

9 March 2017

Internet Freedom Festival (IFF) – Valencia , Spain

By Koliwe Majama

SCRIPT : The Case for Digital Rights: Strategies for increasing Private Sector accountability and transparency

Objective: Advocacy strategies to increase accountability and transparency of the private sector in information and communications technology sector

This workshop will:

1. Revisit the status and role of the private sector in violating user rights particularly in the wake of internet shutdowns on the continent
2. Explore and analyse the legal and operational environment for ISPs in the African and Arab regions that make it easy for governments to identify an intermediary and target it for a criminal or civil offence, rather than directly policing the 'behaviour' of the users.
3. Share SMEX 'mini ranking' tool
4. Draw up advocacy strategies to ensure 'safe harbour' for African intermediaries to ensure that they are protected from potential liability and can also upholding human rights online

PRESENTATION 1 [15 mins] - Koliwe

Title: What are the trends?

It is important for Internet Governance processes to recognise the importance of roping in the private sector in the promotion of a free and open internet. Particularly following recommendations in the Human Rights Council report on Freedom of expression and the private sector shared at the 32nd Session of the Human Rights Council in June 2016. However there are a number of critical issues/trends worth noting as we strategise on interventions to make in seeking the transparency and accountability we desire from the private sector.

1. Snooping legislation

With the expansion of independent content production and platforms to transmit that content and public opinion, African governments have stepped up restrictions and regulation to 'censor' the information made available especially on the internet.

In the process, African states have/are creating new laws or regulations to complement already existing legislation that makes internet intermediaries legally liable for third-party content on their networks or platforms. This makes them vulnerable as they 'censor' content that may be deemed 'controversial', a 'national threat', 'causing disorder' , 'disaffection'. ISPs are increasingly being used to play 'watchdog' and enforce controls on user behaviour/access. This has

affected especially particularly activists who target/challenge governments/political elite [policy] and some 'powerful' private citizens .

Zimbabwe - Interception of Communications Act¹ which outlines mandatory Interception & compliance of ISPs. Services providers must ensure that their equipment is able to facilitate interception of information, installation of software, hardware, allow for simultaneous interception, call-relation upon termination, access or decryption.² The ICA criminalises the non-compliance or uncooperative service providers.

Zimbabwe Internet Service Providers Association (ZISPA) in the past raised concerns with this Act, but there is no record indicating whether their members then objected to installation of intercepting software and involvement in administering or executing search warrants. The recorded complaint was from the access providers complaining of the costs for such equipment, which was probably passed down to the consumer through increased rates or loss of unused or "expiring" data.³ This Act severely encroaches on communication rights and freedoms, through unregulated surveillance, potentially undermining the implementation of just and fair internet governance regime.

Egypt : Clearly states the licensees' obligations include "commitments related to national security restrictions" (article 25.11) ISPs are required to provide "all technical potentials including equipment, systems, software and communication which enable the Armed Forces, and National Security Entities to exercise their powers within the law" (article 64)

¹ Has a clear intention of intercepting of personal, private or such communications without limitation. Grounds for interception include economic interests, public order, public safety and crime. ICA provides a limited number of individuals that are authorised to apply for a warrant of arrest¹, these individuals apply for the warrant before the responsible minister.¹ The question is whether there is any prospects of oversight under this current enforcement regime? First of concern is the fact that the warrants are issued on grounds of belief and not of reasonable suspicion that a criminal offence is about to be committed or was committed, this is the standard test for issuance of warrants that invade personal and privacy spaces.¹ The minister/responsible authority has unfettered powers and is supposed to submit a list of warrants issued to the Attorney General annually.¹ The Attorney General will give guidance on future warrants and ministerial discretion but does not address if there is any harm suffered or remedial action, the persons whose communications have been intercepted is not aware.¹ There is no judicial oversight in respect of the interception and extensions of the warrants can be obtained before the Administrative Court through an *ex parte* applications.

² Section 12

³ See 47 above, ISPs reported in 2010 that they required over \$1million to get the required equipment, reports indicate that Econet, Telone and Telecontract complied with this request from government,

This is further emphasised in the Act in the state authorities have the power to “subject to their administration” operators in cases “of natural or environmental disasters or during declared periods of general mobilization in accordance with the provisions of Law No. 87 of 1960 or any other cases concerning National Security” [this is the article used by the Mubarak regime to order providers to cut internet and mobile phone services during the revolution of 25 Jan in 2011]

2. Private sector in bed with governments?

However it is important to note that in some, if not most instances, the commercial interests of the private sector expose it to the risk of being complicit with authoritarian governments. This status has made surveillance, censorship, monitoring, trials, and arrests of especially political activists easier for governments. Commercial interests are rooted largely in the licensing conditions of the ISPs which involve both the State and the Private sector as they collude on a common motive – revenue.

Zimbabwe presents a clear case in the 2015 Econet Wireless and Steward Bank “raid” of a media house ‘The Source’, following a High Court order granted to a search and seize operation at the agency over stories it published on its site. One of the stories The other story Debt-distressed Zimbabwe moves to reschedule domestic debt claimed that the government had borrowed \$30 million from Econet to pay civil service salaries, disbursed through its banking subsidiary Steward, in a deal brokered by former Econet chairman Tawanda Nyambirai. This raised eyebrows on the relationship between Government and the Mobile Network operator, given also past media reports on precedent ‘transactions’ between government and the service provider⁴. In 2013, during the transitional government, telecommunications companies and their subsidiaries were arm-twisted to fund the constitutional referendum and in part, also the elections⁵.

Over the years, Econet has been allowed it to expand its core business and other sectors such as banking, insurance, health and vehicle tracking which already had other players registered under different pretexts. Government has a financial interest in the business of MNOs since through Potraz, the regulator, it derives income directly from the revenues of the regulated entities. Potraz gets 6% of the revenues of MNOs derived from the provision of mobile services. In 2014, Government also imposed a 5% excise duty on airtime and mobile data. In the 2017 budget statement issued in December, Finance minister Patrick Chinamasa also proposed a new 5% levy on airtime and mobile data which he said would support a Health Fund. This is in addition to corporate taxes, VAT, employee income taxes and other contributions. This shows that the telecoms sector is not only one of the most highly taxed sectors but that it has become a cash-cow for government.⁶

⁴ <http://takura-zhangazha.blogspot.com/2015/03/just-how-much-influence-does-econet.html>

⁵ <http://www.newzimbabwe.com/news-10545-Poll+cash+hunt+targets+Econet,+Telecel/news.aspx>

⁶ <https://www.theindependent.co.zw/2017/01/20/money-politics-data-wars-zim/>

3. Powerful/Lack of independence of regulators

Telecomms regulators are mandated with the promotion of the interests of consumers, purchasers and other users of telecommunication services in a country.

There is an equal need for POTRAZ to rebrand itself as a neutral and impartial broker.

African countries regulators often enjoy broad administrative power, being able to intervene swiftly through the administrative process, for example, changing the conditions of the licences. This enables governments and regulators to basically order intermediaries to do whatever they want (or at least, to operate with insufficient limits and safeguards for constitutional rights),

Uganda - The Uganda Communications Act (2013) - ICT minister, has the authority to approve the regulator's budgets and appoint board members with the approval of the cabinet. This law merged the Uganda Communications Commission and the Broadcasting Council and reconstituted them as one body known as the Uganda Communications Commission which has control over both broadcasting and the internet and gives directives to even radio stations on what not to air.

In 2011 the UCC issued a directive to ISPs to temporarily block access to Twitter and Facebook during opposition-led protests on high food and fuel prices. While the independence of the regulator has been questioned, the new law gives it Particular individuals are also being targeted, as seen in the Facebook transparency report for the first half of 2013, where Uganda was one of the five African countries that asked the company to disclose information on a user. Facebook turned down Uganda's request. The increased government interest in what users are doing online is likely prompting self-censorship among citizens.

Zimbabwe - Established in terms of Section 3 of the PTA and expansive mandate under Section 4 of the PTA. The mandate of POTRAZ is wide and inclusive of many aspects that would be best placed to have other actors supervise or oversee to avoid conflict and have clear separation of roles. The POTRAZ board is responsible for oversight and management of the POTRAZ and is constituted of not less than five (5) but not more than seven (7) individuals with experience in law and telecommunications and should ideally be expanded to cater for other much specialised areas such as consumer protection, which is its mandate.⁷ Even though the regulator commissioned a consumer survey research in 2013, whose findings remain instructive for the proper functioning of the telecommunications industry and provision of satisfactory services to consumers.

⁷ Section 4 (1) of the Botswana Telecommunications Act, establishment, constitution and membership of the Telecommunications Authority constitutes five members appointed by the Minister with qualifications, expertise or experience in a) information and communication technology, b) law; c) consumer protection; d) financial accounting; e) economics; or f) general business management.

United Arab Emirates -The Telecommunications Regulatory Authority (TRA) is a powerful body in the UAE. It licenses operators, sets prices, and most importantly enforces existing regulations, this includes regulations banning the use of VoIPs and VPNs, and the country's repressive cybercrime law, and deciding on copyright policies

-- **The** decisions it makes to grant or refuse a license by the board of the telecommunication regulatory authority cannot be challenged or appealed (article 34)

-Licensees can be fined up to 10million AED for violating regulations, telecom law and the authority's instructions

--Article 31: "It is not permitted to conduct any Regulated Activity unless authorized by a License or exempted in accordance with the provision of this Federal Law by Decree or its Executive Order" (used to ban VoIP services in the emirates)

4. Conflicting jurisdictions & extra territorial interventions?

In the case of multinationals companies operating in other jurisdictions there is need for interventions to reduce violations of user rights based on government requests to disclose data, interception and take downs etc. What do we do to ensure that they respect human rights and might therefore need to resist efforts to shut down?

5. Consumer Rights and Responsibilities

Consumer Rights and responsibilities are an integral part of this conversation – the extent to which users play an important role in increasing the transparency and accountability of their ICT service providers. This is particularly so given the increase competition in the sector and their drive to maximise on profits of their services. To what extent are consumers and consumer rights groups alive to anti-competition behaviour from service providers and even false misleading and misrepresentation of services available.⁸ And to what extent are they monitoring it?

Consumer rights would cover-

The Right to Privacy:

To enjoy lawful personal privacy and protection against unauthorized use of personal information including confidentiality of electronic communications, prohibition of unsolicited marketing material; the right not to be listed in a telephone directory etc

The Right to Protection Against Market Abuse:

⁸ See for South Africa's Consumer Protection Act (2008),

Protection from market abuse such as excessive pricing, discriminatory pricing, contractual lock-ins, unfair trade practises including false and misleading advertising as well as any form of anti-competitive behaviour.

The Right to a Responsive Regulatory Authority:

To be represented by a responsive regulatory Authority that is continuously and proactively looking out for their interests, taking into account their needs, expectations, preferences and values.

The Right to Consumer Education and Awareness:

To acquire knowledge and skills needed to make informed, confident and intelligent choices about goods and services while being aware of basic consumer rights.

The Right to Safety:

To be protected against products, equipment and production processes that are hazardous to health or dangerous to life of present and future generations as well as guaranteed access to emergency calling services.

The Right to be Heard:

The right to actively participate in the formulation and implementation of government policy, regulations as well as the development and delivery of products and services that they use.

The Right to Complain and Redress:

To have access a fair and transparent complaint process against service providers through fair settlement of just claims, compensation for misrepresentation, service failure or interruption, inferior or unsatisfactory services.

Consumer Responsibilities :

Critical awareness - consumers must be aware and be more questioning about the provision of services as well as the quality and variety of goods and services on offer

Social responsibility - consumers must act with social responsibility, concern and sensitivity to the impact of their actions on other citizens, in particular, in relation to disadvantaged groups in the community and in relation to the economic and social realities obtaining.

Involvement or action participate in all forums to do with policy formulation and legislation for the services they use.

Solidarity – Mobilising and organising themselves as consumers through to promote and protect their interests.

Monitoring of product quality in respect of internet usage or subscription is a very technical and complicated process. In Zimbabwe, mobile and internet users

have raised repeatedly the challenges of expensive internet bundles and unexplained disappearance of units (airtime leakage). This was more pronounced on value added services (VAS).⁹ Some service providers market their ability to provide for instance \$39/month of unlimited data, but in fact would throttle the downloading speeds or the volumes or not be able to offer that in all locations.

Beginning of this year saw a data war ensue when On January 9, the Posts and Telecommunications Regulatory Authority of Zimbabwe (Potraz issued a regulatory notice announcing the introduction of floor prices for mobile data, voice services which were effected by only one service provider. On January 12, Information Communication Technology minister Supa Mandiwanzira and Potraz appeared to have succumbed to public pressure when they announced the suspension of the regulatory notice setting the floor price.

In the US, a mobile and internet service provider, AT & T was in 2015 found liable and subjected to fines of over \$100 million¹⁰ for slowing down speeds of its 'unlimited' data by the Federal Communications Commission.

PLENARY – (30 minutes) - TBA

Strategies to focus on Openness, transparency and Accountability in respect of the 3A's Affordability/Access/Availability

Summary of recommendations by Special Rapporteur report

- *States must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means.*
- *Any demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19 (3) of the International Covenant on Civil and Political Rights. Particularly in the*

⁹ Econet is one such that faced a deluge of complaints on social media accounts forcing them to reconsider some of their costing practices and provision of third party services. The Telegraph, *Econet separates VAS billing after customer complaints*, 24 June 2015. Retrieved from: <https://www.telegeography.com/products/commsupdate/articles/2015/06/24/econet-separates-vas-billing-after-customer-complaints/> (accessed 6 July 2015). There have been complaints that such practices for Econet are contrary to competition and violate anti-trust laws with creation of monopolies, see The Herald, *Econet in Anti Competition Behaviour*. Retrieved from: <http://www.herald.co.zw/econet-in-anti-competition-behaviour/> (accessed 6 July 2015)

¹⁰ The Federal Communications Commission plans to fine AT&T Mobility, LLC \$100,000,000 for misleading its customers about unlimited mobile data plans. The FCC's investigation alleges that AT&T severely slowed down the data speeds for customers with unlimited data plans and that the company failed to adequately notify its customers that they could receive speeds slower than the normal network speeds AT&T advertised. 17 June 2015. Retrieved from: <https://www.fcc.gov/document/att-mobility-faces-100m-fine-misleading-consumers> (accessed 6 June 2015)

context of regulating the private sector, State laws and policies must be transparently adopted and implemented.

- *Governments must also adopt and implement laws and policies that protect private development and the provision of technical measures, products and services that advance freedom of expression. They must ensure legislative, policymaking and other relevant norm-setting processes concerning rights and restrictions on the Internet in order to provide the private sector, civil society, the technical community and academia meaningful opportunities for input and participation.*
- *Among the most important steps that private actors should take is the development and implementation of transparent human rights assessment procedures. They should develop and implement policies that take into account their potential impact on human rights. Such assessments should critically review the wide range of private sector activities in which they are engaged, such as the formulation and enforcement of terms of service and community standards on users' freedom of expression, including the outsourcing of such enforcement; the impact of products, services and other commercial initiatives on users' freedom of expression as they are being developed, including design and engineering choices, and plans for differential pricing of or access to Internet content and services; and the human rights impact of doing business with potential government customers, such as the operation of telecommunication infrastructure or the transfer of content-regulation or surveillance technologies.*
- *Private entities ensure the greatest possible transparency in their policies, standards and actions that implicate the freedom of expression and other fundamental rights.*
- *Private entities should also integrate commitments to freedom of expression into internal policymaking, product engineering, business development, staff training and other relevant internal processes.*
- *International organizations provide meaningful public access to policies, standards, reports and other information concerning Internet governance created or generated by the organization and/or its membership, including through facilitating access to free online resources and public education initiatives. More generally, the multi-stakeholder process for Internet governance has been an important driver for policies supportive of freedom of expression. With that in mind, international organizations should ensure meaningful civil society participation in policymaking and other standard-setting processes, including through increasing the presence of technical experts sensitive to human rights concerns.*