PRIVACY INTERNATIONAL

Human Rights Committee 116th Session

The Right to Privacy in South Africa

Submission in advance of the consideration of the periodic report of South Africa, Human Rights Committee, 116th Session

7 – 31 March 2016


PRIVACY
INTERNATIONAL


RIGHT2KNOW


APC

1. Introduction

Privacy International, Right2Know, and the Association for Progressive Communications (hereinafter "the organisations") note the written replies by the government of South Africa to the list of issues on South Africa's laws, policies and practices related to interception of personal communications and protection of personal data.[1]

The organisations have on-going concerns on the practices of surveillance by South African intelligence and law enforcement agencies.[2] In this submission, the organisations provide the Committee with additional, up to date information to that contained in the briefing submitted to the Committee in advance of the adoption of the list of issues in April 2015.[3] They also reiterate some of the concerns expressed in the April 2015's briefing.

2. Interception of communications, including mass surveillance, outside of RICA

As noted in the government's replies, the Regulation of Interception of Communications and Provision of Communication-related information Act (RICA) was enacted in response to modern day criminality.

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 (Article 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) (Article 30.) Article 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.[4]

There is no other legislation in South Africa specifically regulating the interception of communications. Interception of communications outside the RICA regime would be unlawful, and RICA itself criminalises unlawful interception.

1 UN Doc. CCPR/C/ZAF/Q/1/Add.1, 31 December 2015.

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.

3 Available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fICO%2fZAF%2f20241&Lang=en

4 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

Mass Interception of Communications

There continue to be consistent reports of state surveillance being carried out outside the RICA legal framework, in manners that violate the right to privacy.[5] 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 passes through or ends in South Africa.)

Since in 2008 the Ministerial Review Commission on Intelligence in South Africa (known as 'Matthews Commission') 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,[6] reports of unlawful surveillance continue to emerge.

Most recently, according to the Mail & Guardian in 2015, the NCC has the capacity for mass interception of communications and is carrying out mass interception of communications within South Africa.[7]

Significantly, the NCC has never been regulated by law. Attempts to give the NCC a statutory basis dates back to at least 2008.[8] Later, in 2011, the General Intelligence Laws Amendment Bill aimed to bring all the intelligence structures under the State Security Agency. However, during deliberations on the Bill all references to foreign signals intelligence were withdrawn, and attempts to introduce measures to regulated the NCC were blocked.[9]

Hence, when eventually adopted, the General Intelligence Laws Amendment Act (2013) missed the opportunity to close this 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.

The technical capabilities of South African agencies to conduct surveillance are unknown and the government refuses to respond to requests of more

5 See, for example, Right2Know, Big Brother Exposed: How South Africa's intelligence structures monitor and harass our movements, unions and activists (http://bigbrother.r2k.org.za/wp-content/uploads/Big-Brother-Exposed-R2K-handbook-on-surveillance-web.pdf); Jane Duncan, Communications surveillance in South Africa: The case of the Sunday Times newspaper (https://www.giswatch.org/en/country-report/communications-surveillance/south-africa); and Mail & Guardian, Spy tapes: McCarthy, 'Billy the Kid' and me (http://mg.co.za/article/2014-10-02-lessons-in-accountability-on-spy-tapes).

6 Available at: http://www.ssronline.org/document_result.cfm?id=3852.

7 See Mail & Guardian, Say nothing – the spooks are listening, 18 December 2015 (available here: http://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening)

8 The then Minister of Intelligence, Ronnie Kasrils, introduced two Bills, the Intelligence Services Amendment Bill and the National Strategic Intelligence Amendment Bill, to give a legislative backdrop to the NCC. The first provided for the establishment of the Centre and the second provided for the functions of the Centre, including the collecting and analysing of foreign signals intelligence (see Mail & Guardian, Spooks skip legal process, available here: http://mg.co.za/article/2008-07-16-spooks-skip-legal-process.) The bills were both withdrawn in 2008, as the Parliamentary committee apparently felt that too much work had to be done on these bills. They recommended that they be reintroduced when the new parliament was established (an election was pending).

9 The Parliamentary committee minutes record the following: "The Chairperson advised that the omission of any reference to the NCC and NICOC was a matter of policy. The proposed new White Paper on Intelligence would be a more suitable forum for introducing policy changes relevant to the NCC and NICOC. The intention of the Bill was to establish the SSA as a legal entity so that proper managerial and financial controls could be implemented." (Minutes available here: https://pmg.org.za/committee-meeting/15643/).

information under the policy that they cannot "disclose operational details and capabilities".[10]

The Matthews' 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]

"Grabbers" or "IMSI catchers"

Recently, it emerged that a particular type of privacy intrusive surveillance technology, "grabbers" or "IMSI catchers", has reportedly been deployed by the South African police. RICA does not regulate this specific type of technology and it is not clear if the police applies for interception direction under RICA before deploying it. On 20 November 2015, following reports that one officer was in possession of one of these devices for private intelligence use, the Parliament Joint Standing Committee on Intelligence expressed concerns about the use of such technology and stated that it intends to "revisit RICA with a view of whether any changes would be required to strengthen the Act in the likely event that the Judge is not sufficiently empowered to deal with matters such as grabbers."[12]

"IMSI catchers" are devices that mimic the operation of a cell tower device in order to entice a users' mobile phone to surrender personally identifiable data such as the SIM card number (IMSI). In recent years, "IMSI catchers" have become far more sophisticated and can perform interception of voice, SMS and data. They are also able to operate in a passive mode that is virtually undetectable as it does not transmit any data. In its concluding observations on the Republic of Korea, the Committee expressed its concerns about "the operation and insufficient regulation in practice of so called 'base-station'".[13] The technology reportedly in the hands of the South African police raises similar concerns, due to the lack of specific regulations of its use.

3. Blanket, indiscriminate retention of metadata

Beyond the concerns already expressed in the previous submission, the organisations would like to draw the Committee's attention to the regime of retention of communications data in South Africa. Article 30(1)(b) of RICA requires telecommunication service providers to store communications data, i.e. information about a communication, but not the content of such communication[14], for up to five years.

10 S The Parliamentary committee minutes record the following: "The Chairperson advised that the omission of any reference to the NCC and NICOC was a matter of policy. The proposed new White Paper on Intelligence would be a more suitable forum for introducing policy changes relevant to the NCC and NICOC. The intention of the Bill was to establish the SSA as a legal entity so that proper managerial and financial controls could be implemented." (Minutes available here: https://pmg.org.za/committee-meeting/15643/).ee, for example, reply from spokesperson for the State Security Agency reported in Mail & Guardian, How cops and crooks can 'grab' your cellphone - and you, 27 November 2015 (available here: http://mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-cellphone-and-you)

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 See http://www.parliament.gov.za/live/content.php?Item_ID=8495

13 Concluding observations of the Human Rights Committee on the fourth periodic report of the Republic of Korea, UN Doc. CCPR/C/KOR/CO/4, 3 December 2015.

14 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".

There is a significant interference with individual's rights caused by a regime that permits the retention of immense quantities of their communications data, not based on reasonable suspicion. In Digital Rights Ireland v Minister for Communications and others, the Grand Chamber of the CJEU concluded that the 2006 Data Retention Directive, which required communications service providers to retain customer data for up to two years for the purpose of preventing and detecting serious crime, breached the rights to privacy and data protection.

The CJEU observed that the scope of the data retention "entails an interference with the fundamental rights of practically the entire European population". The Court went on to note the Directive was flawed for not requiring any relationship between the data whose retention was provided for and a threat to public security. The Grand Chamber concluded that the Directive amounted to a "wide-ranging and particularly serious interference" with the rights to privacy and data protection "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary".[15]

Similar conclusions can be drawn with regards to the blanket, mandatory data retention regime imposed in RICA. Because of its untargeted and indiscriminate scope, Article 30(1)(b) of RICA does not meet the requirements of necessity and proportionality and therefore violates Article 17 of the International Covenant on Civil and Political Rights.

4. Draft Cybercrime and Cybersecurity Bill

In August 2015, the government published a draft Cybercrimes and Cybersecurity Bill.[16] The 128 pages draft Bill contains a range of measures which, if adopted, will threaten the respect and protection of the right to privacy, as well as the right to freedom of expression and association. In particular, the organisations are concerned by the following provisions: The lack of any defence for disclosure of information on public interest grounds and the overbroad definition of "national critical information infrastructure" (see definitions in the draft Bill), which could further reduce transparency and access to information of government activities.

The vague grounds for issuing a search warrants (Article 29), the fact that it can affect not only suspects but any persons "who is believed, on reasonable grounds, to furnish information" related to investigation. Further, Article 29(f) the very broad powers that can be given, including to obtain passwords and decryption keys without additional safeguards or limitations (such as those imposed for example in RICA).

The lack of user's notification after a warrant has been issued and the strict prohibition of disclosure of information, applicable also to communications service providers, which is carries a penalty of conviction or a fine (Article 38.)

15 Judgment in Digital Rights Ireland case (joined cases C-293/12 and C-594/12) available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

16 Available here: http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf

Provisions in Chapter 9 of the draft Bill which makes service providers – even if somewhat indirectly – responsible for monitoring the behaviour of users. This could encourage service providers to interfere with users' rights to privacy.

5. Data protection

The South Africa government, in its replies, states that the national assembly is identifying candidates for the Chairperson and other members of the information and privacy regulator to be recommended to the President for appointment. However, no indication has been given on the process to identify suitable candidates, nor is there a schedule. While appreciating that the South African institutions need adequate time and have competing priorities, the organisations remain deeply concerned that three years since the adoption of the Protection of Personal Information Act, the Act remains, for most significant part, unimplemented and, in particular, there is still no independent mechanism to monitor and enforce data protection legislation.

As noted in the organisations' submission of April 2015, the lack of implementation of the data protection law is of particular concerns given the requirements imposed by RICA on telecommunications service providers to retain communication data as well as mandatory SIM card registration.

6. Proposed recommendations

Based on these observations, Privacy International, Right2Know, and the Association for Progressive Communications propose the following recommendations to the South African government:

- Take all necessary measures to ensure that its surveillance activities, both within and outside South Africa, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance; refraining from engaging in mass surveillance and adequately and transparently regulating information sharing with intelligence partners.

- In particular review RICA to ensure that it is consistent with protections in the Constitution and that it covers all forms of interception, retention and analysis of personal data for surveillance purposes; and ensure that interception of communications, including of communications data, by law enforcement and security services are only carried out on the basis of judicial authorisation.

- Develop a legislative framework for the activities and mandate of the National Communications Centre (NCC) in way that is compliant with the International Covenant on Civil and Political Rights.

- Publicly avow the surveillance technologies capacities of law enforcement and security services and ensure that the use of technologies such as "grabbers" or "IMSI catchers" are properly regulated and overseen by independent authorities to prevent arbitrary use.

- Establish strong and independent oversight mandates with a view to preventing abuses and ensure that individuals have access to effective remedies including by notifying persons whose communications are subjected to surveillance as soon as notification can be done without seriously jeopardise the purpose of the measure.

- Repeal the provision in RICA imposing mandatory retention of communication data and SIM card registration.

- Regulate the export of surveillance technologies by private companies based in South Africa, including by preventing the export of surveillance technologies where there is a risk they will be used to undermine human rights, or if there is no clear legal framework governing their use.

- Expedite the process of appointment of the information and data protection authority and the overall full operationalisation of the Protection of Personal Information Act.