

GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

Creative Commons Attribution 3.0 Licence <creativecommons.org/licenses/by-nc/3.0/>

UGANDA

Gender dynamics need to be addressed in communications surveillance in Uganda



Women of Uganda Network (WOUNGNET)

Dorothy Okello, Cleopatra Kanyunyuzi and Winnie Mbabazi
www.wougnet.org

Introduction

In 2000, Uganda was recognised as one of the most liberal telecommunications markets in Africa and one in which the number of mobile subscribers exceeded fixed-line subscribers.¹ By 2013, it was estimated that 39% of Ugandans were using mobile phones, and 17% were daily users of the internet – primarily accessing the internet via mobile devices.²

Uganda is a landlocked country in East Africa with an estimated population of 35.4 million.³ Females represent 49.9% of the population, while 49% of the population is 14 years old or younger.⁴ This means that while Uganda’s population is fairly balanced by gender, it is also a very young population with a potential affinity for the use of information and communications technologies (ICTs). Uganda has an ICT Development Index (IDI) score of 1.81, which is below the world average IDI of 4.35.⁵ IDI is a reflection of three ICT development drivers, namely, infrastructure and access to ICTs, level of ICT use in the society, and impact resulting from efficient and effective ICT use.

Policy and political background

Uganda has witnessed tremendous growth in the ICT sector, with the expansion of ICT applications and services including information generation and dissemination, mobile money, and innovative mobile apps – particularly in the agriculture and health sectors. The ICT policy and regulatory environment has also evolved from a focus on promoting widespread

access of ICTs to a focus on management of computer/mobile usage and internet freedoms. Examples of Uganda’s ICT policies and regulations include the National ICT Policy (2003), Access to Information Act (2005), National Information Technology Authority Uganda Act (2009), Regulation of Interception of Communications Act (2010), Electronic Signatures Act (2010), Computer Misuse Act (2011), Electronic Transactions Act (2011), and Uganda Communications Commission Act (2013).

Other acts that have implications on ICT usage and surveillance include the Anti-Terrorism Act (2002), which gives security officers powers to intercept the communications of a person suspected of terrorist activities and to keep such persons under surveillance; the Anti-Homosexuality Act (2014), which outlaws the use of “electronic devices which include internet, films, and mobile phones for purposes of homosexuality or promoting homosexuality”; and the Anti-Pornography Act (2014), which mandates a Pornography Control Committee to “expedite the development or acquisition and installation of effective protective software in electronic equipment such as computers, mobile phones and televisions for the detection and suppression of pornography.”⁶ The Uganda Communications Commission is also to conduct a study with a view to ensuring “responsible use of social media and the internet” through regulation of social media content and internet usage.⁷

Communications surveillance in Uganda: Cause for concern?

In March 2014, the media in Uganda were flooded with stories of the fate of the country’s prime minister, Amama Mbabazi. According to one newspaper, an opposition politician was noted as having remarked how the prime minister “seems to be the first victim of a repressive law that clearly violated the right to privacy.”⁸ The comments arose when pri-

1 International Telecommunication Union. (2001). *The Internet in an African LDC: Uganda Case Study*. www.itu.int/ITU-D/ict/cs/uganda/uganda.html

2 Unwanted Witness. (2014). *The Internet: They are coming for it too!* www.unwantedwitness.or.ug/wp-content/uploads/2014/01/internet-they-are-coming-for-it-too.pdf

3 Uganda Bureau of Statistics. (2013). 2013 Statistical Abstract. www.ubos.org/onlinefiles/uploads/ubos/pdf%20documents/abstracts/Statistical%20Abstract%202013.pdf

4 World Bank Database: Uganda. www.worldbank.org/en/country/uganda

5 International Telecommunication Union. (2013). *Measuring the Information Society 2013*. www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx

6 CIPESA. (2014). *State of Internet Freedoms in East Africa 2014: An Investigation Into The Policies And Practices Defining Internet Freedom in East Africa*. www.cipesa.org/?wpfb_dl=76

7 Lule, J. A. (2014, May 12). UCC to control internet, social media content. *New Vision*. www.newvision.co.ug/news/655459-ucc-to-control-internet-social-media-content.html

8 Kizza, B. (2014, March 5). Is Amama Mbabazi falling on his own sword? *The Observer*. www.facebook.com/ugandaobserver/posts/479565065499306

vate conversations between the prime minister and his wife that had been allegedly secretly recorded were played back at a caucus meeting of the ruling party to which the prime minister belongs. The “repressive law” was the Regulation of Interception of Communications Act (RIC Act, 2010) which had been tabled as a bill to the ruling party caucus by Mbabazi himself while he was security minister in 2007. The RIC Act provides for “lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda.”⁹

It should be noted that the Constitution of the Republic of Uganda 1995 under Article 27 states that “[n]o person shall be subjected to unlawful search of the person, home or other property of that person; or unlawful entry by others of the premises of that person,” and that “[n]o person shall be subjected to interference with the privacy of his home, correspondence, communications or other property.”¹⁰ Furthermore, Article 29(1)(a) states that “every person shall have the right to freedom of expression and speech which includes freedom of the press and other media.” In the absence of a data protection authority, complaints that arise out of issues concerning the abuse of privacy are currently handled by the Uganda Human Rights Commission (UHRC).¹¹

The incident involving the prime minister highlights why there is growing concern over the governance and regulation of communication surveillance, and how it is being used to infringe on one’s right to privacy in Uganda. Because this case affected a high-ranking Ugandan official, the question is, how safe is the ordinary Ugandan? And from a gender activist perspective, what are the gender concerns in the emerging policy and regulatory environment? Two recent studies on internet freedoms in Uganda were conducted by Unwanted Witness and Collaboration on International ICT Policy in East and Southern Africa (CIPESA). While both studies review the communications surveillance environment in Uganda, there is no specific focus on issues of concern by gender. However, both studies did raise various concerns that are relevant to women’s use of the internet and social media.

Enforced under the RIC Act, the mandatory subscriber identity module (SIM) card registration, with a deadline of August 2013, is reported to have increased the opportunity for citizens to be subject to secret surveillance and had a chilling effect on free speech online.¹² In May 2014, an official from the Ugandan police’s Electronic Counter Measures Department noted that while collection, storage and sharing of users’ data through lawful means is for ensuring citizens’ safety, the use of the SIM card registration records had not been that effective.¹³ This was because some SIMs are not yet registered or are only partially registered with alias names such as “gxp”. As such, it makes it hard for the Ugandan police to track down some offenders using SIM card records.

As noted by the media platform Unwanted Witness, without a data protection law in place, Ugandans are not only exposed to surveillance by the state but by anyone who can influence workers at telecom companies.¹⁴ This was evident in the number of reported court hearings where phone call printouts have been presented as criminalising evidence to convict alleged offenders without questioning the processes under which such information was acquired. In addition, anecdotal evidence seems to suggest that it is easier for males to obtain call records when tracking suspected infidelity of their spouses. This would be in line with cultural traditions that permit polygamy, but absolutely object to any “infidelity” on the part of females.

Another key issue, raised by the CIPESA report, was that knowledge and skills about threats to online safety appeared to be widely lacking, including amongst bloggers, journalists and activists that regularly used the internet.¹⁵ As stated in the report, “many online users were prone to attacks and hacks into their private communication due to the lack of requisite skills to secure their communication and information. Similarly, there seemed to be a general lack of knowledge on what constituted online freedoms and what was needed to protect and to promote them. This partly explained why there were few conversations on internet freedoms in the East Africa region. A final plank in the deficiency in knowledge and skills was related to online ethics among internet users.” It is widely known that women’s ICT skills significantly lag behind those of men,

9 The Regulation of Interception of Communications Act, 2010. www.ulii.org/files/Regulations%20of%20Interception%20of%20Communications%20Act,%202010.pdf

10 Privacy International. (2006). *Legal Framework in Uganda: Constitutional privacy framework*. <https://www.privacyinternational.org/reports/uganda/i-legal-framework>

11 Ibid.

12 Unwanted Witness. (2014). Op. cit.

13 Remarks by an official from the Uganda Police’s Electronic Counter Measures Department during the Internet Freedom Forum attended by WOUNET on 23 May 2014, Kampala, Uganda.

14 Unwanted Witness. (2014). Op. cit.

15 CIPESA. (2014). Op. cit.

so a lack of knowledge and skills on online safety should be expected to follow a similar pattern.

While many Ugandans are not aware of the pending threats to the right to privacy, little if anything has been done to safeguard communication platforms to guarantee the freedoms of speech, expression, assembly and association online. For women in Uganda, these platforms are an essential tool to advocate for equality given the gender gap at the decision-making level. The internet is a vital resource offering a platform for women as well as men to express themselves and find valuable information.

As internet use continues to grow worldwide, the debate between greater cyber security and internet freedom is also expanding.¹⁶ Going online presents many opportunities and dangers because there are hackers, fraudsters and overzealous surveillance systems even while online forums present a place for people to express themselves, find useful information, and grow their businesses. Women are uniquely affected by ICT policy decisions as the internet presents a space and opportunity for women's greater involvement in society and the economy as a whole.¹⁷ Women are also distinctively at risk of abuse online. Because of this, women's organisations, especially those with expertise on ICT issues, need to be given an active role in national discussions regarding a balanced policy on cyber security and internet freedom.

It should also be acknowledged that the need for a balanced communications surveillance policy is within an environment where infrastructural, economic and cultural reasons also serve to constrain access to the internet for women. For instance, while 73% of Ugandans over the age of 15 can read or write at a basic level, 83% of men are literate compared to only 65% of women.¹⁸ Additional barriers include working infrastructure, physical mobility, and limited affordability.¹⁹ If women cannot access ICTs then they cannot utilise them. Indeed this situation typically attracts the question as to whether women should even be concerned about internet freedom matters given their limited access!

However, barriers to internet access coupled with excessive communication surveillance can only

serve to push women further away from inclusion when it comes to using ICTs. Anecdotal evidence reveals women who willingly give up access to ICTs so as to minimise potential domestic confrontations and violence. The small percentage of women who are able to access and utilise ICTs both online and offline have not been spared the negative effects of surveillance by the state or private individuals.

Currently, technology-related violence against women takes on a variety of forms such as cyber stalking, sexual harassment and unauthorised use, manipulation and dissemination of personal information – including photographs and videos.²⁰ Manipulation and intimidation of women through unauthorised use of personal information have been evident through leaked private photos in local tabloids, which is a clear violation of these women's rights to privacy as stated in the Access to Information Act. The Act contains the only statutory definition of privacy available in Uganda: "the right of a person to keep his or her matters and relationships secret." This Act also provides that the right of access should not interfere with the right to privacy. Unfortunately, the fear of surveillance by either the state or private individuals further drives away or self-censors citizens from using ICTs online/offline to freely express themselves and be heard on issues that affect them politically, socially, economically and culturally.

Conclusions

Government agencies all over the world are increasing surveillance on their citizens due to perceived and real internal and external threats but, unfortunately, in the process they undeniably find themselves violating citizens' rights to privacy.²¹ Within the East African region, Uganda enacted its interception of communications law in 2010, Rwanda in 2013, and Ethiopia in 2009. Burundi's amended Code of Criminal Procedure 2013 provides for interception of communications, and Kenya's Intelligence Service Act 2010 also provides for interception.

At the same time, there is no question that the responsible development of communications surveillance and in general cyber security is necessary to protect women from cyber violence. However, the internet is also a useful tool for women to seek assistance and connect anonymously with various centres and organisations, for instance, those that assist survivors of violence against women (VAW). Anonymity is only achieved when users are confident that their actions are not being tracked, and that they can seek safety without fear of repudiation. Additionally, the

¹⁶ WOUNGET. (2014). *Cyber Infrastructure: A Women's Issue Too!*

¹⁷ Moawad, N. (2013). How does gender intersect with Internet governance. *Association for Progressive Communications*. <https://www.apc.org/en/node/18677>; Amuriat, G. Z., & Okello, D. (2005). Women on ICT Policy Making in Uganda. In F. Etta & L. Elder (Eds.), *At the Crossroads: ICT Policy Making in East Africa*. Kampala, Dar es Salaam and Ottawa: East African Educational Publishers Ltd., Ujuzi Educational Publishers Ltd. and the International Development Research Centre. web.idrc.ca/openbooks/219-8

¹⁸ UNESCO Institute of Statistics. Country Profiles: Uganda. www.uis.unesco.org/DataCentre/Pages/country-profile.aspx?regioncode=40540&code=UGA

¹⁹ WOUNGET. (2014). Op. cit.

²⁰ Moawad, N. (2013). Op. cit.

²¹ CIPESA. (2014). Op. cit.

right to privacy online allows women to decide how they want to share their personal information through ICTs.²² Because of this there is a need for a balanced framework between communications surveillance and internet freedoms that protects women online, while not interfering with their ability to exercise their rights online. With a Gender Inequality Index score of 0.517 and ranked 110 out of 148 countries,²³ Uganda's rating is better than the sub-Saharan Africa average score of 0.577, but leaves plenty of room for concern on gender issues. Within the East African region, Rwanda fares best with an index score of 0.414 and a country ranking of 76.

For instance, without a data protection law to regulate the collection, storage and access to citizens' personal information, their security is endangered regardless if one is in public office or a private citizen, since this information can be accessed by anyone. A case in point is our key story in which a very high-profile public figure was not spared from surveillance that infringed upon his right to privacy. How much more, then, can be expected to happen to the ordinary Ugandan woman – with the aid of current cyber laws through which the government can control how digital freedoms should be exercised through surveillance?

As a topical issue, communications surveillance has attracted various reactions from different activists, stakeholders and experts at forums in Uganda, with some arguing that people give up their right to privacy once they go online. Others stress that self-censorship is the only way one can be assured of privacy and security online. Proponents for self-censorship argue that, even with data protection and privacy laws in place, it is difficult for the government to protect users once they enter cyber space due to the existence of third parties who also store users' information. However, others still insist that security/privacy, as ensured offline, should be available online. Proponents for online and offline privacy include those advocating for the amendment of oppressive sections in the laws that facilitate communications surveillance. Women's marginalisation in all these debates has also been discussed – notably at the national decision-making level. Even with fair gender representation, there is little or no input by women representatives in communications surveillance-related policies.

Action steps

Even while women may currently be limited in access to ICTs, they no less suffer various violations resulting from cyber crime and communications surveillance. There is a need for action steps to address the following:

- As civil society organisations advocate for government to uphold citizens' rights to freedom of expression, privacy and security, there is a need to acknowledge that in order to achieve a holistic approach to observing human rights offline and online, a balance between surveillance and freedom has to be achieved. If either is too extreme, it will lead to the abuse of human rights, in which women will be distinctly affected.
- There is a need for public sensitisation on privacy laws and citizen rights. The government, private sector and civil society should run awareness programmes so that when internet users come online they are aware of the pros and cons of the online environment.
- The right to freedom of expression should not be abused by ICT users online/offline. There is a need for public sensitisation on the rights and responsibilities that go along with internet freedoms.
- Individuals need to ensure that they stay safe online as much as they do offline. In particular, there is a need for awareness and capacity-building programmes for women on keeping safe online.
- There is a need for gender awareness and sensitisation for all actors in the communication surveillance space:
 - Civil society organisations need to advocate in a gender-sensitive manner for enactment of "safe" laws and amendment of laws that infringe on citizens' rights to privacy, freedom of expression and security both online and offline.
 - Publishers need to ensure that the information they post online and offline is factual, and that it does not perpetuate gender stereotypes or gender-based violence.
 - As the government enforces cyber security laws, the legitimate aim of protecting its citizens online and offline should be upheld with due consideration to gender concerns.
- There is a need for quantitative and qualitative research on women's knowledge, skills and reasons for going online in a context where communications surveillance is a reality. There is a need for studies on the effects and impacts of the prevailing online surveillance environment on women and their uptake of ICTs.

22 Take Back the Tech! (2013, November 15). Public/private. *Define your line. Shape your space. Take Back the Tech!* APCNews. <https://www.apc.org/en/node/18739/>.

23 UNDP. (2012). Gender Inequality Index. <https://data.undp.org/dataset/Table-4-Gender-Inequality-Index/pq34-nwq7>