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

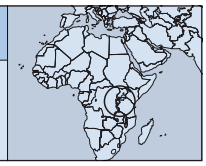
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

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

RWANDA

Ensuring security, or violating privacy and freedom?



Emmanuel Habumuremyi
www.giswatch.org/users/ehabumuremyi

Introduction

The rapid growth of information and communications technology (ICT) services in Rwanda has brought new policies, laws and strategies. These are aimed not only at alignment with established economic development and poverty reduction strategies, but also at ensuring that citizens and non-citizens enjoy full freedom, security and privacy. At the moment, the mobile phone penetration rate is estimated at over 65.4% when it comes to active SIM cards,[1] up from 53.1% in December 2012, and the internet penetration rate was approximately 22% in terms of mobile broadband subscriptions by June 2014.[2] The statistics are based on a population of 10,515,973 recorded in the 2012 national census.[3] However, communications surveillance is not a common issue discussed publicly. The reasons are hypothetical, including a lack of awareness of why surveillance is necessary, what its advantages or disadvantages are for people's rights, and how it is done.

The focus of this report is to discuss existing measures to keep citizens' personal data safe from internal and external intruders, and to examine the reasons and conditions under which surveillance of communications is conducted, as well as who is authorised to do so. It explores the current Rwandan legal framework, government commitments in this area and the international community's views on how the government honours these commitments.

Policy and political background

As Rwandans are becoming active users of smart devices (like mobile phones, iPads and tablets), as well as consumers of social media and other online facilities, on the one hand people are discovering how ICTs are helping them to share their private information, store personal data and discuss sensitive issues. On the other, they are finding out that if these communications are not well protected, they can be misused or abused by corporate entities, malicious people and public officials.

While writing on the rights to privacy in the digital age, the National Commission for Human Rights (NCHR) in Rwanda ascertained that measures have been taken at the national level to ensure respect for and protection of citizens' freedom and rights to privacy, including in the context of digital communications.[4]

The NCHR says that the first measures can be traced to the Constitution of the Republic of Rwanda,[5] which guarantees the protection and respect of the right to privacy. Article 22 states that the private life, family, home or correspondence of a person shall not be subjected to arbitrary interference, and that a person's home is inviolable. Article 34 paragraph 2 states that freedom of speech and freedom of information shall not prejudice public order and good morals, the right of every citizen to honour and good reputation, and the privacy of personal and family life.

The most cited laws established to ensure the respect of the right to privacy and data protection in Rwanda are the following:

- Law No. 02/2013 of 8 February 2013 regulating media (article 9)[6]
- Law No. 03/2013 of 8 February 2013 regulating access to information (article 4)[7]
- Law No. 48/2008 of 9 September 2008 relating to the interception of communications[8]
- The recently enacted ICT law[9]

1 www.rura.rw/fileadmin/docs/Montly_telecom_subsribers_telecom_subcribers_as_of_June.pdf

2 Republic of Rwanda. (2004). MYICT performance contract for FY 2014-2015, p. 4.

3 www.statistics.gov.rw

4 National Commission for Human Rights. (n/d). *The rights to privacy in the digital age*. www.ohchr.org/Documents/Issues/Privacy/RwandaNHRC.pdf

5 www.parliament.gov.rw/fileadmin/Images2013/Rwandan_Constitution.pdf

6 www.mhc.gov.rw/fileadmin/templates/PdfDocuments/Laws/Official_Gazette_n__10_of_11_March_2013.pdf

7 www.mhc.gov.rw/fileadmin/templates/PdfDocuments/Laws/Official_Gazette_n__10_of_11_March_2013.pdf

8 lip.alfa-xp.com/lip/AmategekoDB.aspx?Mode=r&pid=7801&iid=2369

9 www.parliament.gov.rw/uploads/tx_publications/DRAFT_LAW___GOVERNING_INFORMATION_AND_COMMUNICATION_TECHNOLOGIES.pdf

- Law No. 44/2001 of 30 November 2001 governing telecommunications[10]
- Law No. 18/2010 of 12 May 2010 relating to electronic messages, electronic signatures and electronic transactions (the e-signature law)[11]
- Law No. 54/2011 of 14 December 2011 relating to the rights and the protection of the child (Article 16).

The government of Rwanda honours international commitments on internet governance. During the NETmundial internet governance discussions, at which Rwanda was represented by its Minister of Youth and ICT Jean Philbert Nsengimana,[12] the internet was taken as "a universal global resource, that should remain a secure, stable, resilient, and trustworthy network" and Rwanda supported the proposal of an internet governance framework which is "inclusive, multistakeholder, effective, legitimate, and evolving."[13]

Rwanda ratified the International Covenant on Civil and Political Rights, and is therefore bound by Article 17, which states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[14]

The above-mentioned regulations are applied domestically. According to Privacy International, the corporate sector plays a critical role in facilitating surveillance.[15] Interception and monitoring of individuals' communications are becoming more widespread, more indiscriminate and more invasive, just as our reliance on electronic communications increases.[16] This report does not have data on how big corporations' privacy policies, such as those of Google and Yahoo, among others, affect internet users in Rwanda. This is a matter for attention, since some of the spokespeople of these companies have been wilfully tone-deaf on the issue in the past: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[17]

Communications interception and collection of personal data vs international human rights principles

Rwanda, like many countries in the world, has put in place "measures to establish and maintain independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for state surveillance of communication, its interception and collection of personal data."[18]

A certain number of international human rights organisations and external journalist reports attack the government, at the level of ranking the country not free or partly free, citing the interception of communications among other factors they consider hindering freedom and privacy.

When the bill on the interception of communications was awaiting approval by the Rwandan Senate, sensational headlines in international newspaper reports and interpretations like "in the name of 'public security' Rwandan police and security forces will be able to spy on journalists, human rights defenders, lawyers and activists who criticise or oppose the Kagame regime" appeared.[19]

With today's global evolution driven by the advance of ICTs, the registration of identity information to activate a mobile SIM card is fast becoming universal in Africa. SIM registration and the collection of biometric data were among the most criticised projects when they were being implemented in Rwanda. They were considered by some as components of a growing surveillance assemblage that also incorporates other technologies such as electronic passport systems, new video surveillance technologies, and electronic health systems.[20]

SIM registration

2013 was characterised by a campaign encouraging all citizens of Rwanda to begin registering their SIM cards, an activity started in February and ending in July the same year. According to

10 www.rura.rw/fileadmin/laws/TelecomLaw.pdf

11 www.rwanda.eregulations.org/media/Electronic%20law.pdf

12 Kenyanito, E. P. (2014, May 9). What did Africa get out of NetMundial internet governance discussions? *Access*. https://www.accessnow.org/blog/2014/05/09/spotlight-on-african-contributions-to-internet-governance-discussions-part-

13 document.netmundial.br/1-internet-governance-principles

14 www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

15 Nyst, C. (2014, July 17). UN privacy report a game-changer in fighting unlawful surveillance. *Privacy International*. https://www.privacyinternational.org/blog/un-privacy-report-a-game-changer-in-fighting-unlawful-surveillance

16 https://www.privacyinternational.org/issues/communications-surveillance

17 Taylor, A. (2014, June 16). Google and Yahoo want to 'reset the net'. But can it work? *The Guardian*. www.theguardian.com/commentisfree/2014/jun/16/google-yahoo-reset-the-net-tech-nsa-data-collection

18 National Commission for Human Rights. (n/d). Op. cit.

19 Nyst, C. (2012, August 25). Rwandan government expands stranglehold on privacy and free expression. *Privacy International*. https://www.privacyinternational.org/blog/rwandan-government-expands-stranglehold-on-privacy-and-free-expression

20 Donovan, K. P., & Martin, A. K. (2014, February 3). The rise of African SIM registration. *First Monday*. firstmonday.org/ojs/index.php/fm/article/view/4351/3820

the then-director general of the Rwanda Utilities and Regulatory Authority (RURA), the exercise was due to "East African Community (EAC) resolutions where all countries agreed to implement the SIM card registration (SCR), which is related to the security of mobile subscribers – such as fighting mobile-based crimes – in the region."[21] This was confirmed by some researchers such as Nicola Jentzsch, who affirms that the East African Communications Organization (EACO) has been a major proponent of SIM registration, encouraging national governments in the region to adopt relevant laws and regulations, or to support voluntary initiatives. She went on to mention EACO's motivation: the belief that forcing customers to register SIM cards will reduce the opportunities for malevolent actors to use mobile devices anonymously to undertake unlawful or socially harmful activities, including kidnapping, drug trafficking and terrorism.[22]

East African countries like Kenya, Rwanda, Uganda and South Sudan are working towards establishing a cross-border SIM card registration framework in a new effort to curb the rise in crimes perpetrated through the use of mobile devices.[23]

Biometric identity

A biometric system for the identification of citizens stores all the resources needed to identify a person, based on their digitised fingerprints and photographs.

In Rwanda, the National Identification Agency (NIDA) has opted for ICT-based initiatives to speed up citizen registration. Under the motto "Smart ID, Smart Ideas", Rwanda has built a population register to issue secure national identity cards, driving permits and integrated smartcards that will be multi-purpose to enhance quick public services delivery.[24] Services that come with the card include personal identification, insurance assessments, and bank and immigration services, among others. This avoids the need to carry many cards to access the different services.

Since January 2014, citizens from three partner states (Rwanda, Kenya and Uganda) have begun to use the smartcard to cross their respective borders without presenting any passport or pass.[25] The interconnected national ID system is meant to facilitate the faster movement of people between the three countries, and at the same time to ensure that people moving from one country to another do not fake their nationalities and identities.

Arguments against the establishment of biometric data collection state that studies of national ID card programmes have consistently found that certain ethnic groups are disproportionately targeted for ID checks by the police. Privacy International goes further by pointing to the genocide against Tutsis in 1994, when ID cards designating their holders as Tutsis cost thousands of people their lives. For them, an ID card enables disparate identifying information about a person that is stored in different databases to be easily linked and analysed through data-mining techniques. This creates significant privacy vulnerability, especially given the fact that governments usually outsource the administration of ID programmes to unaccountable private companies.[26]

Following the success of the national ID programme, Rwandan government stakeholders are optimistic about the potential success of this initiative. Many stakeholders believe that the Rwandan smartcard initiative will enhance their quality of service delivery while reducing lengthy turnaround time.[27]

Interception of communications

In August 2013, the Rwandan government passed amendments to a 2008 law relating to the interception of communications. While reading most media articles criticising the law, laypeople in the field lose track of what it is and what it is not, when it is lawful and when it is unlawful, and who is authorised to intercept communications.

The law defines communications interception as "any act of listening, recording, storing, decrypting, intercepting, interfering with, or carrying out any other type of surveillance over voice or data communications without the knowledge of the user and without explicit permission to do so."[28]

21 Bright, E. (2013, February 4). SIM card registration gets under way. *The Rwanda Focus*. focus.rw/wp/2013/02/sim-card-registration-gets-under-way/

22 Donovan, K. P., & Martin, A. K. (2014, February 3). Op. cit.

23 Wokabi, C. (2013, December 23). East African states to share SIM card, national ID data. *Pan African Visions*. panafricanvisions.com/2013/east-african-states-share-sim-card-national-id-data

24 www.worldbank.org/content/dam/Worldbank/Event/social-protection/Building_Robust_Identification_Systems_Session_Packet.pdf

25 IWACU. (2014, January 14). ID cards to replace passports in EAC. *IWACU English News*. www.iwacu-burundi.org/blogs/english/id-cards-to-replace-passports-in-eac/

26 https://www.privacyinternational.org/issues/id

27 Sivan, S. K. (n/d). *Enhancing public and private sector delivery through Rwandan national smart card initiative*. www.appropriatetech.net/files/ENHANCING_PUBLIC_AND_PRIVATE_SECTOR_DELIVERY.pdf

28 Law relating to the interception of communications.

Relevant authorities are authorised to carry out interception of communications for national security purposes.[29] According to the law, this is done on a criminal suspect: "[W]hen all other procedures of obtaining evidence to establish truth have failed, the prosecutor in charge of investigations, may, after obtaining a written authorisation by the Prosecutor General of the Republic, listen, acknowledge and intercept record[ed] communications, conversations, telegrams, postal cards, telecommunications and other ways of communicating."[30]

The law governing telecommunications, meanwhile, recognises privacy and data protection, and forbids interception of communications in its Article 54. It states: "Every user's voice or data communications carried by means of a telecommunications network or telecommunications service, remains confidential to that user and the user's intended recipient of that voice or data communications." If a court authorises the interception or recording of communications in the interests of national security and the prevention, investigation, detection and prosecution of criminal offences, the above article is not applied.

Government authorities of "the relevant security organs" are authorised to apply for an interception warrant. In May 2014, the government appointed the Ombudsman and Deputy Ombudsman as a team of inspectors in charge of monitoring that interception of communication which is done in accordance with the law.[31] No person shall reveal any information which he/she accessed in the exercise of his/her responsibilities or duties in relation to this order, except when authorised by the head of the security organ which has carried out the interception (Article 8).[32]

The following acts are not considered as interception of communications:

- Evidence of a crime collected after the message reached the receiver.
- Evidence based on communication recorded by the sender or the receiver or other person without using a monitoring device for interception of communications.[33]

Conclusion

As is becoming the practice in most democratic countries, in Rwanda intercepts of oral, telephonic and digital communications are initiated by law enforcement or intelligence agencies only after approval by a judge, and only during the investigation of serious crimes.

Arguments against communication interception, based on asserting that the reasons advanced for interception are weak, seem to be on the extreme side when a developing country is involved. In the absence of clear case studies and unbiased opinions that consider both the pros and cons of communications surveillance, the public is not able to know how surveillance can make a safer society as proposed by governments, or how it can deteriorate their rights as argued by human rights activists.

With SIM registration, your email, ID and phone are linked together. The requirement by big corporations to provide a telephone number when using their services, for instance, is also dangerous and promotes unnecessary personal data surveillance, since users are not aware who is accessing their data and what the data is being used for.

Action steps

Apart from the existing laws in place, the Rwandan government should consider the following when it comes to communications surveillance:

- The government needs to sensitise Rwandan citizens through awareness campaigns on procedures, practices and legislation regarding the surveillance of communications. This should be done in order to increase their knowledge on matters related to surveillance on the one hand, and to help them use communication channels responsibly on the other hand.
- Telecommunications and internet service providers should increase the quality of what they offer to the clients, since poor service that requires citizens to seek help from a customer care desk is likely to expose the clients' privacy.
- Rwandan civil society and human rights organisations should be in a position to understand well what is involved in communications surveillance in order to avoid relying on speculative information.

29 Ibid.

30 Law N° 13/2004 relating to the Code of Criminal Procedure. www.refworld.org/docid/46c306492.html

31 2014 Presidential Order appointing inspectors in charge of monitoring the interception of communication.

32 2014 Prime Minister's Order determining modalities for the enforcement of the law regulating interception of communication.

33 Ibid.