Report on Online Discussions on Promoting Internet Freedoms in Africa
November 11 – December 6, 2013

Prepared by:

This report has been developed in collaboration with the Paradigm Initiative Nigeria (PIN) as part of the Cyber Stewards Network funded bythe International Development Research Centre (IDRC), Ottawa, Canada.CIPESA's OpenNet Africa project is aimed at promoting online freedoms in Africa and is also supported by FIRE and HIVOS.

Background

Africa's internet usage continues to grow steadily, with an estimated 16% of the population on the continent using the internet. The increased availability of affordable marine fibre optic bandwidth, a rise in private sector investments, the popularity of social media and innovative applications, and increased use of mobile phone to access the internet, are all enabling more people in Africa to get online. In turn, there are numerous purposes to which users in Africa are putting the internet-from mobile banking, to connecting with fellow citizens and leaders, tracking corruption and poor service delivery, innovating for social good, and just about everything else.

The increasing usage of the internet, however, has in some countries attracted the attention of authorities, who are eager to provide limitationsto the openness of the internet and the range of freedoms which citizens and citizens' organisations enjoy online. The popularity of social media, the Wikileaks diplomatic cables saga and the Arab Spring uprisings have led many governments including those in Africa to recognise the power of online media. In a number of African countries, there are increasing legal and extra-legal curbs on internet rights, in what indicates tougher times ahead for cyber security.

The Collaboration on International ICT Policy in East and Southern Africa (CIPESA) and Paradigm Initiative Nigeria (PIN) co-hosted an online internet freedom discussion during November and December 2013. The purpose of this forum was to attract discussions from key ICT experts both within and outside Africaon key online safety matters onthe continent.

Discussions were hosted on selected online platforms in Uganda, Kenya, Nigeria and a mailing list comprising of African Internet Governance experts. The platforms were:

- Association for Progressive Communications (APC) AfricanInternet Governance Mailing List
- Kenya ICT Action Network (KICTANet) mailing list
- Information Network (Uganda) mailing list
- Naija IT Professionals mailing list
- West African IGF mailing list
- Freedom of Information (FOI) Coalition (Nigeria) mailing list

The lists were moderated by a representative from both CIPESA and PIN. Each week, a new topic with guiding questions was introduced on the listserves and a summary of responses provided at the end of each week.

The outcomes of these discussions will inform the work of CIPESA, PIN and their partners that are working in the area of online freedoms.

Discussion Outline

Discussion Topic	Questions Explored
Week 1: ***Status of Internet Freedom in African Countries***: Freedom of expression both online and offline; Internet intermediary liability; censorship and surveillance incidents; regulations, laws and policies governing freedom of expression online and perspectives on the African Convention on Cyber Security.	1. What are the major issues surrounding online freedom of expression in Africa? 2. What convergences and tensions exist between freedom of expression and privacy? 3. What are the implications of approaching the balance between freedom of expression and privacy from a freedom of expression–centric point of view? 4. What actions can governments, civil society, media and the private sector take to balance privacy with freedom of expression online? 5. What is the best way to empower users to stay safe online while protecting their freedom of expression?
Week 2: ***Global Surveillance Revelations and Impact on Africa***: incidents like the NSA/Edward Snowden drawing lessons for Africa stakeholders i.e. governments, activists, CSOs and private sector; how to balance privacy while maintaining security for citizens.	1. What can African governments learn from the NSA surveillance and Snowden revelations? 2. What are the current technology trends and which cybersecurity threats raise the greatest concern? 3. How are evolving Internet services and technologies, such as mobile and cloud computing services, affecting these security threats? 4. Is there any country data, across the continent, on how surveillance has really helped to curb – or prevent – acts of terrorism? 5. Are African countries spying on each other? Are there countries that have shown a tendency to breach the rights of other sovereign nations on the continent?
Week 3: ***Best Practices on Internet Policy in Africa***	1. What policies are working in your country and what needs to be streamlined or strengthened? 2. Are there African countries that offer a model, or close enough to Best Practice scenarios that can be highlighted for other countries to learn from, or emulate 3. What are the signs to look out for in our various countries' ICT policies, to be sure that the country plans to improve Internet Freedom? 4. What worked well for countries that have shown steady progress in the annual Freedom House ratings? 5. What can other countries learn from those that have, or are developing, crowd-sourced (and citizen-led) Internet Freedom Charters?
Week 4: ***Recommendations for Africa***: ways to improve internet security, data and privacy protection in Africa.	1. What elements need to be put in place to ensure all Internet users (including citizens, companies, government, etc) continue to have confidence in the Internet? 2. How can African civil society organisations engage ICT policy processes to ensure that rights are not traded for security? 3. Considering the ongoing discussions around the African Convention on Cybersecurity, what recommendations should be made to improve the text? 4. How do activists and rights' advocates protect themselves in scenarios where government clampdown could affect their work? 5. Should African academia incorporate this new reality into classroom discussions? If they should, is there a model to learn from?

Analysis of responses

On the ***Status of Internet Freedom in Africa***:It was observed that there is increased government monitoring of citizens'internet traffic both in Africa and beyond. Drawing from the Freedom House reports on internet freedoms in 2013, respondentsnoted that the report is not only reflective of the restriction on online freedoms by various countries but it is also able to dwell onother underlying issues like surveillance."Even the seemingly free [countries] are not totally free not just in Africa but even in Europe and America," noted one participant.

The growing development and encouragement to build national Internet Exchange Points (IXPs) in Africa was also pointed out as a mechanism through which governments will easily be able to monitor and to some extent control internet access in a given country. Although IXPs in some countries are not governed by the state and subscription is voluntary, the centralised routing of local traffic in some countries may provide for easier interference by authoritarian regimes.

Also as shown in the Google transparency reports, the number of governments requesting for data about online users has doubled in the last three years (2010 - 2012). It was observed that although a few requests came in from Africa, it shows a cause to worry as some of the requests for content removal may be politically motivated.[1]

While discussing scenarios on the negative impact of the internet on African countries, it was noted that Kenya has a challenge of hate speech while Nigeria is faced with 419scams.Hate speech is outlawed in Kenya and surveillance of online users in relation to divisive language has been on the risesince the 2007 post elections violence. However, it should be noted that no cases have been registered where the government has tried to muzzle freedom of expression online if the freedom was exercised within the confines of the law. Nonetheless, one respondent shared that a Kenyan blogger was accused in court for allegedly publishing on his Facebook account content that was deemed to set two communities against each other.

Meanwhile, in Uganda, politically motivated interference with citizens'access to the Internet was highlighted with the 2012political opposition led 'walk-to-work' campaign during which the national communications regulator (Uganda Communications Commission) ordered ISPs to block access to Facebook and Twitter.

Responding to the question on what convergences and tensions exist between freedom of expression and privacy, one participant observed that user interaction online and information flowwas beyond national borders and any government restrictions would be "superficial". A question on "How much can you restrict if those with no restriction can interact with and pass on information to the restricted using alternative methods of communication?" was also raised.

It was also noted that with regard to online privacy a challenge exists in determining how much we can actually do vis-à-vis how much we want to do online.It is therefore important to give thought to what we do, say and who accesses our material online because of the endless possibilities that convergence [of both online and offline media] brings. A respondent shared that "If online actions done in private are seemingly harmless to freedoms of others we should think through the related restrictions. However, if the freedom of expression online hinders other freedoms, perhaps we need

[1]Online Freedoms Under Siege as African Countries Seek Social Media Users' Information, http://opennetafrica.org/wp-content/uploads/researchandpubs/Online%20Freedoms%20Under%20Siege%20as%20African%20Countries%20Seek%20Social%20Media%20Users'%20Information.pdf

to rethink how we go about these issues."Another respondent stressed that the tensions and conflicts between privacy and freedom of expression are thus ever present. Seemingly, what we do online is often a reflection of our realities offline.If online actions done in private are seemingly harmless to freedoms of others, thought should be given when applying the related restrictions online.

On how to develop the best way to empower users to stay safe online while protecting their right to freedom of expression, respondents observed that countries with recognised internet freedoms tend tohave an open democratic space that allows their citizens to express themselves. That "freedom comes with responsibilities, and good leadership entails mentoring and providing a general vision to the populace that enables them to take advantage of freedom for their development." The challenge is therefore to continue promoting responsible use of the freedoms provided by the internet.

The African dilemma of governments using cybercrime monitoring as an excuse to create tight measures on freedom of expression is highlighted by another respondent, "we want freedom and not the responsibility it carries. Africa therefore needs to deal with the issue of cybercrime so that those concerned with restrictions find a middle ground." Besides, data privacy in Africa will be cryptographically enforced by conscientious citizens, noted another respondent.

Global Surveillance Revelations and Impact on Africa: It was heard that there are some African countries attempting to deploy surveillance technology without fully understanding the implications ofthis technology to social economic development .For instance, in Nigeria works to install an Internet Spy facility provided by Elbit Systems were reported to be underway.[2]And in Uganda a revelation by the Security Minister to create a social media monitoring centre to curb cyber security while bolstering national security was made in early 2013.

In regard to such trends, African governments were cautioned to learn that surveillance can only cause a negative impact on innovations from internet users. That surveillance could also "indirectly" slow-down internet business development on the continent as new service providers may not want such to happen on their networks. That governments should thus learn that, for a continent like Africa, surveillance into a fast growing internet community will only slow down its pace. Thus the key to maintaining this growing community is by ensuring that the basic principle of openness that guides the internet is maintained.

Still another respondent shared that the challenge faced is with 'Digital Content' Vs 'Creators' and 'User Attitude' at local (content root/source) and global (consumer/Access) levels. According to him, "the core challenge is the acceptance model to design a global standard for 'Trust Architecture'. Central to this is "Culture of tolerance and Peace" - and in-between is a mirage of group-interest illusions within African nations and their 'myopic' institutions." Thus the challenge in Africa is the bridge or absence of bridges between the various interests groups.

On current technology trends and which cyber security threats raise the greatest concern for Africa, a participant identified the "rapid growth of the 'un-educated/un-aware' Africa internet user community as one of the major treats to cyber security. That many people are not aware of the need for privacy on the internet and those who are aware donot know how to securely use the internet.Another respondentsaidthat "several foreign websites were blocking Nigerian traffic" due to cyber crime in the country and that Nigerians use proxies and Onion routing based products to circumvent these restrictions. Further, it was heard that in some parts of Lagos, youths were being

[2] http://shar.es/DgwQt

targeted by authorities, who seize their laptops and smartphones on allegations of involvement in online fraud. Such acts according to this respondent show the absence of structures on the ground to educate the regulatory authorities on what constitutes surveillance and what constitutes outright denial of basic freedom to citizens.

While responding to the question on how evolving internet services and technologies, such as mobile and cloud computing are affecting these security threats, it was shared that most cloud services are engaging in unified mobile integrations/solutions. For instance, with the Google all-in-one account sign in and social networking sites like Facebook, Twitter, Instagram integration apps, comes an increase in privacy and data protection.

There was no particular mention on how internet surveillance has been used to curb – or prevent – acts of terrorism on the continent or how African countries are spying on each other. However, further research on the two topics was suggested.

Best Practices on Internet Policy in Africa: Respondents pointed to the need for progressive legislations that not only recognise the internet as a useful resource but also protect against its misuse. Kenya's Information and Communication Act, 2009 was highlighted for addressing the issue of hate speech on the internet but at the same time criticised for its vague provisions. Its Section 29 states that *"a person who by means of a licensed telecommunication system a) sends a message or other matter that is grossly offensive or of an indecent, obscene or menacing character, or b) sends a message that he knows to be false for the purpose of causing annoyance, inconvenience or needless anxiety to another person commits an offense and shall be liable on conviction to a fine not exceeding fifty thousand shillings, or to imprisonment for a term not exceeding three months, or to both."*

One respondent was concerned that the term *"a licensed telecommunication system"* seems to be misplaced. That if an unlicensed system or a system was used to promote divisive speech outside Kenya, then the law wouldn't prevail.

Respondents also shared views on theproposed Africa Union Cyber Security Convention (AUCC) and focus was placedon particular articles that have been identified to infringe on privacy and freedom of expression of users(See report on the AUCC discussions: http://opennetafrica.org/civil-societys-proposals-on-the-african-cybersecurity-convention/.

Participants expressed concern that legislation similar to this one have been put in place in many African countries but thechallenge is always with implementation and willingness of some service providers to support the implementing powers to see these laws work.One participant summarised it as follows: "Because our regulators and other government bodies don't report to ahigher powerin a real sense, there is usually less incentive for themto crack the whip on content and service providers. However this willchange once they are bound by the convention."

Recommendations

Make Internet access a constitutionally ratified fundamental Human Right in preparation for an 'always on' knowledge society. This is a scenario in which an internet user is always connected to the internet even when they are not using it. It is unlike connecting to the internet on a 'need to' basis in a bid to save resources.

- Negotiate the limits of individual rights, community rights and universal rights within the context of life and property - in relationship with Individual Security and that of Constituted Authority's limits to the protection of life and property.

- A declaration on the proposed Africa Cyber Security Framework is required as Africa must get IT Policy Framework right before getting other potential segments right. This is a strategic imperative to ensure sustainability before we engage the sub-sets. Cybersecurity is and should indeed be viewed, organised and implemented as a significant sub-set of a holistic IT Ecosystem. How these subsets such as institutional frameworks, IT Education, Cyber-security Domain, e-Transaction, etc., are importantto the application of the Super-Structure Framework is entirely another matter.

- Internet rights activists and advocates need to work together in building a robust open and accessible internet. Bridges and partnerships need to be put in place between private institutions and civil society organisations to lobby governments and state institutions in order to improve what needs to be at all levels.

- Africa needs to define what her interests on the internet are in order to protect these interests. An investment in IT development and progress may not reside in the conventional law of "market forces" alone. Thus an innovative knowledge-conversion strategy to compete in the Information Society is required than the conventional/traditional education methodology.

- Governments should not strip away the power of the internet and abuse the privacy of the citizens under the guise of fear of uprising and security reasons. In such instances, governments should do so with efficient creations of laws, regulations and internal consultation with other stakeholdersso that people aware of their rights.

***Emerging questions**:* these were raised during discussion but did not yield responses.

- Are restrictive governments up to date with technology on surveillance?
- How does one remove content which is on distributed systems, and being shared using different platforms like Whatsapp, Facebook and sites built for their own purpose?

Materials shared:

http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

http://falkvinge.net/2013/11/19/swedish-regime-to-give-police-customs-tax-authorities-realtime-access-to-citizens-phone-mail-more/