Date: 09-MAR-2017 (Day-4)

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

1. Session output

--Presentation on digital rights violations on the part of telecommunication companies in the regions of Southern and Eastern Africa , the Middle East and North Africa (10mins)

--Presentation on Legal Environment with particular refrence to the licensing and regulatory conditions from of Southern and Eastern Africa, the Middle East and North Africa the two regions

--Presentation of preliminary results of the Ranking Digital Rights Pilot Research in the Arab Region (5mns)

--Open Discussion: Advocacy strategies (30mns)

2. Next Steps

1. Internet rights advocates should formulate human rights assessment plans to monitor trends of violations for advocacy purposes
2. Civil society organisations working on internet governance programming should make efforts to increase interaction with the private sector in efforts to increase their human rights for capacity
3. Strategise on discourse /framing of language to be used when interacting with the private sector that appeals to them. This includes consumer rights issues and corporate social responsibility framing.
4. Advocacy for change in licensing and operational legislation and policies for the private sector that facilitates their violations of rights online.
6. Sensitize the media on the legislative and operational issues and digital rights violation trends so that they have the capacity to report more effectively.

3. Additional notes

Legal Controls, Licensing, and Operating Conditions

United Arab Emirates

--Decisions 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

--The TRA is a powerful body in the UAE: it sets licensing conditions, 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 censorship policies.

--Under Resolution No. (7) of 2008 Regarding the Licensing Regulations, a license could be suspended or revoked for a number of reasons including for breaching license conditions and if it is deemed in "the national interest", without specifying what this actually means (articles 4 and 5).

--License No 1 of 2006 (Etisalat license): Etisalat is required to "comply with any directions as the TRA or any other competent authority may issue from time to time on matter relating to public interest, safety and/or national security", and "undertakes to install at its own expense any equipment required to allow access to its Telecommunication Network and/or the retrieval and storage of data for reasons of public interest, safety and national security (article 8.2)

Egypt

Telecomms Law

--Licensees' obligations include "commitments related to national security restrictions" (article 25.11)

--Operators 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)

--Article 67: 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"

Zimbabwe

---Combination of direct or indirect surveillance and censorship of user behaviour on the internet while leveraging on its administrative and regulatory powers vis-à-vis network operators.

----ISPs are legally liable for the content that they 'host' so they voluntarily censor content - intermediary censorship.

----the Interception of Communications Act (2007) empowers the state to intercept and monitor communications presumed to be threat to "national security, public safety and national economic interest"

---No judicial oversight or independent safeguards against abuse

Zambia

----All Internet and mobile service providers are privately owned, with the exception of Zamtel, which was renationalized in January 2012

-----Regulated through the Information communications and Technologies (ICT) act (2009) which established Zambia Information and Communications Authority (ZICTA) which is generally autonomous in its decision-making. But ISPs and content producers remain vulnerable.

---Intermediaries are not held liable for content under the Electronic Communications and Transactions Act (2009) though transparency and accountability not guaranteed especially given mandates of compliance

4. Relevant resources

Zimbabwe

Blog: Just How Much Influence Does Econet Zimbabwe Have Over

Government? http://takura-zhangazha.blogspot.com/2015/03/just-how-much-influence-does-econet.html

Online article: Election cash hunt targets Econet, Telecel
http://www.newzimbabwe.com/news-10545-Poll+cash+hunt+targets+Econet,+Telecel/news.aspx

News article: Money, politics and data wars in Zimbabwe
https://www.theindependent.co.zw/2017/01/20/money-politics-data-wars-zim/

Report: 2016 report of the Special Rapporteur on freedom of expression, David Kaye, to the Human Rights Council
http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/38

Working paper: OTT - threat or opportunity for African Telcos?
https://www.researchictafrica.net/publications/Other_publications/2016%20_Working_paper_1_OTT-threat%20or%20opportunity%20for%20African%20Telcos.pdf

Ranking digital rights website: https://rankingdigitalrights.org/

Contributors

Koliwe Majama – Media Institute of Southern Africa – Zimbabwe Chapter (Presenter)
Afef Abrougui – Social Media Echange (Presenter)
Megan Deblois – Internews (Rapporteur)