

State of Internet Freedom in Africa 2016

KENYA Report

By Kenya ICT Action Network (KICTAnet)

29th Sept 2016, KAMPALA UGANDA

Freedom of Expression



- High court ruling in April 2016 declared Section 29 of Kenya Info&Comm Act) -misuse of telecoms systems unconstitutional
 - ***A person who by means of a licensed telecommunication system — sends a message or other matter that is grossly offensive or of an indecent, obscene or menacing character..;***
 - ***commits an offence and shall be liable on conviction to a fine not exceeding fifty thousand shillings, or to imprisonment for a term not exceeding three months, or to both.***

Freedom of Expression



- **Point 1:** Misuse of telecommunication system is outlawed and now the preferred charges are:-
 - *'Undermining Authority of a public officer' Section 132 of penal code &*
 - *Section 13 of NCIC Act on hate speech.*
- **Point 2:** Only high profile cases taken up and relatively little number convictions so far- indicating that perhaps they are used to intimidate freedom of expression online (trigger chilling effect to online activists)
- **Point 3:** Little understanding by both public and some law enforcement on the thin line between hate speech and free speech.

Surveillance / Privacy



- Many Acts have sections dealing with surveillance and interception of data for security reasons.
- National Police Service Act, Prevention of Terrorism Act, National Intelligence Service Act,
 - *provides for interception of communications for purposes of detecting, deterring and disrupting terrorist activities,*
- KICA has clause on privacy
 - *prohibits sharing of citizen data by service providers*
- In 2015 A miscellaneous amendment bill tried to enhance the provision of in the Prevention of Terrorism Act by making the Interior (security) Cabinet Secretary the sole decider of whom, when and how to intercept communications.
- This was defeated after the opposition & human rights groups filed a petition in court to stay the contentious clauses.

Surveillance / Privacy



- **Content Control:** No deliberate attempt by service providers to block content was observed. However,
 - Kenya Film & Classification board formally wrote to Google to pull down a youtube video on homosexual love (Google declined); Netflix.
- **Infrastructure Control:**
 - In 2015, Regulator indicated they wanted cybercafes to install CCTVs to log in users while WI-FI providers were to record the physical number of the devices in use – this seems to have gone quiet after some outcry
- **Human Rights NGOs** being followed and threatened with De-registration and their accounts frozen.
- **Proposed social media bill** ahead of next years elections... talked about, but not yet public/published.

Surveillance / Privacy



- **Point 4:** Kenya Film & Classification Board seems to be over reaching its mandate which originally focused on content rating for the traditional broadcast film (not online content)
- **Point 5:** Lack of a Data Protection Act means that data collected on citizens remains vulnerable to state and business actors. *Eg. MPESA details being shared publicly during police vetting. CCTV camera personnel abusing their privilege.*

Activism & Propaganda



- Both Citizen and State Actors seem to be involved in activism and propaganda
- **Citizen Examples**
 - Twitter used successfully for various campaigns
#SomeoneTellCNN #MyDressMyChoic #IsUhuruinKenya
#DeadBeatKenya
- **Government Examples**
 - Director of Digital Communications at Statehouse suspected to create robot accounts to flood the Twittersphere with government friendly data.
 - Robots were posting the same messages simultaneously.
 - **Emergence of Government -friendly bloggers**
- **Parody Accounts have emerged** to counter government sponsored messages.

Public Participation



- **Public Participation** enshrined in the constitution
 - government must seek view, get and consider from stakeholders prior to writing public policy
- **Successful example:**
 - Using the Internet list forums, the Ministry of ICT with KICTAnet have held several online discussion on ICT Policy, CyberCrime Bill and other topical issues.
- **Point 6:** However lack of a standard framework for public participation mean some ministry /gov agency may not be as embracing hence quality of public participation varies across ministries /county

Role of Intermediaries



- Google, Facebook, Twitter regularly file reports on number of takedown requests from governments, and those that have been granted.
- They also publish reports on government requests on/citizen related data.
- Vodafone also publishes similar report but had none for Kenya: - (Safaricom) cited lack of local laws to facilitate and guide the same.
- Other critical players with citizen data but often ignored include Utility companies (Water, Electricity) , Hospitals, Banks, etc
- More transparency on what they do with citizen data and how its is protected/secured.

Recommendations

- **Government** - find a fair balance between genuine security concerns and internet freedoms),
- **Civil Society** -keep monitoring and reporting violations,
- **Academia** - carry out evidence based research on violations, data protection, opportunities and challenges
- **Media** (particularly traditional print media, participate and be more vocal on internet freedoms than now)
- **Intermediaries** (local and global) should be more transparent, particularly on what they do with data and assurance on its security.

Ends

- Q&A

