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

April 2015

Main concerns on the right to privacy and communication surveillance in South Africa

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]

Privacy International, Right2Know, and the Association for Progressive Communications have on-going concerns on the practices of surveillance by South African intelligence and law enforcement agencies.[2] National legislation governing surveillance is inadequate, leaving significant regulatory gaps and providing weak safeguards, oversight and remedies against unlawful interference with the right to privacy, including mass surveillance. The government has also failed to meaningfully regulate the practice of the surveillance industry, having instead provided public funding to companies that export surveillance technologies to be used in violation of the right to privacy.

1. Inadequacies of national legislation regulating domestic surveillance

Broad powers to intercept personal communications and cases of abuse

Surveillance of domestic communications is regulated by the 2002 Regulation of

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 Privacy International is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. The Right2Know Campaign is a broad-based, grassroots campaign formed to champion and defend information rights and promote the free flow of information in South Africa. The Association for Progressive Communications (APC) is an international network and non-profit organisation founded in 1990 that wants everyone to have access to a free and open internet to improve lives and create a more just world.

Interception of Communications and Provision of Communications Related Information Act (RICA.)[3] The most recent report of the Parliamentary oversight committee noted a significant increase (170%) of the number of warrants for interceptions between 2008 and 2011, followed by a drop from 2012 to 2013.[4]

RICA requires the permission of a judge for the interception of communications, which can be granted if there are "reasonable grounds to believe" that a serious criminal offence has been or is being or probably will be committed (Section 16.)

There is no provision to require that those subjected to communication surveillance are notified that their communications have been intercepted, not even after the completion of the relevant investigation.

To guarantee the capacity of relevant state agencies to conduct interceptions, RICA requires that telecommunication service providers provide telecommunication services which have the capability of being intercepted (i.e. by building in their networks a backdoor for surveillance) (Section 30.)

The South Africa periodic report notes that "while the Act [RICA] may seem draconian on the face of it, one ought to bear in mind the elaborate mechanisms that the Act puts in place to ensure that its provisions are not abused."[5] In fact, the low threshold to trigger surveillance ("reasonable grounds") under RICA and the weakness of the oversight mechanism have led to abuses leading to violations of the right to privacy.

Notably, two journalists of the Sunday Times (the biggest weekend newspaper in South Africa) investigating cases of government corruption had their communications intercepted from 2010 reportedly with the view to disrupt their investigations and uncover their sources. The police obtained the judicial approval to intercept the mobile phone communications of the journalists by giving fictional names and suggesting such interception was needed to investigate a criminal syndicate. The Sunday Time has taken the case to court and two officers have been charged with violations of RICA.[6]

Retention of metadata

RICA also requires companies to store metadata (information about a communication, but not the content of such communication.)[7] Unlike for content of communication, a warrant to collect metadata requires the permission of any judge or magistrate.

3 Available at: http://www.internet.org.za/ricpci.html#interceptionofcommunicationunderinterceptiondirection
4 See Right2Know, Secret State of the Nations Report 2014, available at: http://www.r2k.org.za/2014/09/09/r2k-secrecy-report-2014/
5 South Africa initial report, UN doc. CCPR/C/ZAF/1, 28 November 2014, paragraph 184.
6 For more information, see Global Information Society Watch 2014, Communications surveillance in the digital age, pages 224-227.
7 This is defined in RICA as including "switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system".

The interception, collection and use of metadata interfere with the right to privacy, as it has been recognized by human rights experts, including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights.[8] The Court of Justice of the European Union noted that metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" and concluded that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[9]

Weak oversight and insufficient transparency

A Parliamentary committee to oversight the work of intelligence services in South Africa is mandated to release public report on the application of RICA. However, the data released do not provide number of individuals whose communications are subject to interception (only the number of warrants, that could include any number of individuals.) The report does not go into any details on the reasons these interceptions are carried out nor on the outcome and effectiveness they may have in preventing or investigating crimes. Further, there appears to be no centralised oversight or requirement of public disclosures of statistics on metadata's collection and use.

The lack of transparency on RICA's implementation has been a growing concern. Notably, Section 42 of RICA prohibits the disclosure of any information on the demands of interception. As a result, telecommunications companies are barred from publishing information, including aggregated statistics, both of interception of communications and of metadata.[10]

3. Mass surveillance by South African intelligence agencies and surveillance of political and social activists

Despite the aim of RICA to regulate the interception of communications, there have been consistent reports of state surveillance being carried out outside the RICA legal framework, in manners that violate the right to privacy. This is particularly so with regards to the National Communications Centre (NCC), the government's national facility for intercepting and collecting electronic signals on behalf of intelligence and security services in South Africa. It includes the collection and analysis of foreign signals (communication that emanates from outside the borders of South Africa or

8 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

9 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

10 See Vodafone, Law Enforcement Disclosure Report, 2014 and February 2015 update, available at: http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf

passes through or ends in South Africa.)

The capacity of the NCC to conduct unregulated mass surveillance was highlighted by the Mail & Guardian in 2013. The report noted how the agency is able to conduct mass monitoring of telecommunications, including conversations, emails, text messages and data, without judicial authorisations or other safeguards.[11]

A Ministerial Review Commission on Intelligence in South Africa (known as 'Matthews Commission') set up to review intelligence gathering in South Africa found that the NCC carries out surveillance (including mass interception of communications) that is unlawful and unconstitutional, because it fails to comply with the requirements of RICA.

The Matthews Commission report, released in 2008, made a series of recommendations to address the lack of control and regulations of the South African intelligence agencies. These recommendations have, by and large, not yet been acted upon by the government.[12]

South Africa adopted the General Intelligence Laws Amendment Act in 2013. The Act specifically excludes from the mandate of the intelligence agencies surveillance of "lawful political activity, advocacy, protest and dissent." Despite of this positive development, police and intelligence agencies continue to conduct surveillance of those legitimately exercising their right to freedom of expression, association and peaceful assembly.[13]

Concerns about the activities of the South African intelligence agencies have recently been surfaced when Al-Jazeera News reported in February 2015 on the leaked 'Spy Cable' documents.[14] One document, for example, revealed a secret agreement between Zimbabwe's Central intelligence Agency and South Africa's State Security Agency to exchange intelligence and information about "rogue NGOs" and "identify and profile subversive media".[15]

Further, the 2013 Act missed the opportunity to close a significant legislative gap, by failing to regulate the interception of foreign signal intelligence. The regulation of interception of foreign signal intelligence is instead expected to be considered in the context of the on-going review of the South African intelligence services.

---

11 Mail & Guardian, Spy wars: South Africa is not innocent, 21 June 2013, http://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent And also, Secret state: How the government spies on you, available at: http://mg.co.za/article/2011-10-14-secret-state/
12 Available at: http://www.ssronline.org/document_result.cfm?id=3852.
13 See Right2Know, "Big Brother Exposed: How South Africa's intelligence structures monitor and harass our movements, unions and activists", to be published in 2015.
14 See http://www.aljazeera.com/investigations/spycables.html
15 See http://www.documentcloud.org/documents/1672718-south-africa-zimbabwe-joint-action-plan-2011-2012.html

4. Support of surveillance technologies: the case of VASTech

On at least two occasions (2008 and 2010)[16], the South African government directly provided public funding to a surveillance technology company, VASTech, which in the mid/late '00s supplied mass surveillance technologies to the Libyan government of Colonel Gadhafi.[17] In 2005, according to a report leaked in February 2015, an Iranian delegation reportedly met with the South African government and companies such as VASTech in a bid to obtain surveillance technology.[18]

One of VASTech surveillance products, Zebra, was reportedly provided to the Libyan government in 2011. Zebra allowed the security services to capture "30 to 40 million minutes of mobile and landline conversations a month and archived them for years". Zebra also meant it could help those security services identify relationships between individuals based on analysis of their calling patterns.[19] It is advertised as a monitoring system "which connects to telecoms networks and intercepts voice, fax, and SMS communications" and has the "power and capacity to record everything, content included".[20]

Responding to a Privacy International letter, the South Africa Department of Trade and Industry noted on 18 December 2013 that VASTech provided all the required information in advance of the funding being made available and had the government known that the technology involved was advertised as being capable of mass surveillance, the outcome of the funding would "certainly" have been different.[21] Further, a spokesperson of the Department of Trade and Industry confirmed that the government approved the funding of Zebra and "knew that it would be for mass surveillance". However, the Department noted that when the approval took place, it did not know it would be "used for nefarious purposes" and they were "led to believe" Zebra was only meant for "monitoring borders and stadiums, among other things". However, according to the Mail & Guardian, the South African government continues to fund VASTech, supporting a new software, called "Next".[22]

The government's reply suggests that any due diligence process being carried out in either the direct funding of the development of the technology, or the export process

16 See http://www.spii.co.za/content/Annual%20Reports/SPII_Annual_Report_2008.pdf and http://www.spii.co.za/content/Annual%20Reports/SPII_Annual_Report_2010.pdf
17 Mail & Guardian, Millions were handed to an SA company that supplied mass surveillance technology to Libya, available at: http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware
18 See https://s3.amazonaws.com/s3.documentcloud.org/documents/1672715/south-africa-operational-target-analysis-of-iran.pdf
19 Wall Street Journal, Firms Aided Libyan Spies First Look Inside Security Unit Shows How Citizens Were Tracked, available at: http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388
20 See at: http://wikileaks.org/spyfiles/files/0/182_VASTECH-201110-BROCHURES.pdf
21 Letter by Dr Rob Davies, MP, Minister of Trade and Industry, 18 December 2013.
22 Mail & Guardian, DTI 'funded Gaddafi spyware', 22 November 2013, available at: http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware

did not include any meaningful assessment of the surveillance technology's effects on human rights, including the right to privacy.

5. Failure to fully implement legislation on data protection

In 2013 South Africa passed a data protection law, the Protection of Personal Information Act.

The Act does not apply to the processing of personal information carried out for purposes of national security (including identification of terrorist activities) and prevention or investigation of crimes "to the extent that adequate safeguards have been established in legislation for the protection of such personal information" (Section 6.)

However, the President has yet to set a commencement date for the full enactment of this legislation. As a result, the potential of this law to protect the right to privacy remains untested and notably the authority envisaged to monitor the protection afforded to personal data is yet to be constituted.

This is of particular concern in light of the requirement under RICA for mandatory SIM card registration, and the introduction in recent years of government backed schemes to collect personal data of individuals, such as using of biometrics for passports and banking.

Mandatory SIM registration, in effect, eradicates the ability of mobile phone users to communicate anonymously and facilities mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies. The potential for misuse of such information is enormous. SIM registration can also have discriminatory effects – the poorest individuals (many of whom already find themselves disadvantaged by or excluded from the spread of mobile technology) are often unable to buy or register SIM cards because they do not have identification documents or proof of residence.[23] The justifications commonly given for SIM registration – that it will assist in reducing the abuse of telecommunications services for the purpose of criminal and fraudulent activity – are unfounded. SIM registration has not been effective in curbing crime, and instead has fueled the growth of identity-related crime and black markets to service those wishing to remain anonymous.[24]

23 See Freedom House, Freedom on the Net, 2014, page 703.
24 See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2013.

7. Proposed questions for the list of issues

Based on these observations, Privacy International Privacy International, Right2Know, and the Association for Progressive Communications propose the following questions for the List of Issues:

Article 17:

- What measures is South Africa taking to ensure that its state security and intelligence agencies respect the right to privacy?
- In particular, how does South Africa ensure that all interception activities are only carried out on the basis of judicial authorisation and communications interception regime complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are intercepted?
- What measures is South Africa planning to strengthen effective oversight over the surveillance practices of its state security and intelligence agencies?
- How does South Africa regulate the export of surveillance technologies by private companies based in the country and how such export regulation takes into consideration the potential risks that such technologies pose to the right to privacy when sold to foreign governments or other third parties?
- When is South Africa going to fully operationalise the provisions of the Protection of Personal Information Act 2013?

Articles 19, 21 and 22

- What measures is South Africa taking to address the reports of unlawful surveillance of journalists, political activists and human rights defenders to ensure that their right to freedom of expression, peaceful assembly and association are respected and protected?