Forum on Internet Freedom in East Africa (FIFEA) 2015

Summary of Proceedings
November 2015

Supported by:

FORDFOUNDATION
Hivos people unlimited
OPEN TECHNOLOGY FUND
ACML AFRICAN CENTRE FOR MEDIA EXCELLENCE
UNESCO

Contents

Introduction 3
Why we Need a Forum on Internet Freedom 4
Electioneering and Extremism in the Digital Age 4
Media Role in Promoting Internet Freedoms 6
Internet Freedom Perspectives of Human Rights Defenders and Activists 8
The State of Internet Freedom in East Africa 2015 country insights 9
Bridging the Gap Between Techies and HRDs 10
Non-Adoption of Digital Safety Tools: 11
Understanding Creative Expression Online 12
Violence Against Women Online 14
Marking a Decade of the Access to Information Act in Uganda 15
Cybercrime vs. Internet Rights in Africa 17
The Economics of the Internet 18
Recommendations 20
Conclusion and Way Forward 20
Participants' Thoughts and Highlights 20
Media 21

Introduction

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA), under the OpenNet Africa initiative, held the second Forum on Internet Freedom in East Africa on September 28–29, 2015, at the Golf Course Hotel in Kampala, Uganda. The two-day forum coincided with the International Right to Know Day.

The Forum discussed the state of internet freedom in Africa, including threats, emerging issues, and opportunities for action to promote access, privacy and security online. The Forum was also used to launch the 2015 edition of the State of Internet Freedom in East Africa report, which is centred on citizens' knowledge and perceptions of internet freedom and the effect of information controls on the online behaviours and freedom of expression for ordinary citizens, journalists and human rights defenders.

The Forum was supported by the Ford Foundation, Hivos, the Open Technology Fund, Web We Want, the African Centre for Media Excellence (ACME), and UNESCO East Africa Sub-Regional Office. CIPESA also partnered with the Africa Freedom on Information Centre (AFIC) in the commemoration of the tenth anniversary of the Access to Information Act (2005) in Uganda.

The Forum brought together 200 human rights defenders, journalists, government officials, bloggers, developers, and representatives from academia, the arts community, law enforcement agencies, and communication regulators from 18 countries. This tripled the number of those who attended the inaugural 2014 forum, which hosted 85 participants from six countries.

Countries represented at the 2014 forum	Countries represented at the 2015 forum
Burundi, Kenya, Nigeria, Tanzania, Rwanda, and Uganda.	Burundi, Cameroon, Democratic Republic of Congo, Ethiopia, Germany, Italy, Kenya, Nigeria, Rwanda, Tanzania, South Africa, South Sudan, Sudan, Somalia, Uganda, United Kingdom, United States of America, Zambia

There were 13 panel discussions which took place over the two days and each explored a different facet of internet freedom. Panelists represented a diversity of backgrounds, positions and organisations working both directly and indirectly on internet freedom, which contributed to vibrant discussions across the entire Forum program.

Among other, panelists came from Article 19, Association for Progressive Communications (APC), Bayimba, Bloggers Association Kenya (BAKE), East and Horn Human Rights Defenders Project, ICT Association Uganda (ICTAU), Globaleaks, iHub Research (Kenya), Internet Society (Africa, Burundi, Uganda, and U.S.), Facebook, and Kenya ICT Action Network (KICTANet). Others were from Makerere University, Media Council of Kenya, Media Institute of Southern Africa (MISA), Ministry of ICT (Uganda), the National Coalition of Human Rights Defenders-Kenya, Open Technology Fund, Paradigm Initiative Nigeria, Protège QV of Cameroon, Uganda Communication Commission (UCC), Ugandan Police Cyber Crime Unit, Uganda Media Centre, UNESCO, University of Nairobi, Web We Want, Writivism and Women Of Uganda Network (WOUGNET).

Online engagement: Live streaming of the Forum proceedings allowed stakeholders that were not able to physically attend the event to follow the proceedings remotely. On social media, the hashtag #FIFEA was used to reach an online audience through the @cipesaug and @opennetafrica accounts.

Why we Need a Forum on Internet Freedom

Africa has registered a rise in abuses and attacks on internet freedom, including a proliferation of laws, legal and extra-legal affronts, as well as limited judicial oversight over surveillance and interception of communications. However, there is widespread lack of knowledge on what constitutes internet freedom, coupled with limited skills and information about threats to online safety.

In his keynote address, Jaco du Toit, Adviser for Communication and Information at UNESCO Regional Office for Eastern Africa, noted the importance of bringing together stakeholders in East Africa to discuss the limitations on the rights of citizens and governments' increasing efforts to monitor and control digital communications. He noted that the rate of internet penetration in Africa nearly quadrupled between 2007 and 2012. However, this increased number of internet users adds to growing concerns about the poorly understood area of mass surveillance and monitoring mechanisms that undermine the rule of law and democratic principles by intruding on citizens' privacy.

He also pointed out that African authorities are resorting to more direct forms of internet censorship, such as the harassment or arrest of bloggers and online journalists, rather than using sophisticated Uniform Resource Locator (URL) blocking or systematic filtering, as many still lack the technical capability to do so.

Discussion on the importance of a free internet should go alongside efforts to address access and infrastructural challenges that keep costs high and thus limit internet use to a minority as highlighted by Crystal Simeoni, Projects Coordinator with Hivos East Africa. Simeoni noted that East African governments are increasingly effecting controls on the use of the internet under the guise of fighting terrorism, child pornography and cybercrime. She added that this is a practice that needs to stop for the internet to be fully recognised as a valuable tool for development.

In his opening remarks, Dr. David Turahi, Director of Information Technology with the Ugandan Ministry of ICT, stressed the role of the internet as an enabler of development, and in the Ugandan context it was a key platform where a lot of conversation on society, economy and politics was taking place.

In order to enjoy the opportunities presented by the internet, Solana Larsen and Renata Avila of Web We Want emphasised the need to develop the capacity of users in securing their rights online. They highlighted simple strategies on creating awareness on digital rights in the global South, based on a Cookbook titled Recipes for a Digital Revolution. "It takes a community, it takes volunteers and it takes collaboration with people outside of the usual circles" to advocate successfully for internet rights, they said.

For Africa, Wairagala Wakabi from CIPESA noted, the conversation on the need to promote internet freedom is crucial and the Forum serves as one of a kind on the continent committed to advancing an understanding and upholding of internet freedom. The Forum is building a network of African actors to promote internet freedom for a range of civic actors such as journalists, bloggers, human rights defenders, sexual minorities, women, and political actors.

Electioneering and Extremism in the Digital Age

Election periods are often characterised by excitement and anxiety as citizens go to the polls to have a say in determining the leadership of their countries. Increasingly, candidates are utilising digital technologies for their campaigns, while civic groups and citizens are also using ICT to discuss candidates' campaign manifestos and issues they want addressed in the elections. Although ICT can generate greater transparency during election periods and increase citizens' access to information on political issues, it also has its downsides. In recent years, election periods have come hand in hand with a spike in misinformation, defamation and hate speech online, particularly on social media platforms. Infringement on press freedom also tends to increase around this period, as does self-censorship by netizens who fear attracting reprisal from authorities. This session explored the tensions between the right to free expression online and extremism in the digital age.

Electioneering and Extremism in the Digital Age Panelists: L-R: Emma Belinda Were (Uganda Media Centre), Nanjira Sambuli (Umati/ iHub Research Kenya), James Marenga (NOLA Tanzania), Gbenga Sesan (Paradigm Initiative Nigeria)

Issues Raised

Navigating social media: Politicians are increasingly utilising social media to reach their audiences; conversely, citizens have more access to candidate information now than in previous elections. Social media has created an avenue for the flow of both legitimate information and misinformation. Despite increased use of the online platforms, governments remain unsure of how to address the flow of 'misinformation' and often revert to control rather than regulation. Governments have yet to find a way to regulate or monitor the flow of "false information", especially in election times, without imposing overly restrictive measures that lead to censorship and self-censorship. These measures often include closure of media even if freedom of expression and of the media is guaranteed in national constitutions.

Fast tracking laws: In East Africa, many recent laws negate rather than safeguard internet freedom. Some of the laws proposed in election times undermine access to information, as was seen in Tanzania with rushed enactment of the cybercrime law, and the draft access to information and media services laws unveiled just before the October 2015 elections. Other laws passed in reaction to events in society such as terrorist attacks also tended to undermine freedom of expression. For instance, following the terrorist attack at the Westgate mall and attacks on buses by Somalia-based Islamic militant group Al-Shabaab, the Kenya Security (Amendment) Act, 2014 was passed. Earlier, Uganda's Regulation of Interception of Communications Act, 2010 was passed in haste following bomb attacks on revelers watching the World Cup finals in the capital Kampala in July of the same year. The process of drafting these laws and their eventual enactment comes with little stakeholder input.

Curbing Hate Speech: In the aftermath of the 2007/8 post-election violence in Kenya**,** which government officials said was fuelled by SMS, the National Integration and Cohesion Act (2008) was enacted in a bid to prevent the spread of hate speech, including through digital tools. The Act has since been used to charge bloggers and journalists for their online activity. The definition of what constitutes hate speech is ambiguous, leaving room for abuse of the Act. Nanjira Sambuli of iHub Research said during Kenya's 2013 elections, the media aimed to repress online ethnic tensions at all costs in a bid to prevent a repeat of the post-election violence of 2007.

Transparency: The need for access to information especially during election times was highlighted as integral to maintaining government credibility. Gbenga Sesan from Paradigm Initiative Nigeria (PIN) recounted how Nigerian citizens went online with the campaign "#OccupyNigeria" calling for transparency and accountability in government activities in response to corruption concerns in the fuel and petroleum industry.

Governments should not have to block and censor websites and social media platforms during times of political instability. Instead, there should be more proactive release of information, and governments should be more responsive to concerns raised and provide counter arguments where there is mis-information. As such, there is a need for transparency to ensure that government conduct in monitoring communication can be held accountable.
Moreover, there are few legal measures, if any, which citizens can take to ensure their liberties online are protected, including on issues of hate speech, surveillance, and freedom of expression. This threatens the extent to which

legitimate participation takes place online especially on sensitive topics related to elections, politics and politicians. However, users were urged to verify claims, exercise judgment try to verify information for accuracy and the credibility of the source before re-sharing it.

Surveillance: In many instances of abuse of online rights and monitoring of citizens' communications, national security is used as a justification. The legal term 'national security' is broad and open to abuse. Participants argued that online surveillance on the continent was often justified by governments with reference to similar practice in Western countries. However, many Western countries have data protection laws and citizens have some level of legal recourse, measures which are often absent in Africa. It was also highlighted that surveillance practices online were a reflection of what was taking place offline and could not be viewed exclusive of each other. It was important therefore to understand what was taking place offline that also proliferated into online forums, such as gender disparities, ethnic tensions, and crackdowns on political assembly.

Gender: The gender inequalities that exist offline are transferred online and as such fewer women participate in online political discourse. Political conversation remains largely male dominated. Furthermore, violence against women online was said to sometimes lead to women opting out of participating in online discourse.

Recommendations

- More citizens should be enabled to access and utilise online tools and platforms. As such, capacity and awareness building on the use of digital security tools as enablers of civic participation during elections should be pursued. Further, there should be a move to encourage women to stay online - even when attacks are made against them - through digital safety and advocacy for policies that better protect women online.
- The use of counter speech and transparency to combat hate speech, misinformation and false claims can limit the opportunities for the imposition of tougher measures that limit online freedom. Availing relevant content is a shared responsibility between citizens and government, so governments should provide proactive and factual information to limit the spread of false information.
- Citizens should take a more active stance to keep governments in check and to prevent information "control" from being the recourse that is taken especially during times of unrest.
- Laws should be more in line with the changing technologies as, currently, many laws are outdated or do not adequately address digital technologies.

Media Role in Promoting Internet Freedoms

The media plays the integral role of society's watchdog that promotes vigilance towards the rule of law and accountability of public institutions. In recent years, the way in which the media sources and delivers information has changed in tandem with advancements in ICT. Increasingly, the public is actively contributing to content shared through digital platforms and in mainstream media. However, in some African countries online media and users of social media are becoming targets of internet freedom abuses and violations. This panel explored possible ways in which the media can advance internet freedom in Africa.

Panelists

Eric Chinje, Africa Media Institute (Moderator) | Victor Bwire, Media Council of Kenya |Collin Akim Lasu, Association for Media Development in South Sudan | Robert Mugabe, Great Lakes Voices Rwanda | James Wamathai, Bloggers Association of Kenya | Jean Claude Kavumbagu, NetPress Burundi | Alexandre Niyungeko, Burundi Union of Journalists | Anteneh Abraham Babanto, Ethiopia National Journalists Union | Paul Kimumwe, African Centre for Media Excellence

Issues Raised

Poor appreciation of internet freedom: The media is presently not playing a sufficient role in creating awareness and advocating for internet freedom. This is mainly because journalists have a limited understanding of what internet

freedom entails and how it affects the media and society at large. Too often, the media views internet freedom as just a connectivity issue not as an all-encompassing concept that includes unbridled privacy, access to information and freedom of expression. On the other hand, in some countries media is sometimes viewed as trying to instigate the overthrow of the government as opposed to being society's watchdog and in many instances the media are threatened, harassed and face closure due to the content published.

Limited online content: Although radio remains integral to the dissemination of content in Africa, issues of limited internet access, language, and illiteracy contribute to the exclusion of many from popular online narrative. Radio stations, however, often rely on online content to fulfil their role as information disseminators.

For many African countries, the diaspora community maintains a keen interest in the affairs of their home countries, often relying on online content and increasingly streaming online radio. However, for countries with limited infrastructure or tight information controls, the online content is limited and in instances it is skewed in favour of the government.

Internet access limitations: in some African countries such as South Sudan, few citizens are internet savvy and internet infrastructure is scanty. Limited internet access and infrastructure also impacts upon the information which is disseminated and consumed in authoritarian regimes. An Ethiopian participant observed that with no private television station, four FM radio stations and about 15 newspapers – all concentrated in Ethiopia's capital Addis Ababa - "most of the country has no free radio station and limited newspaper distribution." As such information distribution across the various media platforms was limited. Kenya and Uganda were said to have a better balance between traditional media and the Internet which enjoyed a mutually beneficial relationship.

Although Rwanda has far-reaching internet infrastructure and high access rates, a very restricted traditional media environment was extended into the online sphere. This was the case too for neighbouring Burundi. Meanwhile, Ethiopia had a tightly controlled internet infrastructure and poor access as the government retains a stranglehold on the internet with websites considered hostile being blocked and bloggers harassed and arrested.

Online ethics: Panellists noted that a key foundation to internet freedom is using the internet responsibly. However, the way in which some journalists have violated traditional media ethics by not verifying information sourced online and consequently disseminating false information has damaged their credibility and provided an opportunity to governments to clamp down on media freedom.

It was noted that the practices exercised in traditional journalism should be maintained when online tools are used, including protecting sources and verifying information. "In Kenya there is an ongoing promotion of responsible use of the internet. This includes training journalists on what are good online reporting standards, of which a key outcome has been the adoption of online editorial policies by various media houses," said James Wamathai of the Bloggers Association Kenya (BAKE), on the need to promote ethical standards in order to keep online content credible.

Recommendations

- Call on the media to actively pursue more coverage on internet freedom such as reporting on initiatives upholding online rights, the laws governing these rights, documenting and flagging cases of persecution and intimidation of internet users.
- There is need for awareness raising among media about the dangers of compromised security of online communication and highlighting the rights of internet users as this impacts upon the security of sources both online and offline, whistle blowers and investigative journalists.
- Responsible, balanced and accurate journalism should be maintained even when using online based content and sources. The verification of information remains an important aspect of journalism and should be pursued at all times even when information is sourced through social media.

Internet Freedom Perspectives of Human Rights Defenders and Activists

Advocacy for human rights is taking place in a myriad ways in the online space, ranging from crowd funding initiatives, Twitter campaigns, to signature gathering to raise awareness of socio-economic concerns. However, various laws and actions appear to shrink the space for human rights defenders (HRDs) and activists. Panellists discussed the current landscape in which HRD groups work and how they can contribute to the advancement of Internet Freedom and the promotion of social inclusion, democracy, and good governance.

Panelists
Emilar Vushe, Association for Progressive Communications APC (Moderator) | Nicholas Opiyo, Chapter 4 | Richard Lusimbo, Sexual Minorities Uganda (SMUG) | Helen Mwale, Media Institute of Southern Africa (MISA) Zambia | Gaius Kowene, Goma Web Activism Summit/ Yole!Africa DR Congo

Issues Raised

Rising attacks vs. limited use of digital safety tools: ICT is a double-edged sword; it can be used to amplify rights concerns but also leaves one susceptible to risk - especially HRDs. It has exposed HRDs to more avenues for attacks such as website hacks and communication tracking. Online information is used as a tool to infringe the rights of others such as by publication of private content, demeaning sexual statements, and unfounded accusations. This abuse is committed by the media, citizens, and government. In some countries, the use of digital tools to harass activists and human rights defenders is rising. In South Sudan, online attacks are minimal but physical threats via phone, threats made at places of residence, police intimidation, and unlawful detention are rife.

Discussion also centred on the concern that there is limited familiarity with digital security tools amongst HRDs and even fewer are utilising them due to a perceived technical savviness required to use them.

Unsupportive legal structures: In many countries, HRDs are viewed with suspicion by the state, sometimes falling victim to online harassment, blackmail, humiliation and physical attacks on their persons or property both online and offline. Panelists pointed out that in many developing countries, the judicial system still lacks sensitivity towards some of the issues they work on, such as abuse based on gender and sexuality, with victims sometimes taking the blame or lenient sentences being handed to perpetrators of crimes. It was noted that in many African countries, HRDs working on sexual rights were under increasing attacks from non-state actors due to homophobic perceptions that lesbian, gay, bisexual, transgender, queer and intersexed (LGBTQI) individuals were “un-African”.

Discussion also focused on the legislative limitations which are increasing and threatening to shrink the work of HRDs, such as the Public Benefit Organisation Act (2013) in Kenya and the NGO Bill in Uganda, which places limitations on the operations of civil society.

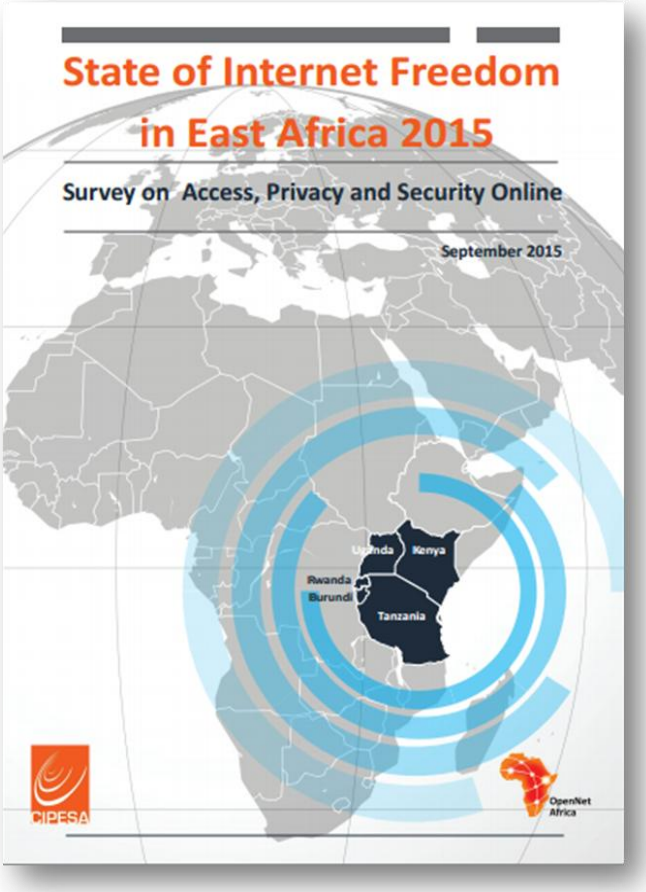
Strengthen networks of HRDs: Participants highlighted the need to adopt a cohesive framework to advance human rights both online and offline, comprised of HRDs across all levels of society. This can be enabled by increasing knowledge sharing on issues such as gender, sexuality, freedom of expression, privacy and hate speech.

The struggle that many human rights organisations face for financial sustainability was brought up with some HRDs pointing out that high internet costs and unreliable connectivity impact upon their operations. While public spaces like libraries and schools may provide access to internet and information for human rights defenders, anonymity cannot be guaranteed when using such public spaces. There was a call for continuous engagement and awareness about the importance of shared responsibilities between governments and civil society in addressing human rights issues online.

Recommendations

- Develop comprehensive legal frameworks to protect all citizens regardless of race, religion and sexuality to ensure protection for vulnerable communities and HRDs. This should be supported by augmenting the legal implementation of safeguards for data privacy.
- There should be a concerted effort to popularise digital safety tools amongst civil society players as more tools are available and are getting easier to utilise.
- Develop a cohesive network of HRDs that allows CSOs to raise awareness for their causes and to pursue linkages through the network.

The State of Internet Freedom in East Africa 2015 Country Insights



The Forum served as a platform for the launch of the State of Internet Freedom in East Africa 2015 report. This is the second edition of the report and this year focused on Access, Privacy and Security Online in Burundi, Kenya, Rwanda, Tanzania and Uganda. It builds upon the 2014 report which was an Investigation Into The Policies And Practices Defining Internet Freedom in East Africa.

Researchers on each of the countries shared some country insights revealing shared concerns such as mistrust and suspicion of governments on mass surveillance and privacy infringement and limited awareness of safety tools. A limited understanding of what constitutes internet freedom was noted in all countries covered by the report.

Burundi

Jean Paul Nkurunziza, ISOC Burundi Chapter Vice President, noted a challenge in getting respondents due to the political instability that coincided with the research. Shortly before the Burundi elections, there was a coup attempt which saw media houses shut down (many remain closed). However, respondents who participated in the research feared that government was monitoring their communication, and felt there was a need for judicial oversight in monitoring of citizens' communication. Meanwhile, the cost of internet access remains restrictive and policies need to be put in place to enable cheaper access.

Ethiopia

The country is still classified as the most repressive when it comes to internet freedom in Africa, in part due to the monopoly of the telecommunications service provider Ethio Telecom. This has led to many websites being hosted outside of the country in a bid to avoid takedown and content filtering. Many websites, both local and international, are blocked in Ethiopia. Currently, there is no legislation to safeguard against the infringement of rights, and there is rampant persecution of bloggers and journalists who voice anti-government positions.

Kenya

Grace Githaiga of the Kenya ICT Network (KICTaNet) noted that the Kenyan parliament needs to update and enact laws that are in line with and uphold the country's constitution. She noted that the Security Amendment Act, 2014 poses a threat to press freedom and access to information. She added that as the arraignment of

bloggers, requests for information, and take down requests by the Kenya government increase in number, there is a need for transparency on the related investigations and prosecutions.

Rwanda
Independent researcher Jean Claude Niyibizi reported that the Government has taken steps to regulate media content and online media. This is despite a lack of polices that adequately safeguard citizens and the media. It emerged that there is a strong call for capacity building primarily amongst journalists on issues of internet freedom.

Uganda
Esther Nakkazi, a journalist and independent researcher, reported that the media and political opposition groups are the most concerned about surveillance. She added that many respondents often opted not to communicate online due to a fear of interception of their communications. Despite this, there was low usage of digital security tools that could enable encrypted communication. This underlined a need for digital security skills capacity building for the media, HRDs, and for women who are increasingly becoming the targets of online violence.

Tanzania
Asha Abinallah of Jamii Forums noted that there was increased deployment of ICT infrastructure by the government but internet uptake remained low. Respondents in the country also had perceptions of widespread surveillance on their communications by the government. Meanwhile, there was vague understanding of what constituted internet freedom.

Overall, the State of Internet Freedom in East Africa 2015 revealed poor usage of digital safety tools across East Africa. Usage was lowest in Rwanda and highest in Uganda, where the LGBTQI community were some of the major users. Besides government surveillance, other emerging internet freedom concerns in the region were violence against women, an issue that the research revealed has to be addressed but remains widely misunderstood. There was also growing concern over the lack of data protection laws. The need for public awareness campaigns, and for developing criteria or benchmarks to assess internet freedom in East Africa, was also observed.

Bridging the Gap Between Techies and HRDs

Technology tools are being used in the advancement of a free and open internet at a time some countries are seeing a rise in abuses and attacks on internet freedom. There is widespread lack of knowledge on what constitutes internet freedoms, and limited skills and information about minimising threats to online safety, including among HRDs. With the involvement of some frontline users, the OpenNet Africa Challenge earlier in 2015 tested some digital safety tools for their efficacy in the East African context. However, there is minimal collaboration between tools developers and those on the frontlines defending human rights. This session therefore brought together technical experts and HRDs to explore ways in which technology can assist in advancing internet freedom in the region.

Panelists
Neil Blazevic, East and Horn of Africa Human Rights Defenders Project (EHAHRDP) - Moderator | Dan Meredith, Open Technology Fund (OTF) | Kelly Daniel Mukwano, Winning Team – OpenNet Africa Tools Testing Challenge (Uganda) | Davide Del Vecchio, GlobaLeaks | Crystal Simeoni, Hivos East Africa | Edward Sekyewa, Hub for Investigative Media

Issues Raised

Data Protection: Participants noted that the transition of physical data to digital data in government offices is slow. Further, concerns on data protection were raised as there is more user data requested from citizens now than ever before. However, many countries have yet to enact data protection laws to secure information provided by citizens.

L-R: Edward Sekyewa, Hub for Investigative Media, Kelly Daniel Mukwano, Winning Team – OpenNet Africa Tools Testing Challenge Uganda, Davide Del Vecchio, GlobaLeaks, Dan Meredith, Open Technology Fund (OTF)

Anonymity: The role that anonymity plays in promoting human rights remains misunderstood by governments, as it is mostly viewed with suspicion and governments consider it open to abuse by citizens. For instance, whistleblowing was highlighted as an enabler of human rights and good governance, yet it was often perceived negatively when done anonymously. Davide Del Vecchio of GlobaLeaks stressed the need for more user-friendly anonymity tools which should be "10% tech and 90% usability" and developed in collaboration with end-users. At GlobaLeaks, development work is underway on a suite of software which enables secure anonymous whistle-blowing through simplified interfaces.

Non-Adoption of Digital Safety Tools: A general lack of knowledge or utilisation of digital security tools among journalists and HRDs in Africa was widely cited. Although there is an assortment of tools available (including easy to use open source ones) for securing communications, hindrances to their use include a perception among users such as HRDs that they need to be tech savvy to use these tools. The digital safety tools need to be demystified to enhance their uptake by HRDs and other vulnerable groups. Further, digital safety training has to be appreciated from an internal level within organisations in order for it to be taken as a capacity building priority for staff. Staff need to be afforded time off to attend digital security workshop organised externally, which is not always seen as necessary.

There is also a need to understand security needs for activities deemed illegal, such as training LGBTQI groups or providing online spaces for women to discuss issues such as abortion. Kelly Mukwano of iFreedom Uganda spoke of the need for "security for the illegal", making reference to the safety challenges faced by the LGBTQI community in Uganda both online and offline. In the past, workshops for LGBTQI groups in Uganda were interrupted by law enforcement officers.

Moreover, many individuals were unable to recognise that they are human rights defenders through their online activities such as sharing, via social media, opinions that challenged the status quo on. Very often, such individuals did not realise the need for securing their online communications.

Applicability of tools: Different contexts require different tools. Therefore, it is important to test and localise digital safety tools, with a focus on language and data requirements, among others. Reference was made to Panic Button, which raises a digital alarm to preselected numbers by sending the GPS location of where a report is originating from.

However, such a safety tool requires a consistent data connection by all parties for it to work efficiently, hence being ineffective in parts of Africa where challenges of internet connectivity and electricity shortages still exist.

Recommendations

- Although there are digital security training initiatives for activists and HRDs in a number of countries, there is need to reach bigger numbers of HRDs with such trainings.
- More media managers and individuals in positions of leadership need to be exposed to the need for digital security. This will enable the internal culture and appreciation of digital security tools and their consequent use especially in media houses.
- Establish a "digital training ecosystem" where knowledge and skills can be shared beyond workshops and training days. This could be a network of journalists and human rights defenders.
- Away from the technological aspects, legal representation should be encouraged especially where freedom of expression is hindered especially during offline attacks (e.g. shutdown of workshops promoting the use of online security tools)
- Localise digital safety tools in collaboration with end users.
- Avail affordable tools like smart phones and computers, as well as affordable internet access, for rural based activists and HRDs so they can utilise online safety tools.

Understanding Creative Expression Online

A growing number of African artists are aiming to use creative expression for human rights advocacy and for social innovation. Some African artists are carving a niche in the online space through the use of digital technologies but also through the transfer of offline content onto online platforms. In doing so, they are creating local content, and igniting debate online on issues of community concern. This session thus sought to spark discussion on how artists can utilise the internet to promote social actions and whether they have adequate protections should they fall on the wrong side of the law.

L-R: Stella Chege, Jukumu Letu/HIVOS, Roland Niwagaba, Writivism, Faisal Kiwewa, Bayimba

Panelists
David Kaiza, Writer, (Moderator) | Faisal Kiwewa, Bayimba | Stella Chege, Jukumu Letu/HIVOS | Roland Niwagaba, Writivism | Naamala Samson, Culture and Development East Africa (CDEA) | Tom Odhiambo, University of Nairobi

Issues Raised

Role of creative expression: Panelists noted that creative expression has made the internet much more exciting through the packaging of content. Even in traditional media forms, creative expression is present: for example, news photographers exercise some form of creativity in framing their images to be more appealing to their audiences. David Kaiza stressed the need for understanding of the different types of relationships between creative people and the internet. "There is the relationship between creative people and the internet itself, the relationship between creative people and society, and the relationship between creative people and the government or the state."

Legal frameworks: The dilemma that the creative industry faces is the same as that faced by other internet users when it comes to freedom of expression. While the media plays the role of society's watchdog, the creative industry has evolved into a "social commentator" and the two face similar restrictions.

In Uganda (and in similarity to other African countries) there have been cases of plays being banned due to their content – often related to political issues or "taboo topics" such as homosexuality. Samson Namaala of Culture and Development East Africa (CDEA) in Tanzania said the country's laws are silent on creative expression on the internet and this leaves creative content open to abuse by law enforcement agencies. He made reference to Tanzanian performer Vitali Maembe who was arrested after singing about a "vaccine for corruption" in Tanzania.

Speakers referred to a pre-internet time, when there were self-policing mechanisms within the industry through which content was reviewed - such as editors, bookstores or even a theatre. Today, content does not always go through the various checks and balances as was done in the past. This echoes the surge of citizen journalists, personal blogs and many other forms of online content which go straight from the content producer to an online audience without an editorial process. This led to questions such as, how do artist draw the line between entertainment and promoting hate speech?

During this session, limited protection of intellectual property online was raised. It was noted that many people – artists inclusive - are generally unaware of legal and regulatory frameworks that protect artistic work. .

Online Content: There is a mutual dependence between artists and the internet. Many are posting content online which has led to a reliance on the internet for their livelihoods. However, currently, the creative industry uses just a small percentage of the online tools available to them that can enable and promote innovation and their expression online. There is a growing recognition of online celebrity and in this regard reference was made to Ugandan performer Anne Kansime who has gained international recognition primarily through social media platforms where her comedy acts have gained popularity. The Kenyan group 'Just a Band' also gained popularity after sharing their work online.

However, the content available online tends to favour certain aspects of creativity over others. The internet seems to be more responsive to film and music than it is to books and literature. This is similar to the celebrity-driven news content which gains popularity online more than topical social and governance issues.

Recommendations
- Artists and various forms of art need to find a stronger presence online to further contribute to local content online.
- Intellectual property is an issue that requires further discussion and awareness especially with regard to online content and data protection.
- Freedom of expression in the creative industry remains largely undervalued and with little or no policies to protect creative rights. It should become a priority in the creative industry discourse.

Online Violence Against Women

Offline, women are often subjected to various forms of violence and marginalisation. Some of these have been transferred online to an audience of strangers who exacerbate the abuse through their use of social media platforms and phone messaging services like Whatsapp. Cases of revenge pornography, cyber stalking and cyber bullying are becoming rampant. In many instances, these cases go unreported and victims have limited room for seeking justice. The session sought to explore ways in which violence against women (VAW) can be prevented online.

L-R: Crystal Simeoni, Hivos East Africa, Jan Moolman, Association for Progressive Communications (APC), Moses Owiny, Women of Uganda Network, Prudence Nyamishana, Global Voices, Victor Kapiyo, International Commission of Jurists (Kenya)

Panelists

Dr. Ruth Nsibirano, Makerere University (Moderator) | Crystal Simeoni, Hivos East Africa | Prudence Nyamishana, Global Voices | Jan Moolman, Association for Progressive Communications (APC) | Moses Owiny, Women of Uganda Network

Issues Raised

Sources of violence: In many instances, violence against women is inflicted by people they know. However, online violence against women is further compounded by the popularity of social media and the sheer number of users who can fuel violence against one individual through commentary and re-sharing of information. In some instances women contribute to the violence committed against others by perpetuating gender stereotypes. It was noted that even women who are not online are targets of online violence. An example was given of a woman whose picture in a compromising position was re-shared yet she was unaware since she was not online.

Women who suffer violence online are often chastised and blamed, while perpetrators face small or no consequence, especially in instances of revenge pornography. Violence against women online is a reflection of existing offline structural inequalities in society, and such inequalities need to be addressed so as to check online VAW.

Lack of legal recourse: There are inadequate and for the bigger part unknown legal and regulatory mechanisms to protect women against violence online. Further, women who suffer violence rarely speak out and as a result there is a lack of adequate information and statistics on the vice. This makes it hard to know the extent of the problem at national and continental level.

Participants noted a need for clarity on the difference between moral, cultural and legal rights where instances of violence against women are deemed legally wrong but culturally right e.g. genital mutilation and violence based on dress style such as mini-skirts.

Digital safety awareness: Many women remain unaware of their rights online and are also unaware of the tools available to secure their online communications and information. Besides, there are no online platforms dedicated to the reporting of online VAW. This consequently makes their online communications more vulnerable to being abused. As a result, online violence against women is influencing the decision of some women not to contribute to online conversations.

Recommendations

- There is a need for analysing internet policies and legislation to identify gaps exploited by perpetrators of violence against women online.
- More women should be made aware of digital security so they are better placed to protect themselves against violence. Workshops and information about protection measures should be more readily available.
- An online portal where women report acts of online violence against them should be established. This will encourage more individuals to report violence and serve as a hub of information on digital security tactics and incidents.
- More women should be enabled and encouraged to be active online and to also stay online. Currently, there are more men than women online, reflecting the economic disparities which also exist offline.

Marking a Decade of the Access to Information Act in Uganda

In 2005, Uganda enacted the Access to Information Act (ATIA), and six years later the regulations to give effect to the law were enacted. The Forum served as an opportunity to look at the progress the Act has made over the last decade, as it opened on the International Right to Know Day celebrated on September 28. In his remarks, Gilbert Sendugwa, Coordinator of the Africa Freedom of Information Centre (AFIC), said although the law had been in place for a decade, it was not adequately used as there was narrow awareness of its existence among citizens.

Speakers

Simon Mayende – Office of the Prime Minister (OPM) | Gilbert Sendugwa – Africa Freedom of Information Centre (AFIC) | Imelda Namagga, Uganda Debt Network (UDN) | Mohammed Ndifuna, HURINET | Edward Sekyewa, Hub for Investigative Media (HIM) | Parliament, Uganda | Hon. Kenneth Lubogo, Member of Parliament, Uganda

Issues Raised

Ignorance at Civic, Media and Government levels: Mohammed Ndifuna of Human Rights Network (HURINET) Uganda stressed that, “access to information is at the heart of the enjoyment of all the other rights” but implementation of the ATIA in Uganda has not been fully realised. The Act has been met with challenges including failure by the information ministry to report to parliament on progress made in implementing the law. As a result, there is poor release of information by state agencies. Often, when information is released it is not comprehensive, which affects service delivery monitoring. Civil society participants agreed that information requests regarding government accountability were often rejected, while the more mundane or public relations information was readily shared.

It was concluded that three key issues impact ATIA in Uganda (1) a high culture of secrecy among public servants, (2) contradictory laws and (3) the low understanding of the law both by duty bearers and the general public. Among journalists, uptake of the law remains poor with many ignorant about the process of requesting information, while others complained that the process is labourious.

Litigation for information release: While the Hub for Investigative Media (HIM) had success in litigation against the National Forestry Association (NFA), it was noted that litigation is seen an elitist channel of forcing government to provide information. However, while litigation may be possible only for few due to the costs associated with it, the court

rulings have wider implications, making it a worthwhile approach. Litigation plays a catalytic role is fostering change as it broadens the effects of the ruling.

> ".. there is a strong correlation between access to budget information and the fight against corruption because the citizens have information upon which to hold the leaders accountable." Imelda Namagga from the Uganda Debt Network

Role of Parliament in Promoting the Access to Information Act: Sylvia Birahwa from the Ministry of Information outlined the achievements of ATIA in Uganda, which include the gazetting of the Access to Information regulations, the development of a government communication strategy, appointment of information officers in all ministries, the establishment of the Inter-Government communication forum, and the launch of the www.Askyourgov.ug online platform.

The Ministry of Lands, Housing and Urban Development (MLHUD) was recognised as the most responsive government agency on www.AskYourGov.ug.

Pictured: Dennis Obbo (centre), Principal Information Scientist at MLHUD, receives the award on behalf of the Ministry. With him are Gilbert Sendugwa of AFIC (left) and Simon Mayende Office of the Prime Minister (right)

However, the human rights committee of parliament being a fairly new outfit still requires capacity building in this regard and given the high attrition of parliamentarians, Hon. Lubogo called for continuous sensitisation and engagement with MPs.

Other challenges to the law such as the lack of internal appeal mechanisms and its emphasis on litigation as the first resort were noted. It was also noted that many public servants lack skills in using new technology, and yet this would simplify their work.

Recommendations

- There should be a shift from the culture of secrecy among public officials which has hindered the dissemination of information.
- Popularisation of the law should be intensified. There should be a multipronged strategy that involves, among other things, building the capacity of citizens and the media to make requests and helps public bodies/officials to understand and use the law effectively.
- Local governments should be proactive and pursue information from the central government to enable their responses to information requests at a local level. Further, information on the Access to information law should be disseminated to local communities to promote awareness and understanding.

- Local government should establish resource centres or libraries to ensure that public information is easily available to the general public. Government should also ensure information is in accessible formats and also available in languages other than English.
- MDAs should comply with the law e.g. by making it mandatory for ministerial statements to parliament on implementation of ATIA, failure of which should be punished accordingly.
- Create an enabling tech based environment for officials to easily release information. Further, shared information should be made public and easily accessible to prevent repeated requests.
- More laws should complement ATIA, as currently there are contradictions between ATIA and other laws such as the Official Secrets Act (1964).

Cybercrime vs. Internet Rights in Africa

As the number of internet users increases, so does the need to fight cybercrime. Cyber fraud, child pornography, hate speech, cyber bullying, promotion of terrorism are becoming a concern for many stakeholders. While these may be genuine concerns, some governments have been faulted for using them to further curtail freedom of expression online, often undermining legitimate opinions online. Perspectives on addressing cross-border cybercrime and internet rights were shared from different stakeholders in a bid to draw lessons for Africa.

Panelists

Ambrose Ruyooka, Vice – President, ISOC Uganda Chapter | Jimmy Haguma, Uganda Policy Cyber Crime Unit | Irene Kaggwa, Uganda Communications Commission | Ebele Okobi, Facebook

Issues Raised

Regulation: Cybercrime laws have to be "looked at holistically not only with a focus on one aspect such as freedom of speech," said Irene Kaggwa, Head of Research at the Uganda Communications Commission, while discussing the safeguards in place to protect against issues such as defamation and attacks on privacy. She noted the challenge of conflicting cross-border regulations. What is acceptable in one country may be unacceptable in another country. An example cited by Kaggwa was that while Uganda has a ban on pornography, some countries allow it as long as it has controlled distribution.

Gaius Kowene, a journalist and web activist from Congo, said cybercrime laws and regulations do not suit non-state actors: "Law enforcement uses the very laws in place to hamper the rights of activists and journalists when content doesn't suit the ruling parties and politicians."

Law Enforcement: While the police have the role of enforcing the law, they also have a key role in creating awareness on safety issues including those related to online activity. Law enforcement plays a role in ensuring that victims of crime receive help, which includes collecting evidence. For instance, Uganda's Computer Misuse Act, 2011 provides for the collection of digital evidence upon the issuance of a warrant. However, there needs to be a balance between online freedom and the conflict with the rights of other users.

The challenges of policing across border were further stressed as the internet has created the space for borderless crime and has resulted in law enforcement greatly relying on information intermediaries to support their investigations. In some instances when fighting crime, law enforcement has made information requests from international entities such as Facebook, but this information has not always been provided. According to Jimmy Haguma of Uganda Policy Cyber Crime Unit, intermediaries should not be held liable for what others do on their platforms but can be approached to assist in crime prevention. However, failure to respond to a court order requesting assistance can turn an intermediary into "an accessory to crime."

Intermediaries: There should be more understanding and dialogue on the role of intermediaries, as sometimes it appears that the roles and responsibilities of the state are transferred or imposed upon intermediaries, such as deciding what is legal and what should not go online. Meanwhile, the question was raised, should an American company such as Facebook be in a position to decide what someone in another country sees or consumes?

Even though countries may follow due process to request user information from Facebook or to have content removed, they will not necessarily receive the information requested. "If Facebook were a country, it would be the biggest country in the world. If you think of jurisdiction in that context, you would see how difficult it is for a platform based in the US to apply the laws of every different country," said Ebele Okobi from Facebook. She added that there was a need to think about different mechanisms that deal with online concerns that are not necessarily crimes, such as teens bullying each other online.

The Economics of the Internet

The internet offers the opportunity to reach wide audiences, the ability to offer tailored services and has a relatively low market entry cost. Many governments have realised the potential of the online economy and have endeavoured to create frameworks that support and safeguard it, such as e-transactions and cyber protection laws, and establishment of cyber crime units. With the low rates of internet usage and zero rating/neutrality of internet access, what does the internet mean for the development of sustainable economic enterprise in Africa?

Panelists
'Gbenga Sesan, Paradigm Initiative Nigeria (PIN) | Ephraim Kenyanito, Access Now | Kevin Chege, ISOC Africa Regional Bureau | Ebele Okobi, Facebook | Michael Niyitegeka, ICT Association of Uganda (ICTAU)

Issues Raised

Cost of privacy: Data Privacy regulations are often built upon documentation prepared by the OECD which the African Union Cyber Security Convention is based upon. At a national level, however, in many African countries there are few frameworks that follow the principles set out in the convention.

Increasingly, websites ask for data in order to grant individuals access to information on the portals. But, as one panellist put it, how much information is too much for one to give away to get to do what they want to do online? Another pointed out that information shared online should not put users or the people around them at risk. The need was stressed for data protection and privacy laws and their implementation as enablers of free and secure use of the internet. It was observed that there were insufficient interactions between government and intermediaries, hence affecting policy making processes. Further, legislators are not well informed about data privacy, especially as the amount of user information collected increases.

Zero-rating: It was argued that zero rating allows people to get a taste of what the internet has to offer. Initiatives like Internet.org have been established to entice more users to get online through providing "free basics" especially in developing countries. Participants stressed that internet.org users need to be informed that they are using just part of the internet free of charge else they could remain in the "walled garden" and their reactions in the long run were not known. According to Okobi, anecdotal evidence indicates that the target users understand that internet.org offers just some of the internet and not all.

While internet.org is a Facebook initiative, it runs in partnership with local service providers who have a bigger say in what content is released on the platform as the cost is mostly carried by the service providers. Okobi pointed out that while it encourages free access to the internet, this would not necessarily result into economic sense for service providers. Sesan noted that "equal access is not necessarily the same as free access," as the latter has content limitations. "We see a lot of sentimental talk and not necessarily informed talk," said Michael Niyitegeka of ICTAU on the need for more informed argument on policy pertaining to internet access models such as internet.org. It was also pointed out that most people opposing internet.org already have access to the internet.

Content: Related to the discussion on free basics was the issue of the amount and cost of African content online. It was noted that there was a large amount of local content online which was not part of internet.org. Although content producers can load their content for inclusion in free basics platform, the decision on which content forms part of the internet.org initiative does not lie with Facebook but with the operators it partners with. Concern was raised that this was comparable to creating "a gate keeper of content."

There was agreement that the internet should remain free and open to enable innovation, and to boost socio-economic development and cultural rights in Africa. The continent needs to be both a creator and consumer of its own content and as such, initiatives such as internet.org should be temporary to allow economies to reach a point where all can access and afford the internet. Further, governments were urged to work towards enabling and rolling out more infrastructure to enable content creation and sharing.

Big Data: A lot of information is volunteered by users who are mostly unaware of what they are signing up for due to the fine print and complexity of online user agreements. As such, user information is utilised for marketing and research purposes without the knowledge of the users. "As a user it is best to know what you are signing up to, who is going to be in control of your data and what rights they have over your data," Stated Kevin Chege.

A clash between big data and privacy was acknowledged, which also threatens online economic opportunities and research. An example of the positive use of big data was noted as instances when sim card movements are tracked to follow the spread of a disease, such as was seen in Haiti where a cholera epidemic spread was tracked.

Moreover, a lot of African user data is stored beyond the continent and there is little use of Mutual Legal Assistance Treaties (MLATs) which aid in cross-border legal issues at an international level.

Innovation hubs have sprouted around the region as more turn to developing tech solutions to address societal challenges. These have been key in providing guidance to start ups in the region. However, innovators need to be tactful in their approach such as where to utilise non-disclosure forms and limit the sharing of information they work with.

Recommendations

- There should be more user notification about data breaches in order to promote online transparency at both a national and business level. The integrity of systems to secure users' data should be well maintained and if compromised, data owners should be informed.
- There is a need for more collaboration amongst players including business entities/private sector/research firms and policy makers in Africa in addressing concerns arising from user data such as privacy and data security.
- Mutual Legal Assistance Treaties (MLATs) should be pursued more in big data and privacy initiatives, especially when working on online issues that span across borders like where user data is stored
- African internet governance issues should be discussed in Africa and not only at international spaces as is currently the trend. More engagement at national and regional levels should be pursued to encourage knowledge and best practice sharing.
- Online user agreements should be simplified for more people to understand what they are signing up for with regards to their data.

Conclusion and Way Forward

Concluding remarks were given by Hon. Vincent Waiswa Bagiire, Chair of the ICT Committee in the Parliament of Uganda. He stated, "the success of the internet is largely attributed to its openness and for this reason, governments have the responsibility to maintain the internet and the multi-stakeholder governance and free character of the internet for it to be relevant to all users." He added that there was a need to continue convening the Forum on Internet Freedom in East Africa to allow stakeholders to discuss how to advance internet freedom in Africa.

Recurring concerns raised at the Forum included a lack of awareness of online rights, deficient digital safety practice, limited access to the internet, and the lack of sufficient legislation to protect citizens online.

Online violence against women is an area that still remains grossly misunderstood and whose extent and manifestation is not well documented, thereby contributing to the slow pace of remedial legislation. The lack of online channels to report online abuse remains a problem. Further, instances of online violence against women often mirror what is happening offline, indicating that there is a need to strengthen legal structures and sensitise the judicial system.

While a myriad legislations exist to address some facets of online rights, they frequently conflict with existing laws by placing undue controls on the flow of information and constricting the right to freedom of expression online. In East Africa, the slow progression of legislation on access to information and data protection and privacy, while laws negating media freedom and civil society activity are fast-tracked, is telling of governments' prioritisation of information controls over citizens' internet freedom.

Each of the panels at the Forum identified key issues to address in order to advance internet freedom in East Africa and indeed in sub-Saharan Africa. A set of actionable recommendations was also made by each of the sessions. These will inform onward engagements on promoting internet freedom in Africa by CIPESA and its partners, and hopefully for other actors in this space.

Participants' Reflections on the Forum

- Chennai Chair of Research ICT Africa shared some insights in an article here
- Catherine Kamatu shared safety tips from the discussion on Violence against women
- Samson Namaala shared his thoughts on why a Forum for internet Freedom is needed

Media Coverage of the Forum

- Techjaja: State of Internet Freedom in East Africa Report To be Launched Next Week
- Dignited: Access to Information in Uganda to be Recognised at Internet Freedom Forum
  Uganda Goes Online (Ugo): Internet Freedom Forum In East Africa 2015 Underway
  UNESCO: UNESCO discusses with stakeholders how Internet Universality principles are relevant to East Africa
- The Horn Observer: High Level Forum On Internet Freedoms In East Africa 2015 Concluded In Kampala, Uganda
- Akvorsr: Forum on Internet Freedoms in East Africa 2015
- Mail and Guardian Africa: The sweet and sour bits from the East African internet freedom report; where Kenya, Rwanda lead and Burundi trails
- Mail and Guardian Africa: BE WARNED! East African states are smart and will kick over your internet freedom; here's how they're doing it
- CPI Financial: Internet As a Basic Human Right
- CEO Magazine: CIPESA unveils State of Internet Freedom in East Africa Report
- Catholic Radio Network: UNESCO recommends South Sudan to establish Internet Society
- Kasese District News: Internet is A Right to Everyone
- Hivos: State of Internet Freedom in East Africa 2015: Survey on Access, Privacy and Security