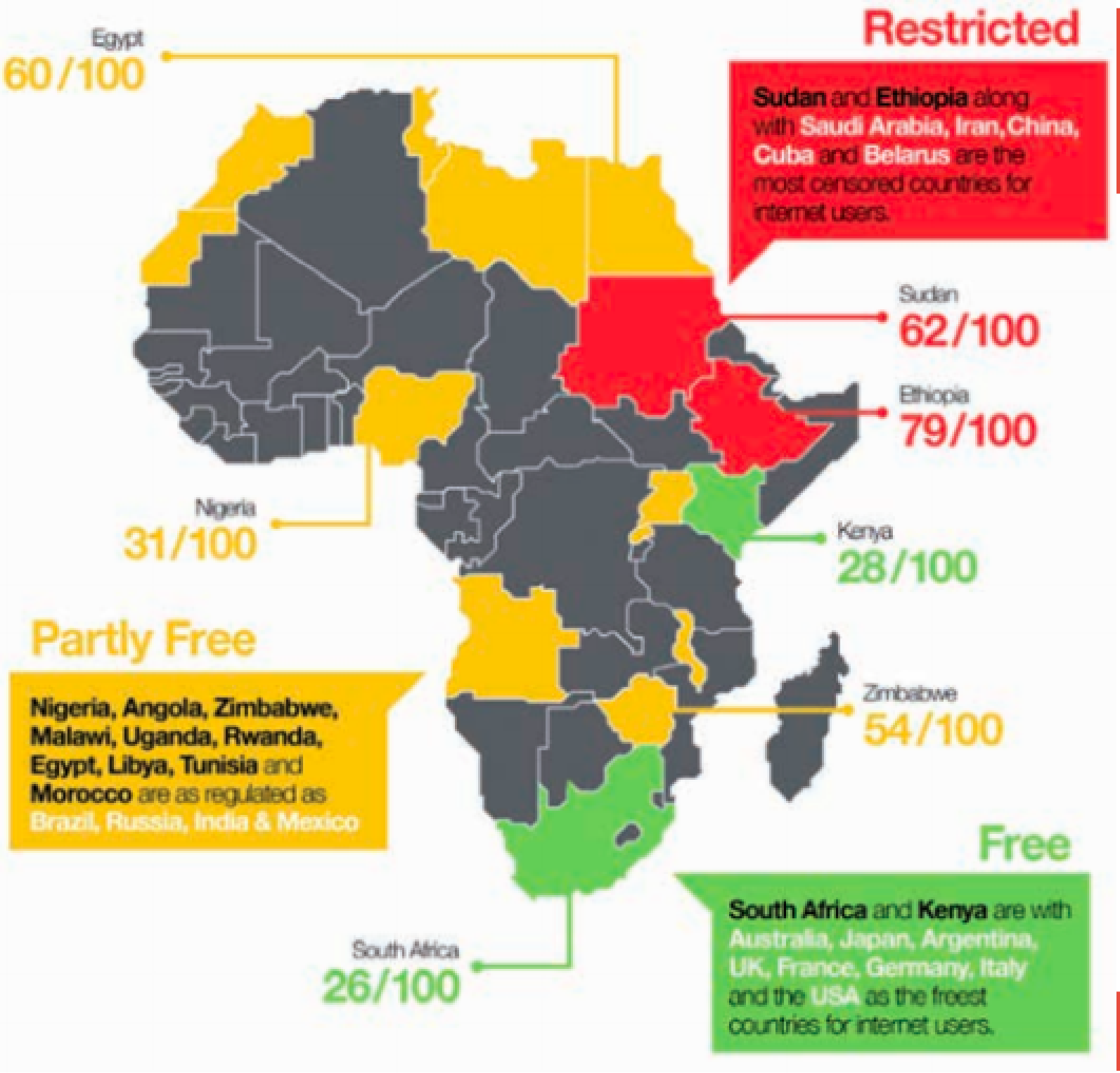
**EAC**- Draft Bill of Rights for the East African Community

SADC, Central Africa (ECCAS /CEMAC)- model laws

*** Within the law**

# National & Regional Laws




Egypt
60/100
Restricted
Sudan and Ethiopia along with Saudi Arabia, Iran, China, Cuba and Belarus are the most censored countries for internet users.
Sudan
62/100
Ethiopia
79/100
Nigeria
31/100
Kenya
28/100
Partly Free
Nigeria, Angola, Zimbabwe, Malawi, Uganda, Rwanda, Egypt, Libya, Tunisia and Morocco are as regulated as Brazil, Russia, India & Mexico
Zimbabwe
54/100
Free
South Africa and Kenya are with Australia, Japan, Argentina, UK, France, Germany, Italy and the USA as the freest countries for internet users.
South Africa
26/100

# Policy and regulation that impacts on development and internet-related human rights (cont..)

**Data retention**- "Data retention, also called records retention, is the continued storage of an organization's data for compliance or business reasons. An organization may retain data for several different reasons. One reason is to comply with state and federal regulations. Examples include: call detail records (CDRs) of telephony and internet traffic and transaction data, (IPDRs)...telephone calls made and received, emails sent and received, and websites visited. Location data is also collected. SIM Cards, Biometrics etc"- example- Ethiopia, South Africa, Kenya

**Internet intermediary liability**- arises when intermediaries are held legally responsible for content posted on their platform or transmitted using their infrastructure, instead of the individual producing, accessing, or sharing the content being held liable. e.g. Tanzania cyberlaw and Jamii Forums

# Policy and regulation that impacts on development and internet-related human rights (cont..)

**Filtering and blocking**- Internet censorship is the control or suppression of what can be accessed, published, or viewed on the Internet enacted by regulators, or on their own initiative. e.g. Sudan and Ethiopia

**Surveillance**- monitoring of computer activity and data stored on a hard drive, or data being transferred over computer networks such as the Internet. The monitoring is often carried out covertly and may be completed by governments, corporations, criminal organizations, or individuals.

**Interception**- Lawful interception is obtaining communications network data pursuant to lawful authority for the purpose of analysis or evidence. Such data generally consist of signalling or network management information or, in fewer instances, the content of the communications.

**Personal data protection**- Any information relating to an identified or identifiable natural person (directly or indirectly) by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental economic, cultural or social identity

# Surveillance in Africa (by states and by corporations) (data from Hacking Team leak)

| Customer | Country | Area | Agency | Year First Sale | Annual Maintenance Fees | Total Client Revenues |
|---|---|---|---|---|---|---|
| CSDN | Morocco | MEA | Intelligence | 2009 | €140,000 | €1,936,050 |
| UPDF (Uganda Peoples Defense Force), ISO (Internal Security Organization), Office of the President | Uganda | Africa | Intelligence | 2015 | €831,000 | €52,197,100 |
| Egypt - MOD[47] | Egypt | MEA | Other | 2011 | €70,000 | €598,000 |
| Bayelsa State Government | Nigeria | MEA | Intelligence | 2012 | €75,000 | €450,000 |

| Customer | Country | Area | Agency | Year First Sale | Annual Maintenance Fees | Total Client Revenues |
|---|---|---|---|---|---|---|
| Information Network Security Agency | Ethiopia | MEA | Intelligence | 2012 | €80,000 | €750,000 |
| Direction générale de la surveillance du territoire | Morocco | MEA | Intelligence | 2012 | €160,000 | €1,237,500 |
| National Intelligence and Security Servicecite_ref-fortune_47-3cite_ref-fortune_47-3 [47] | Sudan | MEA | Intelligence | 2012 | €76,000 | €960,000 |
| Egypt TRD GNSE | Egypt | MEA | LEA | 2015 | | €137,500 |

# Classification Based On Vedors (data from Wikileaks website)

1)**Amesys (France)**- Egypt, Libya
2)**ATISUHER (Germany)**- Tunisia,
3) **Blue Coat (USA)**- Egypt, Kenya, Nigeria,
4)**Gamma Group (UK/ German)**- Angola, Benin, Cameroon, Cote d'Ivore, Egypt, Equitoria Guinea, Ethiopia, Gabon, Madagascar, Morocco, Mozambique, Nigeria, Rwanda, South Africa, Uganda, Zimbabwe
5) **ELAMAN (Germany)**- South Africa,
6)**Hacking Team (Italy)**- Egypt, Ethiopia, Libya, Mali, Morocco, Nigeria, Uganda, (attempted purchases- Kenya, Ghana & Tanzania)
7)**VASTech SA Pty Ltd (South Africa)**- Libya
8) **VERINT (USA)**- Nigeria,
9) **Undisclosed Israeli Firm**- Nigeria, South Africa,

# Connection between Business & Human Rights

This is an indicative list (not an exhaustive one), sourced from the Business and Human Rights Resource Centre and research and advocacy undertaken by the ICAR:

States that have produced a National Action Plan on business and human rights: None

States that are in the process of developing a National Action Plan on business and human rights or have committed to doing so: Mauritius, Morocco, Mozambique & Tanzania.

States in which either the National Human Rights Institution or civil society have begun steps in the development of a National Action Plan on business and human rights: Ghana, Kenya, South Africa, Tanzania & Zambia.

# Encryption

- South Africa- Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (lawful court order)
- Tanzania- Electronic Transactions Act
- Benin
- Mauritania- draft bill (registration)
- Senegal- Law on Cryptography (Law No. 2008-41): Article 16 provides that bodies exercising cryptology services must be licenced by the National Cryptology Commission.
- Malawi- Electronic Transactions and Cyber Security Act, 2016 (lawful, registration, penalty- seven years' imprisonment and a fine of MWK 5,000,000.)
-

# Internet governance and human rights: Frameworks, principles and charters and spaces

**The International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles" or " 13 Principles" are laid out in the following manner:-**

Principle 1: Legality
Principle 2: Legitimate aim
Principle 3: Necessity
Principle 4: Adequacy
Principle 5: Proportionality
Principle 6: Competent judicial authority
Principle 7: Due process
Principle 8: User notification
Principle 9: Transparency
Principle 10: Public oversight
Principle 11: Integrity of communications and systems
Principle 12: Safeguards for international cooperation
Principle 13: Safeguards against illegitimate access and right to effective remedy

# The African Declaration of Internet Rights and Freedoms

**African Declaration Principles are laid out in the following manner**

Principle 1:Openness
Principle 2:Internet Access and Affordability
Principle 3:Freedom Of Expression
Principle 4:Right To Information
Principle 5:Freedom of Assembly And Association And The Internet
Principle 6:Cultural And Linguistic Diversity
Principle 7:Right To Development And Access To Knowledge
Principle 8:Privacy And Personal Data Protection
Principle 9:Security, Stability And Resilience Of The Internet
Principle 10:Marginalised Groups And Groups At Risk
Principle 11:Right To Due Process
Principle 12:Democratic Multistakeholder Internet Governance
Principle 13:Gender Equality

- ARTICLE 19 Global Principles on Freedom of Expression and Privacy (March 2017)
- Participants to refer to the document on ARTICLE 19 Website

# What about NetMundial and Africa? (analysis by Ephraim sourced from Access Now Website)


| | |
|---|---|
| 1 | GOVERNMENT |
| 9 | CIVIL SOCIETY ORGANIZATIONS |
| 3 | PRIVATE SECTOR |
| 1 | TECHNICAL COMMUNITY |
| 1 | MULTI-STAKEHOLDER PLATFORM |
| 4 | ACADEMIA |

# What about NetMundial and Africa? (analysis by Ephraim sourced from Access Now Website)

**14**

ON FREEDOM OF EXPRESSION

- CIVIL SOCIETY ORGANIZATIONS
- PRIVATE SECTOR
- ACADEMIA
- MULTI-STAKEHOLDER PLATFORM
- GOVERNMENT

**11**

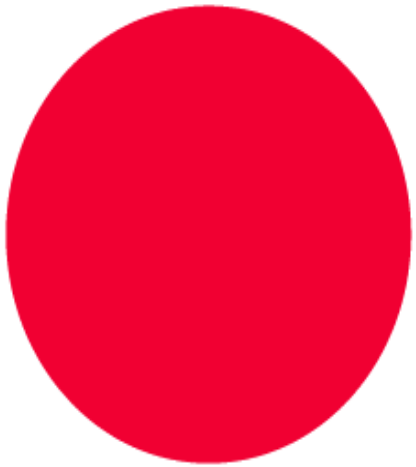
ON ROLE OF GOVERNMENTS

- CIVIL SOCIETY ORGANIZATIONS
- ACADEMIA
- TECHNICAL COMMUNITY
- MULTI-STAKEHOLDER PLATFORM
- GOVERNMENT

**5**

ON SECURITY

- PRIVATE SECTOR
- TECHNICAL COMMUNITY
- ACADEMIA
- GOVERNMENT



**1**

ON GLOBALIZATION OF IANA FUNCTIONS

- GOVERNMENT

# What about NetMundial and Africa? (analysis by Ephraim sourced from Access Now Website)

**4**

ON NET NEUTRALITY

- GOVERNMENT
- PRIVATE SECTOR
- MULTI-STAKEHOLDER PLATFORM

**4**

ON AFFORDABLE ACCESS

- GOVERNMENT
- CIVIL SOCIETY ORGANIZATIONS
- PRIVATE SECTOR
- MULTI-STAKEHOLDER PLATFORM

**4**

ON GLOBALIZATION OF ICANN

- GOVERNMENT
- CIVIL SOCIETY ORGANIZATIONS
- TECHNICAL COMMUNITY

# Emerging issues in internet governance

Surveillance – by states and by corporations

# Session Three:

# Cybersecurity- Legal Analysis of the AU African Union Convention on Cyber Security and Personal Data Protection

# Legitimacy for Internet Regulation

- Increase in a number of Internet users leads to increase in a legitimacy of Internet regulation
- Narrative whereby the Internet is framed as both as a threat and an opportunity- Focus on various apps e.g. MPESA, health applications. On Threat: children protection, Pornography, Cyber crime (both internal and external)

# I. DOMESTIC PERCEPTIONS AND FACTORS MATTER

## The 2011 Arab Spring and other events e.g. Post election Violence has had an unsettling effect on some African Political elites

## First Process: ITU AFRICA HIPSSA PROJECT/ 2009 Oliver Tambo Delaration.

Since 2008, the African Union (AU), has engaged in efforts to harmonize various information and communications technology (ICT) regimes particularly around cyber security laws with funding from ITU.

In 2008 the Ministers in charge of Communication and Information Technologies from the African Union countries adopted a Reference Framework for Harmonization of the telecommunication and ICT Policies and Regulation in Africa (HIPSSA) (Cairo, 2008) during the 2nd Conference of African Ministers in charge of Communication and Information Technologies (CITMC-2). The Reference Framework adopted had one of the key aim, to: "...*Establish harmonized policy, legal and regulatory frameworks at the regional and continental levels to create an enabling environment that will attract investment and foster the sustainable development of competitive African Telecommunication/ICT regional markets, infrastructures, and to increase access [of its people to the related services*..." We can highlight that the International Telecommunication Union supported this initiative under the HIPSSA with a focus on key economic integration organizations in Sub-Saharan Africa.

# 2009 Oliver Tambo Delaration- Going forward

Structured discussions about establishment of a common framework have been ongoing since a 2009 directive, the Oliver Tambo Declaration.
In 2013, a draft African Union Convention on the Confidence and Security in Cyberspace (AUCC) was made pursuant to the resolution of the Assembly of Heads of State and Government of the African Union and was published on the African Union website for discussion from the African internet community. Major concerns were then voiced around this draft, and in May 2014 it was revised to a final version of the Convention, which was approved by African Heads of State at the end of June.

- **Contentious Provisions that caused delay of transmission to heads of State and Government (First Draft)**
- In short, the draft convention included provisions on electronic commerce, personal data protection, cybercrime — with a special focus on racism, xenophobia, and child pornography — and national cybersecurity. It also encouraged member states to promote cybersecurity education for information technology professionals and to add to their legal codes criminal offences for hacking computer systems. Below, we will expand on the problematic issues we identified in the first draft text.
- **Infringing on the right to privacy**
- Articles II (8); II (9); II 28(2); and II 36(9) of the first draft AUCC, allowed African states to process personal and sensitive data without the owner's consent for the purpose of state security and the public interest. Furthermore, the government did have to go before a judge to get approval to violate user privacy in this way, leaving the door open for abuse.

- Article I (4) of the convention compelled a person or corporation engaging in electronic financial transactions (e.g M-PESA) to provide full identity information as prescribed in the clause such as his/her name, identification number, and contact information among other information. This provision puts personal information at risk, given the fact that very few African countries have comprehensive data protection laws. One does not need to look far to see the kind of abuse that can occur in this environment. Recently, a number of Kenyans were unknowingly registered with various Kenyan political parties without their consent; Safaricom, a major African telecom suggested that M-PESA agents might have sold M-PESA registration and transaction records to the political parties.
- **Lack of limitations on judicial power**
- Article III (55) provided for , "...the investigating judge [to] use appropriate technical means to gather or register in real time the data in respect of the content of specific communications in its territory, transmitted by means of a computer system..." The provision empowered judges to assume the role of the prosecutor in both common law and civil law African countries and does not provide checks and balances to ensure a separate investigation and adjudication process.

## Final Document: African Union Convention on Cyber Security and Personal Data Protection

- The final outcome of the convention was adopted at the heads of state summit in June 2014 in Equitorial Guinea, we can note that the change of name is an indication of a shift in focus to Personal Data Protection and that some of the human rights concerns highlighted above were addressed. (thought not all)
- e.g. Introduction of stronger Provisions for Personal Data Protection Authorities under Article 11 (we can note that the new text is more improved as compared to the previous text)
- **Conclusion and way forward for the African governments**
- This new convention will enter into force 30 days after its receipt by the Chairperson of the Commission of the African Union under the 15th instrument of ratification.
- This means at least 15 governments need to accept the text of the convention for it to enter into force. If it is accepted, then it will go through a process of domestication across various national legislatures whereby the convention would be adapted into the local context of each country.

## Importation of norms? And Political Influence in IG Processes

Some of the funders of the AUCC Process:
US DoJ, CoE, UNCTAD, UNODC

## Other Processes:

The BRICS influence and other factors e.g. ICC causing most African Countries to adopt different positions at the international level


FOURTH
BRICS Summit
March 29, 2012 : New Delhi
New Delhi
BRICS
2012

# The potentially good (analysis by Ephraim sourced from Access Now Website)

## 1. Data Protection

A large part of the Convention mirrors the data protection framework and language developed by the European Union. Per the Convention, each member state of the African Union is required to have a national data protection authority (DPA) — an independent administrator to ensure the processing of personal data is conducted in accordance with the Convention. Data can only be processed for a specific legitimate purpose, however, no definition of legitimate purpose is given. Processing and storage are limited to the time necessary for the purpose for which the data were collected or processed, with exceptions for "the public interest, especially for historical, statistical or scientific purposes."

- A specific, individual right to object to processing was added, potentially empowering users, but it's not clear on what "legitimate grounds" objections can be raised (Art. 18). Data subjects have the right to be notified before their data are shared with a third party for the first time (Art. 18).
- a number of other concepts in the data protection section — "consent", "data controller", "data subject", "personal data", "sensitive data" — need further attention. For instance, the definition of sensitive data includes "legal proceedings," which are a matter of public interest and shouldn't be sealed by default; and "health data" is too broad and could even be interpreted to extend to Facebook status updates about having a cold!

# 2. Cybersecurity and human rights

- The cybersecurity sections of the Convention specifically protect human rights. Governments "shall" ensure their new laws uphold the "African Charter on Human and Peoples Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others" (Art. 25 ¶3). The inclusion of privacy is most welcome, considering it is not explicitly found in the African Charter.
- Furthermore, civil society is expressly included as part of multistakeholder and public-private partnerships (Art. 26 ¶3) and the cybersecurity "culture" (Art. 26 ¶ 1b).
- The cybersecurity rules also support the rule of law: The Convention insists that governments sign mutual legal assistance agreements (MLATs) to establish standards for international data sharing in an efficient way (Art 28 ¶ 2).
- Importantly, member states must pass laws protecting data security and notifying users of risks to their data (Art. 29), and of data transfers to third parties (Art. 18), a provision which should apply to data breach and unlawful transfers.

# The possibly bad

- **1. Content restrictions**
- The definition of child pornography seems to include any depiction whether or not real children were used, and the ban is a potentially broad provision that could be enforced in very ugly ways if internet intermediaries are held liable for the behavior of users (Art. 29 ¶3).
- The explanation of incitement under "racism/xenophobia" does not include sexual orientation or gender, though it does cover race, color, ancestry, national/ethnic origin, and religion. Given the serious threats to the safety of LGBT human rights defenders in many African countries, any protections should account for incitement to violence based on sexual orientation and gender.

# 2. cybersecurity

- While encouraging public/private partnerships on cybersecurity, the Convention fails to put safeguards into the sharing of information between companies and governments (Arts 24-27). Moreover, the Convention requests broad cybersecurity authority for regulators without clarifying limits to the regulator's power (Art. 25 ¶2). To protect user data, data protection standards should have a place even in cyber security contexts.
- In fact, the framing of the basic mandate on governments to develop "a national cyber security policy which recognizes the importance of Critical Information Infrastructure (CII)" takes the wrong approach to cybersecurity. Member states should note their reservations about this flawed, top-down paradigm, and signal their intention to put individual users at the center of data security efforts, rather than ill-defined CII.
- Strangely, the Convention defines "secret conventions" as having to do with encryption keys, but never mentions "secret conventions" or cryptography elsewhere in the document — a rather cryptic decision.

# The just plain ugly

- **1. User Consent**
- Personal data should only be processed where the data subjects give express, unequivocal, free, specific, and informed consent. However, the Convention adds exceptions, including for "Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" (Art. 14.2.i). A loophole of this size is ripe for abuse by governments eager and willing to define the "public interest" as their own interest.

# 2. More content restrictions

- The Convention bans use of a computer to “insult” someone for reasons of race, color, national/ethnic origin, religion, or political opinion. It never defines “insult,” leaving this subjective provision to criminalize speech instead of a criminal act. In conjunction with the following provision, which disallows intentionally approving, denying, or justifying “acts constituting genocide or crimes against humanity,” these ill-conceived and harmful provisions will only serve to limit free expression and chill expression online.
- Finally, the Convention confers broad authority to Courts to access databases and conduct surveillance of networks if it is “useful in establishing the truth” (Art. 31.3), a vague, if well-intentioned clause that is open to abuse.

# 3. Computer fraud and journalism

- Vague, broad provisions defining computer fraud hinge on “unauthorized access,” an undefined term. The provision criminalizes attempts to “enter data fraudulently in a computer system” or “remain fraudulently in a computer system” which could apply, among other things, to violations of social media platform’s Terms of Service (Art. 29 ¶ 1).
- One clause increases penalties for existing crimes if they have a computer component, an unnecessary and disproportionate tactic (Article 31.2.a). Simply using a computer does not justify higher penalties.
- Whistleblowers and journalists could suffer under a restriction on the use of “data that was fraudulently obtained” (Art. 29.2). This criminalizes journalism based on leaked documents or disclosures, a necessary activity for journalists in many African countries, which often lack freedom of information and similar information access laws, leaving large swaths of public information off-limits. An exception on data processing only applies to licensed journalists (Art. 14.3), discriminating against many bloggers and independent voices.

# Implementation in various countries:

As at July 2017, nine African nations had signed the convention, including: Benin, Chad, Congo, Ghana Guinea Bissau, Mauritania, Sierra Leone, Sao Tome & Principe, and Zambia
One had ratified: Senegal

Additionally; From our analysis of the 45 Sub Saharan Africa countries, we can note that a total of 13 countries have in the period between June 2014 and September 2016 engaged in attempted domestic reforms on ICT laws; The include: Benin, Botswana, Chad, Ethiopia, Kenya, Madagascar, Namibia, Nigeria, South Africa, Tanzania, Uganda and Zimbabwe.

# Example of Madagascar

- In the first week of August 2014, Madagascar's parliament passed the cybercrime law, which, under Article 20, outlaws the use of print or electronic media to "insult or defame" government officials.
- The crime would be punishable between two and five years of imprisonment and/or a fine of two to 100 million ariary (742 to 37,109 U.S. Dollars). The law fails to define what is meant by "insult" or "defame," creating the opportunity for broad and vague interpretation. As it is written, a simple tweet or Facebook status critiquing government officials could lead to huge fines or years in jail.

# Other Notable Countries

- Botswana passed the Electronic Evidence Bill, which penalises people, up to five years in jail, for insulting others over social media.
- Mauritania- Article 18 stipulates that “all provisions in conflict with this law are annulled,” undermining other laws that “require interdiction prior to jailing journalists.” Other sections of concern included provisions addressing (and prohibiting) encryption, which would limit freedom of expression and privacy online.
- Nigeria- Passed Bill (7 years penalty)
- Ghana- Data Protection Authority
- Uganda- Data Protection Bill

Ephraim Percy Kenyanito
(Digital Programme Officer- ARTICLE 19 Eastern Africa Office)
www.article19.org
Legal Researcher and Policy Analyst
www.ephraimkenyanito.com
ekenyanito@gmail.com
Twitter: @ekenyanito