



Suggestions for right to privacy-related questions to be included in the list of issues on Rwanda, Human Rights Committee, 114th session, June-July 2015

April 2015

1. Main concerns on the right to privacy in Rwanda

Article 17 of the International Covenant on Civil and Political Rights provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour or reputation. Any interference with the right to privacy can only be justified if it is in accordance with the law, has a legitimate objective and is conducted in a way that is necessary and proportionate. Surveillance activities must only be conducted when they are the only means of achieving a legitimate aim, or when there are multiple means, they are the least likely to infringe upon human rights.¹

The right to privacy is enshrined in the Constitution of Rwanda as follows:

"The private life, family, home or correspondence of a person shall not be subjected to arbitrary interference; his or her honour and good reputation shall be respected. A person's home is inviolable. No search of or entry into a home may be carried out without the consent of the owner, except in circumstances and in accordance with procedures determined by law. Confidentiality of correspondence and communication shall not be subject to waiver except in circumstances and in accordance with procedures determined by law." (Article 22.)²

The Rwandan Penal Code establishes a series of offences to protect the right to privacy³ and the 2013 Law on access to information prohibits publication of information held by a public or private body if it may involve interference in the privacy of an individual when it is not in the public interest.⁴

Despite these provisions, Privacy International has on-going concerns on the extent of respect and protection of the right to privacy in Rwanda. National legislation governing surveillance is inadequate, leaving significant gaps in safeguards, oversight and remedies against unlawful interference with the right to privacy. Rwanda has also failed to adopt a comprehensive personal data protection legislation. The recent introduction

¹ See Human Rights Committee, General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17); see also report by the UN High Commissioner for Human Rights, the right to privacy in the digital age, A/HRC/27/37, 30 June 2014. See also International Principles on the Application of Human Rights to Communications Surveillance, available at <https://necessaryandproportionate.org>

² See: http://www.parliament.gov.rw/fileadmin/Images2013/Rwandan_Constitution.pdf

³ Including invasion of personal privacy (Article 281), opening and diverting correspondence, and installing devices for unauthorized interception (Article 285), gathering personal information in computers (Article 286) and recording and publishing personal information (Article 287.)

⁴ Article 4, Law No 03/2013 of 08/02/2013 regulating access to information. See

http://www.humanrightsinitiative.org/postoftheday/2013/18/Rwanda_ATI_Law_March2013_NewDelhi_SatbirS.pdf

of measures to collect personal data in Rwanda make this legislative gap particularly problematic, exposing individuals to a significant breach of their right to privacy by state and non-state actors.

2. Concerns on state surveillance of private communications in Rwanda

The capacity of Rwandan authorities' surveillance of communications is unknown, although given the extent of the restrictions to freedom of expression and association, including repression of political dissent, attacks and threats to human rights defenders,⁵ there is a strong sense that the extent of state surveillance, including of online communications, is vast. This is of significant concern, given that the legal framework and oversight of interception of communication falls short of applicable international human rights standards.

The law that regulates telecommunications contains a general provision safeguarding the privacy of communications and some safeguards (including the requirement of court's authorisation for the interception of communications.)⁶

None of these limitations, nor the requirement of a court's order, are included in the 2013 law regulating the interception of communications (Law No 60/2013). While not explicitly repealing law 44/2001 in the regulation of these matters, the 2013 law repeals "all prior legal provisions".⁷ The 2013 law empowers the police, army and intelligence services to listen to and read private communications, both online and offline, in the interest of "*national security*". There is no requirement to justify the interference with someone's privacy as necessary and proportionate to a legitimate aim.

Interception warrants are issued by a prosecutor designed by the Minister of Justice. As such there is no requirement of prior judicial authorisation. Nor there seems to be independent judicial oversight on the application of the law: the only monitoring envisaged is by inspectors appointed by Presidential Order.

All communication service providers are required to ensure that their system are technically capable to enable communications interception upon request.

The law also provides for the interception of communications using technologies that do not require the facilitation by the relevant communication service provider. De facto, this provision allows Rwandan security agencies to hack into the telecommunication network without the communication provider knowledge or assistance.

The risk of abuse is very high, particularly as in Rwanda there is significant government control of political life and public discourse. For example, in April 2014, it was reported that Rwandan authorities had intercepted the communications of two suspects in a treason trial. According to reports, private messages sent over the phone, Whatsapp and Skype were presented in court as evidence to show conspiracy to topple the

⁵ See <https://www.amnesty.org/en/countries/africa/rwanda/report-rwanda/>

⁶ Law 44/2001 of 30 November 2001, available at: <http://www.rura.rw/fileadmin/laws/TelecomLaw.pdf> See in particular Article 54 ("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 communication.") and Article 55 detailing the procedures and limits of judicial authorisation of interception of communications.

⁷ See Article 15 of Law 60/2013 regulating the interception of communications, available at: http://rema.gov.rw/rema_doc/Laws/Itegeko%20rishya%20rya%20REMA.pdf

government.⁸ On 27 February 2015, the radio journalist, Cassien Ntamuhanga, and other co-accused were convicted and sentenced to imprisonment, in a decision strongly criticized by Reporters without Borders.⁹

3. Concerns about protection of privacy of journalists and their sources

The Media Law of 2013 contains some improvements to the previous legislation, including granting journalists the “right to seek, receive, give and broadcast information and ideas through media,” and explicitly provided for freedom of online communications.¹⁰ Despite these improvements, concerns remain about the protection of the right to privacy and the protection afforded to journalists' sources.¹¹ According to Article 13 of the law, “the court may order a journalist to reveal his/her sources of information whenever it is considered necessary for purposes of carrying out investigations or criminal proceedings.” As noted by Article 19, this provision would apply to any criminal trial and not limited to the most serious of criminal cases. Nor there is a requirement to establish whether other reasonable alternatives are available for obtaining the information before ordering the disclosure of the journalist's sources.¹²

Threats to independent journalists have been reported by the Committee to Protect Journalists. This includes the case of a journalist whose website was repeatedly suspended and who was threatened and warned to leave the country.¹³

4. Lack of comprehensive data protection law

Rwanda does not have yet a comprehensive data protection law. According to reports, a 2013 bill on data protection was drafted, containing provisions that would penalise unauthorised access to computer systems and data, unauthorised modification of computer data, unlawful possession of computer systems, devices and data, and unauthorised disclosure of passwords, among others things. However, concerns were expressed about broad exceptions to protection of personal data, on grounds of national sovereignty, national security and public policy.¹⁴

Rwanda's lack of comprehensive legislation on personal data protection is in contrast with recent positive developments in this area. Over the past decade, at least 15 African countries have enacted data protection laws and on 27 June 2014 the African Union adopted the AU Convention on Cyber-security and Personal Data Protection, which contains important principles to ensure the protection of personal data in the continent.¹⁵

⁸ See: <http://www.theeastafrican.co.ke/news/Phone-evidence-used-in-terror/-/2558/2294196/-/klwpvi/-/index.html>

⁹ See: <http://fr.rsf.org/rwanda-un-journaliste-rwandais-ecope-d-02-03-2015,47637.html>

¹⁰ See: http://rema.gov.rw/rema_doc/Laws/Itegeko%20rishya%20rya%20REMA.pdf

¹¹ See: Article 19 of the 2013 Media Law, Section 3, http://rema.gov.rw/rema_doc/Laws/Itegeko%20rishya%20rya%20REMA.pdf

¹² See: <http://www.article19.org/resources.php/resource/3665/en/rwanda:-media-law-does-not-go-far-enough>

¹³ See Legacy of Rwanda genocide includes media restrictions, self-censorship, available here:

<https://cpj.org/reports/NEWrwanda2014-english.pdf>

¹⁴ See <http://allafrica.com/stories/201307150285.html>

¹⁵ For an initial analysis of the AU Convention, see Graham Greenleaf and Marie Georges, The African Union's data privacy Convention: a major step toward global consistency?, available here:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546652

In Rwanda, the lack of a comprehensive data protection law is of particular concern in view of the introduction in recent years of government backed schemes to collect personal data of individuals.

In particular, according to a presentation made at a World Bank workshop in 2014, the Rwandan National Identification Agency (NIDA) has issued **biometric IDs** to more than 80 percent of the adult population. The IDs are used to proof identity to access a range of services ranging from banking to social security.¹⁶ Biometric IDs are also used to enable fingerprint banking.¹⁷

Further, in 2013 Rwanda introduced a requirement for **mandatory SIM card registration**, demanding SIM card owners to register their cards with service providers and all service providers to set up a database of all registered subscribers.¹⁸ The regulation of SIM card registration allows the Rwanda regulator (the Rwanda Utilities Regulatory Agency, RURA) unfettered access to the SIM card databases and contain other broad provisions to allow other authorized person or institution to have access to them.¹⁹

Mandatory SIM card registration facilitates the establishment of extensive databases of user information, eradicating the potential for anonymity of communications, enabling location-tracking, and simplifying communications surveillance and interception.

Without effective data protection provisions these and other initiatives, such as the introduction of e-passports,²⁰ are also exposing Rwandans to the risk of breaches of their right to privacy by state and non-state actors.

5. Proposed questions for the list of issues

Based on these observations, Privacy International proposes the following questions for the List of Issues:

Article 17:

- What measures is Rwanda taking to review its communications surveillance laws, policies and practices with the view to uphold the right to privacy in line with international human rights standards?;²¹
- Is Rwanda considering adopting a comprehensive data protection law that complies with international human rights standards and establishes an independent data protection authority?

¹⁶ South-South Learning Forum, March 2014, available here:

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

¹⁷ See <http://www.biometricupdate.com/201301/mobicash-and-kcb-bank-launch-fingerprint-banking-in-rwanda>

¹⁸ See:

http://rura.gov.rw/fileadmin/docs/Board_Decisions/FINAL_SIM_CARD_REGISTRATION_REGULATIONS.pdf .SIM card owners were given a deadline of 31 July, after which any unregistered SIM card was disconnected (see See <http://www.monitor.co.ug/News/National/Rwanda-switches-off-unregistered-SIM-cards/-/688334/1934958/-/rj2m4o/-/index.html>)

¹⁹ See:http://rura.gov.rw/fileadmin/docs/Board_Decisions/FINAL_SIM_CARD_REGISTRATION_REGULATIONS.pdf

²⁰ See: <http://allafrica.com/stories/201411250349.html>

²¹ More than 400 organisations and individuals have signed up to the International Principles on the Application of Human Rights to Communications Surveillance. The principles attempts to clarify how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to Communications Surveillance technologies and techniques. See <https://en.necessaryandproportionate.org/text>