A REPORT OF THE ONLINE DEBATE ON AFRICA UNION CONVENTION ON CYBERSECURITY (AUCC)

Submitted to:

Africa Union Commission (AUC)

Compiled By Grace Githaiga

December, 2013

The Kenya ICT Action Network (KICTANet) is a multi-stakeholder platform for people and institutions interested and involved in ICT policy and regulation. The network aims to act as a catalyst for reform in the ICT sector in support of the national aim of ICT enabled growth and development (www.kictanet.or.ke)

Appreciation:

Lilian Nalwoga, CIPESA Uganda, Robert Njathika, Strathmore University, Suresh Ramasubramanian IGC, Lea Kasper, Global Partners, Deborah Brown and Jack Katsman of Access Now and ALL KICTANet Listers for the vibrant debate on the Convention.

1. Introduction

An online debate on the African Union Convention on Cyber Security (AUCC)[1] was conducted on multiple lists of KICTANet and ISOC-KE, in Kenya and on I-Network list moderated through by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) and ISOC -Uganda, from 25 – 29, November 2013. The concerns were also shared with the Best Bits mailing list,[2] the Internet Governance Caucus list,[3] The Web We Want[4] and Access Now.[5] The aim was to get as much input as possible.

The discussion was informed by the fact that the AUC drafters agreed to receive this input in the spirit of consulting stakeholders despite having gone through this process two years ago with African governments. The draft report of this discussion formed part of discussion on the convention during the AU ICT week which took place from 1-6, December 2013.[6]

This engagement was viewed as important for Kenya, the reason being that if Kenya signs into this convention in January 2014, it will become binding as stipulated in Article 2 (6) of Kenya's 2010 Constitution which states: *Any treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution.* The Convention therefore is more like a Bill of Parliament.

2. Background to the African Union Convention on Cyber Security (AUCC)

African Union (AU) Convention (52 page document) seeks to intensify the fight against cybercrime across Africa in light of the increase in cybercrime, and the lack of mastery of security risks by African countries. Further, a major challenge for African countries is the lack of adequate technological security to prevent and effectively control technological and informational risks. As such, "African States are in dire need of innovative criminal policy strategies that embody States, societal and technical responses to create a credible legal climate for cyber security".

[1] http://pages.au.int/sites/default/files/AU%20Cybersecurity%20Convention%20ENGLISH_0.pdf
[2] http://bestbits.net/
[3] http://igcaucus.org/
[4] http://webwewant.org
[5] https://www.accessnow.org/
[6] http://www.africanictweek.org/

The Convention establishes a framework for cyber security in Africa "through organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime" (Conceptual framework).

3. The Discussion

Articles that needed clarity were picked and List participants requested to discuss them and provide recommendations where necessary. List participants were also encouraged to identify and share other articles that in their opinion required clarification.

Article	Concerns	Recommendations/Alternate text
Section III: Publicity by electronic means		
Article I – 7: *Without prejudice to Article I-4 any advertising action, irrespective of its form, accessible through online communication service, shall be clearly identified as such. It shall clearly identify the individual or corporate body on behalf of whom it is undertaken.*	**Question:** Should net anonymity be legislated? If so, what measures need to be or not be considered? Net Anonymity forms a cornerstone of how the Internet has evolved and grown to become the mass communication tool it is today. Although the proposals mean well in terms of trying to cap criminal activities it is a double edged sword.	Emerging trends and security threats have forced people to start thinking of online security and child protection. Crime is not as straight forward. Data protection and net anonymity have to be carefully balanced to log data but retain it under strict controls and regulation of how it can be used (in accordance with privacy regulations). If you legislate blanket anonymity then scam artists and cybercriminals will

	Question: Should individuals or companies be obliged to reveal their identities and what are the implications? a) How will whistle blowers be protected if they feel their identities will be compromised? b) My right as a citizen to contribute in healthy sometimes sensitive political discourse in some cases requires a certain level of anonymity. c) How we counter needs of national security and personal freedoms without blanket condemnation of particular religious or ethnic groups will define us as a nation and continent. d) We need to be very careful that we don't quash the very environment and ecosystem that has allowed some African countries to thrive and be perceived as leaders in the online space. The question to ask here is, what is the cost of banning anonymous advertising in the cyberspace? Is it worth it? And how will it affect business both online and offline? **Even if we are to protect the anonymity of advertisers, there should be a mechanism to**	extensively abuse it to remain undetected. Africa has a very poor electronic commerce track record which might be linked to weak cyber security as such we might want to strike a balance between freedom and responsibility online. Companies have stringent policies regarding the use of their Internet and network resources. There is need to start considering striking a balance between freedom and responsibility online. **Probably, the Convention can read something like this *"Without prejudice to***

	track and identify them when a breach has occurred. **What if a company advertises defamatory remarks about me or my company, I should be able through some mechanism to unveil the source of the defamation, otherwise the intermediary will have to bear the liability. Take an example of Google Ads, they are clearly identified as such, and if the add is not appropriate, there must be a way to identify the advertiser.**	***Article I-4 any advertising action, irrespective of its form, accessible through online communication service, shall be clearly identified as such. ~~It shall~~ [There shall be a mechanism (database) to] clearly identify the individual or corporate body on behalf of whom it is undertaken."***
Article I – 8: *The conditions governing the possibility of promotional offers as well as the conditions for participating in promotional competitions or games where such offers, competitions or games are electronically disseminated, shall be clearly spelt out and easily accessible.*	**Question:** Should an international (or should we call it regional) law legislate on promotional offers and competitions offered locally?	This convention provides a criterion that nations in the Africa will commit to harmonize their current (or more likely proposed, in large parts of Africa) to be uniform on this and other provisions. In this case, it advocates transparency in direct marketing offers which is a best practice.
Article I – 9: *Direct marketing through any form of indirect*	**Question:** Is this a realistic way to deal with spam?	The provision is respectful of user privacy and doesn't allow the sending of unsolicited bulk email, which is the

communication including messages forwarded with automatic message sender, facsimile or electronic mails in whatsoever form, using the particulars of an individual who has not given prior consent to receiving the said direct marketing through the means indicated, shall be prohibited by the member states of the African Union.	Is there any "unsolicited communication" that is not "Direct Marketing"? What does "indirect communication" mean in this clause if that communication is targeting my phone, facsimile, and email address? There is a need for proper acquisition of data for mailing purposes, there has to be proof of willing buyer willing seller. Getting the right balance might be tricky but with an elaborate Data Protection Act, this can be clearly defined. Legislation is not an answer to everything. There are more efficient ways of dealing with spam - blocking it, unsubscribing and in some rare cases actually requesting to be removed from the offending list. Fighting spam or curtailing Direct Marketing is not the business of government and they should let the market (and available online tools) deal with the offending practice. We have a way of punishing intrusive companies and individuals and sooner or later we will push them out of our inboxes and screens by voting with our wallets.	canonical definition of spam. It should not restrict itself to marketing but cover other sorts of bulk mail sent by other organizations or individuals. The provision should be content neutral and cover all forms of unsolicited bulk email rather than just marketing mail. **The articles need to additionally cover criminal forms of spam as the 419 scam, phishing etc.** Further, it should require that penalties are provided both for the organization that commissioned the spam and the marketing agency they contracted with to actually send the spam. **Specific language that would be appropriate is in the Australian Spam Act of 2003 and in the proposed Canadian Anti-Spam law, both of which were drafted after open, consultative and multi-stakeholder processes in the respective countries, including inputs from respected privacy groups.**

	Legislation similar to this one have been put in place not only in Uganda but in many countries in Africa. The problem is implementation and willingness of some service providers to support the implementing powers to see these laws work. SPAM can come in whatever way as long as the user has not been notified. Probably it should be mentioned in the terms and conditions of purchasing when purchasing a sim card, that you will receive promotional messages of our services till you opt out of it.	
Article I – 10: *The provisions of Article I – 9 above notwithstanding, direct marketing prospection by electronic mails shall be permissible where:* *1) The particulars of the addressee have been obtained directly from him/her,* *2) The recipient has given*	**Question:** Are these factors inclusive? Does it have to have all three or just one of the three? As long as any message is sent that jeopardises the users or affects the user in one way or the other, it should be categorised as spam and should be subjected to law and penalty as long the user has not consented to the message received.	There have been attempts to regulate spam before, which have not been very effective. Enforceability comes into play in two ways – if it is under-enforced, then it is unnecessary; but it can also be over-enforced, which could lead to violations of fundamental rights, e.g. freedom of expression, especially if the definition of spam is vague and open to abuse.

consent to be contacted by the prospector partners *3) The direct prospection concerns similar products or services provided by the same individual or corporate body.*		
Article I – 27 Where the legislative provisions of Member States have not laid down other provisions, and where there is no valid agreement between the parties, the judge shall resolve proof related conflicts by determining by all possible means the most plausible claim regardless of the message base employed.	**Question:** What is the meaning of this article and is it necessary? Some clarity needed! This article is so open, lawyers would have a field day with prosecutors since there is no specifics. This clause looks to be like the "copy and paste" legislation. As long as the victim has the spam message and evidence of the spammer then the judge will have to determine the most plausible claim. BUT no punitive measure is defined here, so what will they do with the claim? It sounds like an incomplete statement that needs to be improved.	"Where the legislative provisions of Member States have not laid down other provisions, and where there is no valid agreement between the parties, the judge shall resolve proof related conflicts by determining the most plausible claim regardless of the message base employed" **Remove *by all possible means or in the alternative, change to all legal means***

Article I – 28: A copy or any other reproduction of actions undertaken by electronic means shall have the same weight as the act itself, where the said copy has been certified as a true copy of the said act by bodies duly accredited by a State authority. The certification shall culminate in the issuance of an authenticity certificate, where necessary.	What does the certification here entail? Is there a national system for this?	
PART II: PERSONAL DATA PROTECTION **Objectives of this Convention with respect to personal data**		
Article II – 2: *Each Member State of the*	**Question:** What is the relevance of this article? What are these state prerogatives?	With respect to personal data, state prerogatives must be well defined so as

African Union shall put in place a legal framework with a view to establishing a mechanism to combat breaches of private life likely to arise from the gathering, processing, transmission, storage and use of personal data. *The mechanism so established shall ensure that any data processing, in whatsoever form, respects the freedoms and fundamental rights of physical persons while recognizing the prerogatives of the State, the rights of local communities and the target for which the businesses were established.*	And given the increased interest of state surveillance, how can states balance respect of FOE while recognising state prerogatives? There is need to probe whether the intent was to protect Africans data from external violations of privacy among other fundamental rights, for example, Kenyans private data gathering by US NSA online surveillance reported on 'NSA porn spying' – *"Instead, the NSA believes the targeted individuals radicalize people through the expression of controversial ideas via YouTube, Facebook and other social media websites. Their audience, both English and Arabic speakers, "includes individuals who do not yet hold extremist views but who are susceptible to the extremist message," the document states. The NSA says the speeches and writings of the six individuals resonate most in countries including the United Kingdom, Germany, Sweden, **Kenya**, Pakistan, India and Saudi Arabia".*	not to breach the rights of a private life online or offline. All activities that arise from the gathering, processing, transmission, storage and use of personal data should be well defined and levels of acceptable access and permissions by individual users properly laid out so as not to create a door for perceived surveillance or activities that take away the personal rights of a user.
Article II-6, II-7, II-8, II-11, II-12, II-13 refer to a Protection Authority which is meant to establish standards for data protection. Article II – 14	**Question:** Considering that this article seems to be tied to the Protection Authority, what is its relevance? And who is a 'sworn agent?' What should this authority look like in terms of its composition?	Conceptually "sworn agents" are very important in this scenario – especially if not members of the government. Sworn agents should be considered *unbiased*, to properly fulfil their purpose as stated by

provides for each Member State of the African Union to establish an authority with responsibility to protect personal data. It shall be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with domestic legislations. In article II-17 states that *Sworn agents may be invited to participate in audit missions in accordance with extant provisions in Member States of the African Union.*	These articles define the membership and the constituting mandates of the said 'Protection authority.' However it should be left to the countries to define the authorities under inbuilt country contributions/laws or bylaws so as not to create a different centre of power or parallel agency. 'Sworn Agents' should be well defined and described, their mode of selection, duties, responsibilities should be open to public accountability and transparency.	this convention.
Article II – 20: *…Members of the protection authority shall not receive instructions from any authority in the exercise of their functions.* And **Article II – 21:** *Member States are engaged to provide the national protection authority human,*	**Question:** It appears that this Data Protection Authority is envisaged to be fully government supported. Therefore, should we be talking of its independence? In what way should this article be framed so that it ensures independence of the Authority?	The selection of the membership to the protection authority should allow composition from all stakeholders and not only government.

technical and financial resources necessary to accomplish their mission.		
Article II – 22: *The national protection authority shall ensure that the processing of personal data is consistent with the provisions of this Convention in the African Union Member States.*	**Question:** There is no mention of human rights documents that cover the digital/ cyber space, or have been read to cover the digital space, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, or the African Charter on Human and Peoples' Rights	There are other places this can be included, a provision mentioning international and regional human rights conventions is very important as States are already obligated to enforce them.
Article II – 23 (6) *Speedily inform the judicial authority of **certain types** of offenses that have come to its knowledge;*	**Question:** What is meant by certain types of offenses?	This is conceptually hard to understand and follow. The convention does not give examples or guidance on what types of offenses are covered, but it is clear that it is **not ALL** offenses. The nature of the offences should be clarified.
Article II – 26: *In case of emergency, where the processing or use of personal data results in violation of fundamental rights and freedoms, the*	**Question:** What would happen in a case where all of the data process was a violation of fundamental rights and freedoms?	This can be remedied by adding language to (2) – **to include some OR ALL of the data** processed.

national protection authority may, after adversarial proceedings, decide as follows: *1) Interruption of data processing;* *2) Locking up some of the personal data processed;* *3) Temporary or definitive prohibition of any processing at variance with the provisions of this Convention.*		
Article II – 30 (3): *3) The data shall be conserved for a duration not exceeding the period required to **achieve the ultimate objective** for which the said data have been gathered or processed.* **Article II – 48:** *Personal data shall be conserved for a duration not exceeding the period required to **achieve the ultimate***	**Question:** How does one determine what the ultimate objective is? How specific does the "ultimate objective" need to be?	Having a maximum time period, that could be extended

objective *for which the said data has been gathered or processed*		
PROMOTING CYBERSECURITY AND COMBATING CYBERCRIME		
Article III – 14: Harmonization 1) *Member States have to undertake necessary measures to ensure that the legislative measures and / or regulations adopted to fight against cybercrime enhance the possibility of regional harmonization of these measures and respect the principle of double criminality.*	**Question**: What is the principle of double criminality here? **Double criminality** (also known as **dual criminality**) is a requirement in the extradition law of many countries. It states that a suspect can be extradited from one country to stand trial for breaking a second country's laws *only* when a similar law exists in the extraditing country. For example, if Country A has no laws against blasphemy, double criminality could prevent a suspect being extradited from Country A to face blasphemy charges in another country. This is of course a double edged sword. The implication here on harmonization of regional laws is a red flag.	The emerging trend today is to incorporate provisions that would require states to either surrender the suspects to a state wishing to prosecute or in the alternative, prosecute such persons in their own courts. Therefore, it is important for states to harmonise their legislation with regard to cybercrimes so that such persons may not get away on the basis of

	What may be kosher in Zimbabwe may not pass muster in Kenya. The feeling here is that the interest of the Citizenry is secondary to Government. Let's have less Government. The clause on double criminality basically restates a principle of international criminal law which is generally well accepted and implemented here. It is both a sword and a shield. As a sword, to ensure that criminals are prosecuted for crimes they commit in foreign jurisdictions and as a shield, to ensure that individuals are not extradited to other jurisdictions to face charges for activities which are not criminal in their home countries. Let us remember that states remain sovereign and may or may not extradite or punish criminal suspects if they so feel.	double criminality.
Article III - 34: Each Member State of the African Union have to take necessary legislative or regulatory measures to set up as a penal offense the fact of creating, downloading, disseminating or circulating in	**Question:** How does this balance with the fundamental right to freedom of expression?	This is a bit overbroad, and would create a crime in any statement of racist or xenophobic remarks, even if just a statement of opinion - hampering freedom of expression. Maybe this should be modified with some intentional portion - intention to incite action, for example.

whatsoever form, written matters, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature using an a computer system.		
Article III – 48 *Each Member State of the African Union have to take necessary legislative measures to ensure that, in the case of conviction for an offense committed by means of digital communication facility, the competent jurisdiction or the judge handling the case gives a ruling imposing additional punishment.*	**Question:** What is the interpretation of additional punishment? Is this not granting of absolute powers to judges? We always assume that human behaviour is different online as opposed to offline. Fraud is fraud whether off or online. Impersonation (as opposed to anonymity) is still impersonation and depending on why you are impersonating someone it still is a crime. On additional punishment, the intention is to enhance punishment provided by law for offences which are committed by digital communication. Hence, the effect would be that judges would be required where there is only a minimum sentence provided, to enhance the sentence to the maximum, a higher sentence or order additional punishment where the law so provides. The Nairobi Centre for International	Let us simplify the penal code so that we don't have to create new laws every time a new medium of communication comes! Magistrates and Judges already have this power when sentencing, and as such this would serve as a further deterrent against criminals and discourage judicial officers from ordering the minimum penalties provided.

	Arbitration was established January vide the Nairobi Centre for International Arbitration Act and its board appointed by the President in June 2013. Its key functions include: promoting and encouraging international commercial arbitration; administering domestic and international arbitration, as well as other alternative dispute resolution (ADR) techniques, under its auspices etc. It is not clear though if the court is fully functional or competent to hear domain name disputes at the moment, given that it is still quite new and it may take some time before people take such cases before it.	
Article III – 50 *Each Member State of the African Union have to take necessary legislative measures to ensure that where the data held in a computer system or in a facility that allows for the conservation of computerized data in the territory of a Member State, are useful in revealing the truth, the investigating judge will issue a search or seizure warrant, to access or seize a computer*	**Question:** How would legislation be able to ensure that a data system hold CORRECT data?	This is problematic, because it requires a measure of truth, which is hard to actually legislate or determine owing to the relativity of truth. This sort of law would be basically unenforceable, and there would be no way to guarantee the actual truth of the data anyway. Consider alternative words in place of truth e.g. material facts

system or part of the system or any other computer systems where the said data are accessible from the original system or available in the initial system.		
Other arising issues	1. How will cross-border crimes be prosecuted? 2. Where this draft is in contradiction to local laws, which one will take precedence? 3. How are African states involved in the drafting? And which organizations/companies are involved at country? 4. It does appear that the AU convention does not substantially conflict with the Budapest convention. 5. The (European) Convention on Cybercrime is different from the (African Union) draft convention on the confidence and security in cyberspace. The former is somewhat about computer-related offences, content-related offences and offences	

	related to infringements of copyright and related rights. 6. It seems that the draft convention tries to cover consumer protection, intellectual property rights, personal data and information systems. It is a bit odd to mix all that with legislation to tackle activities which are legislated as criminal activities. The differences between the European convention and this draft AU convention are that the latter: - tries to solve the spam problem - includes electronic transaction - includes a legal framework for personal data protection The scope of the draft convention is broad. However, it does not have any text about lawful interception that can be used to address the problems the draft convention attempts to solve. The drawback is that it might entail less personal data protection.	The sections on data protection, copyright bolted on, and electronic transaction security / spam are specifically referenced here rather than implied in the Budapest convention (where it is quite possible to have inter agency cooperation across countries to arrest a criminal spammer, and this has happened in the past). This may be attributed to the unique needs of Africa. When you have a convention you need enabling legislation around it, which if it does not exist, has to be drafted from scratch, and hopefully drafted so as to be harmonized with the laws drafted by other signatories to the convention. The differences pointed out are related to the maturity level of the laws in various African countries.

	The convention as it is can force reforms at both international and national levels because of its cascading effect. This is the explanation: Once signed nations will endeavour first: to put in place local laws that support compliance with the convention; and second, and also most importantly to enforce these laws for fear of international/continental repercussions of in-action. Because our regulators and other government bodies don't report to a higher power in a real sense, there is usually less incentive for them to crack the whip on content and service providers. However this will change once they are bound by the convention. When you look at spectrum management and other areas where regulators are accountable to higher powers you can tell that this, if done well might just be what saves the day.	The advantage of joining the Budapest convention is harmonizing the local law with those of several countries around the world and also joining a network of Mutual Legal Assistance Treaty (MLATs) that make it easier for a country to pursue cybercrime cases where the offender lives in another country that is a signatory to the convention.

4. General Remarks

- Some of the provisions appears to be a copy and paste from various first world legislation and yes, in an African context some of it may be risky. African countries need most of them for a functioning legal framework for cybercrime. In certain sections, the wording is fuzzy and prone to multiple interpretations. However, it would be good to suggest that appropriate controls / checks and balances be put in place before the treaty is adopted and implemented, rather than to oppose them altogether.
- Some of the laws are already in existence in partner nations but there are weak mechanisms for implementation. There is need to find methods of enforcing them and educating the masses about their rights. There is therefore, need for government commitment and involvement in the implementation of those laws. Little can be done by the various stakeholders if there is minimal commitment from government to implement the laws.
- The greatest challenge faced by the users is ignorance of the law. In ignorance they are eaten up slowly by the vice of the spam. As long users receives messages that they have not consented to, then they are being spammed. Awareness and capacity building is a needed to fight ignorance. It is needed in all aspects of implementation of policy and law.
- **The AUC urgently needs to engage with industry and civil society to find and provide a workable framework for the Convention.**

References

Draft African Union Convention on the Confidence and Security in Cyberspace
http://pages.au.int/sites/default/files/AU%20Cybersecurity%20Convention%20ENGLISH_0.pdf
http://daucc.wordpress.com/

STOP THE RATIFICATION OF THE AFRICAN UNION CONVENTION ON CYBER SECURITY
http://www.thepetitionsite.com/takeaction/262/148/817/

Basic drawbacks of the Draft African Union Convention on the Confidence and Security in Cyberspace
http://daucc.wordpress.com/2013/10/29/paper-review-basic-drawbacks-of-the-draft-african-union-convention-on-the-confidence-and-security-in-cyberspace/

http://michaelmurungi.blogspot.com/2012/08/comments-on-draft-african-union.html

Letter to African Union: http://daucc.wordpress.com/2013/11/25/cipits-letter-to-the-african-union-calling-for-stakeholder-input-on-the-african-union-convention-on-cyberspace/

Self-Regulation: http://www.iab.net/public_policy/self_regulation

DotConnectAfrica Comments to the Draft African Union Convention
http://www.dotconnectafrica.org/wp-content/uploads/2013/10/DotConnectAfrica-Comments-to-the-Draft-African-Union-Convention-on-the-Establishment-of-A-Credible-Legal-Framework-For-Cyber-Security-In-Africa-October-2013.pdf

Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'
http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html