PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
27th Session – South Africa

# The Right to Privacy in South Africa

**Submitted by Right2Know Campaign and Privacy International**

**October 2016**




PRIVACY INTERNATIONAL

## Submitted by Right2Know Campaign and Privacy International

## October 2016

## I. Introduction

1. This stakeholder report is a submission by Privacy International (PI) and the Right2Know Campaign (R2K). This report has been prepared with the assistance and research done by the Media Policy and Democracy Project.

2. PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. R2K is a broad-based, grassroots campaign formed to champion and defend information rights and promote the free flow of information in South Africa.

3. R2K and PI wish to bring concerns about the protection and promotion of the right to privacy in South Africa before the Human Rights Council for consideration in South Africa's upcoming Universal Periodic Review (UPR).

4. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association. Activities that restrict the right to privacy, such as surveillance, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2]

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate state obligations related to the protection of personal data.[3]

6. A number of international instruments enshrine data protection principles,[4] and many domestic legislatures have incorporated such principles into national law.[5]

1 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

2 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 (article 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. 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 (article 17).

3 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 (article 17).

4 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).

5 As of December 2014, over 100 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (December 8, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416.

## II. Domestic laws related to privacy

7. The state is required to respect, protect, promote and fulfil the rights in the Bill of Rights (section 7(2) of the Constitution). The right to privacy is constitutionally entrenched in the South African Bill of Rights. In this regard, section 14 of the Constitution of the Republic of South Africa, 1996 (the Constitution) provides as follows:

> *"Everyone has the right to privacy, which includes the right not to have:*
> *(a) their person or home searched;*
> *(b) their property searched;*
> *(c) their possessions seized;*
> *(d) the privacy of their communications infringed."*

8. There are various pieces of legislation that implicate the right to privacy. Of particular importance is the Protection of Personal Information Act 4 of 2013 (POPI), which deals with data protection; the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), which deals with the interception of communications; and the Electronic Communications and Transactions Act 25 of 2002 (ECTA), particularly in relation to encryption. Reference will also be made to the 2008 report of the Ministerial Review Commission on Intelligence titled "Intelligence in a constitutional democracy"[6] (Matthews Commission report).

9. Of further significance are two proposed laws: the Protection of State Information Bill[7] (POSIB); and the draft Cybercrimes and Cybersecurity Bill.[8] These proposed laws in their current forms are deeply problematic and of significant concern. These, too, will be dealt with in more detail below.

## III. International obligations

10. The Constitution requires that, when interpreting the Bill of Rights, a court "must consider international law" (section 39(1)(b) of the Constitution); and that, when interpreting any legislation, a court "must prefer any reasonable interpretation of the legislation that is consistent with international law over any alternative interpretation that is inconsistent with international law" (section 233 of the Constitution). These provisions – peremptory in their terms – do not stipulate or limit which sources of international law must be considered and applied; rather, as has been interpreted by the Constitutional Court,[9] the Constitution requires the courts to consider the ambit of both binding and non-binding international law as appropriate under the circumstances.

6 Ministerial Review Commission on Intelligence (J Matthews, F Ginwala and L Nathan) "Intelligence in a constitutional democracy: Final report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP" (10 September 2008) (accessible at http://www.r2k.org.za/matthews-commission).
7 B6D-2010 (accessible at http://www.r2k.org.za/secrecy-bill).
8 B-2015 (accessible at http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf).
9 See, for instance, S v Makwanyane [1995] ZACC 3; 1995 (3) SA 391 (CC); 1995 (6) BCLR 665 (CC) (para 35).

11. South Africa's international obligations are therefore of key importance, both on the international and domestic planes. In light of these constitutional provisions, the guidance, observations and recommendations made by relevant treaty bodies, and notably through the process of the UPR, are critical in understanding the ambit of South Africa's obligations in relation to the rights under examination. This may potentially have relevance in a range of ways, such as in monitoring state conduct, advocacy domestically, regionally and internationally, and possibly even in litigation.

12. South Africa has ratified two international treaties relevant to the right to privacy:

    - The African Charter on the Rights and Welfare of the Child (article 10); and

    - The International Covenant on Civil and Political Rights (ICCPR) (article 17).

13. The United Nations Human Rights Committee (the Committee) considered South Africa's initial report on the ICCPR in March 2016, and adopted the following concluding observations in respect of the right to privacy and the interception of private communications:[10]

> *"The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the [RICA]. It is also concerned about the wide scope of the data retention regime under the Act. The Committee is further concerned at reports of unlawful surveillances practices, including mass interception of communications, carried out by the National Communications Centre and at delays in fully operationalizing the Protection of Personal Information Act, 2013, due in particular to delays in the establishment of an Information Regulator (arts.17 and 21).*
>
> *The State party should take all necessary measures to ensure that its surveillance activities conform to its obligations under the [ICCPR], including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality. The State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization and consider revoking or limiting the requirement for mandatory retention of data by third parties. It should also ensure that interception of communications by law enforcement and security services is carried out only on the basis of the law and under judicial supervision. The State party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies."*

14. Thereafter, in June 2016, South Africa presented its state report at the African Commission on Human and Peoples' Rights (ACHPR) regarding compliance with the African Charter on Human and Peoples' Rights (African

10 Human Rights Committee, Concluding Observations on the Initial Report of South Africa, CCPR/C/ZAF/CO/1, 27 April 2016 (paras 42-43).

Charter).[11] Although the right to privacy is not expressly contained in the African Charter, the ACHPR recommended that:[12]

> *"The [ACHPR] recommends that South Africa should:*
> *(i) accelerate the enactment of the Protection of State Information Bill and ensure that the Bill is in line with regional and international standards;*
> *(ii) expedite the establishment of the Information Regulator;*
> *(iii) amend the Cybercrimes and Cybersecurity Bill in line with international best practices on access to information …"*

15. These concluding observations and recommendations bear reiterating as all of the issues highlighted therein – RICA, POSIB and the Cybercrimes and Cybersecurity Bill, as well as the operationalisation of the Information Regulator – are all issues that remain of concern, and will be addressed further below.

## IV. Follow up from the previous review

### *(a) No express mention of the right to privacy*

16. During South Africa's previous review, no express mention was made of the right to privacy in the National Report submitted by South Africa[13] or the report of the Working Group.[14] In light of this, and given recent developments, it is therefore particularly appropriate for these matters to be given due regard in the upcoming review.

### *(b) Recommendations regarding the Protection of State Information Bill*

17. We do, however, note that various recommendations related to POSIB, albeit in the context of the right to freedom of expression and access to information.[15] In addition to these rights, the POSIB does also implicate the right to privacy, particularly insofar as it relates to the powers and accountability of the intelligence and security services. We deal with POSIB in more detail below. Suffice it to say at this stage that, many of the substantive concerns have not as yet been addressed,[16] and the text

11 African Commission on Human and Peoples' Rights, Concluding Observations and Recommendations on the Combined Second Periodic Report under the African Charter on Human and Peoples' Rights and the Initial Report under the Protocol to the African Charter on the Rights of Women in Africa of the Republic of South Africa, 9-18 June 2016.
12 Ibid (paras 35 and 51).
13 A/HRC/WG.6/13/ZAF/1.
14 A/HRC/21/16.
15 These recommendations provided as follows:
Recommendation 124.99: Ensure that the Protection of State Information Bill, when adopted, fully complies with international human rights law (Norway);
Recommendation 124.101: Reconsider the Protection of State Information Bill to ensure its conformity with ICCPR, in particular by removing excessive penalties for publication of classified information and the inclusion of a public interest defence (Czech Republic);
Recommendation 124.102: Continue amending and improving the project of the Protection of State Information Bill as this law, in the form proposed to the Parliament earlier this year, has the potential to undermine the right to access to information and freedom of expression under the pretext of national security and national interest (Poland);
Recommendation 124.106: Engage civil society, activists, NGOs and media to seek common ground on the Protection of State Information Bill (United States of America);
Recommendation 124.107: Safeguard the freedom of the press, through the abrogation of the Protection of Information Bill (Germany);
Recommendation 124.100: Ensure that the Protection of State Information Bill and other statutory measures do not violate the right to freedom of expression or unduly impede access to public domain information (Canada);
Recommendation 124.103: Amend the draft bill on the Protection of State Information so that freedom of press is not curtailed in a disproportionate manner (Switzerland);
Recommendation 124.104: Consider suspending the enactment of the Protection of State Information Bill, approved last November (Portugal);
Recommendation 124.105: Remain a promoter of freedom of expression, at national and international levels, and to review the current text of the Protection of State Information Bill (Sweden).
16 For an overview of our concerns with POSIB, see: http://www.r2k.org.za/2014/09/11/whats-still-wrong-with-the-secrecy-bill/.

has not been revised in line with the recommendations from the previous UPR. In particular, the current draft still does not comply with constitutional or international law standards; still does not include a public interest or public domain defence; and continues to impede the rights to freedom of expression and access to information.

18. We turn next to consider key areas of concern relating to the right to privacy that were not addressed during the previous review.

## V. Key areas of concern

### *(a) Covert surveillance*

*Low burden of proof*

19. RICA sets out the legal grounds on which interception orders may be issued. RICA requires the permission of the designated 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 of RICA). This speculative basis provides a low threshold for the granting of interception directions, and is patently open to abuse.

20. The burden is even lower with regard to stored metadata. In terms of RICA, telecommunications service providers are required to store metadata (ie. information about a communication) for up to five years (section 30(1)(b) of RICA). In order to access this information, any sitting magistrate or high court judge can issue a warrant for stored metadata. There does not appear to be any oversight or reporting on how often magistrates or high court judges issue such warrants. It is now widely accepted that metadata is often as sensitive as the content of the communication, and we would contend that the same safeguards should apply.

*No user notification of interception*

21. The low threshold for the granting of an interception order is exacerbated by the failure of RICA to provide for any mechanism for users to be notified of their communications having been intercepted. Rather, persons whose communications have been intercepted are never informed of this, even if the application is unsuccessful or after the relevant investigation has been completed. User notification provisions would provide a strong and important oversight mechanism to ensure that interception orders were being appropriately sought and granted. At present, there is no opportunity for affected parties to review decisions of the designated judge, as such persons simply do not know of the interception. Failure to provide for this directly impacts individuals' ability to seek redress in case of unlawful infringement of their right to privacy.

*Mass interception of communications*

22. The National Communications Centre (NCC) is 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 (ie. communication that emanates from outside the borders of South Africa or passes through or ends in South Africa).

23. In 2008, the Matthews Commission report found that the NCC carries out intelligence activities, including mass interception of communications, in a manner that is unlawful and unconstitutional because it fails to comply with the requirements of RICA.[17] It is of deep concern, however, that the NCC has never been, and continues not to be, regulated by law. Although the General Intelligence Law Amendment Bill aimed to bring all of the intelligence structures under the State Security Agency, all references to foreign signals intelligence were withdrawn during the deliberations. According to the minutes of the Parliamentary Committee:[18]

> "The Chairperson advised that the omission of any reference to the NCC and [National Intelligence Co-ordinating Committee]. The proposed new White Paper on Intelligence would be a more suitable forum for introducing policy changes relevant to the NCC and [National Intelligence Co-ordinating Committee]. The intention of the Bill was to establish the [State Security Agency] as a legal entity so that proper managerial and financial controls could be implemented."

24. One of the key recommendations contained in the Matthews Commission report was that any legislation regulating the NCC should make clear that the NCC is bound by RICA, most notably the provisions requiring judicial authorisation for interception. Moreover, the Matthews Commission report recommended that any such underpinning legislation should indicate which intelligence and law enforcement bodies are entitled to apply to the NCC for assistance with the interception of communication, and should describe the information that must be contained in an application for signals monitoring.

25. According to the Matthews Commission report, any underpinning legislation should ensure that the interception of communications is a method of last resort, and may only occur where there are reasonable grounds to believe that a serious criminal offence has been, is being or is likely to be, committed. It should also cover the NCC's 'environmental scanning' of signals, and the discarding of personal information that is acquired while intercepting communications where the information is unrelated to the commission of a serious criminal offence.

17 Matthews Commission report (pp 180-202). See, also, Mail & Guardian "Say nothing – the spooks are listening" (18 December 2015) (accessible at http://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening).
18 Accessible at https://pmg.org.za/committeemeeting/15643/.
19 Accessible at http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

26. We are in broad agreement with these recommendations, and would urge that the South African government be called upon to explain whether or not it intends to implement the recommendations of the Matthews Commission report, and particularly whether it intends to enact legislation to regulate and monitor the activities of the NCC to ensure they are legitimate to the aim pursued, necessary and proportionate as per international human rights law and standards. Up until now the government has done nothing to implement the report of the Matthews Commission. The South African government has stated that because the report was leaked they were unable to implement its findings. While the General Intelligence Laws Amendment Act has now been enacted, it has failed to regulate and hold the NCC accountable; mass surveillance has thus continued to be carried out by the NCC without objection or regulation.

*Blanket, indiscriminate retention of metadata*

27. As mentioned above, in terms of section 30(1)(b) of RICA, telecommunications service providers are required to store communications data for up to five years. 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.

28. In Digital Rights Ireland v Minister for Communications and Others,[19] the Grand Chamber of the Court of Justice of the European Union (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 CJEU 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, and 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".

29. Similar conclusions can be drawn with regards to the blanket, mandatory data retention regime imposed in RICA. Because of its untargeted and indiscriminate scope, section 30(1)(b) of RICA does not meet the requirements of necessity and proportionality, and would arguably be in breach both of domestic and international law.

*Role of the telecommunications service providers*

30. In addition to requiring the storage of communications data, RICA also requires that telecommunications service providers provide telecommunication services which have the capability of being intercepted (eg. by building in a backdoor for surveillance into their networks) (section 30 of RICA). Furthermore, RICA prohibits the disclosure of any information on the demands of interception (section 42 of RICA). As a result, telecommunications companies are barred from publishing information, including aggregated statistics, both of interception of communications and of metadata.

31. This veil of secrecy is concerning as there is a risk of abuse. Disclosures by the telecommunications companies could also provide an additional oversight mechanism in understanding the extent of the surveillance activities that are taking place.

*Intrusive methods and technological capabilities*

32. The technological capabilities of South African agencies to conduct surveillance are generally unknown, and the government refuses to respond to requests of more information under the policy that they cannot "disclose operational details and capabilities".[20] It has been reported, however, from the Hacking Team leaks that various South African government agencies, including the South African Revenue Services, have expressed interest in acquiring such technology.[21]

33. The use of such technology has serious implications on the rights to privacy and dignity, as well as political rights enshrined in the Constitution. As noted in the Matthews Commission report:[22]

> "Because intrusive methods infringe rights, they are unconstitutional unless they are employed in terms of law of general application. Legislation currently permits the intelligence services to intercept communication and enter and search premises. Other intrusive methods – such as infiltration of an organisation, physical and electronic surveillance, and recruitment of an informant – are not regulated by legislation and are thus unconstitutional."

34. Accordingly, the Matthews Commission report recommended that legislation should be introduced to govern the use of all intrusive measures by the intelligence services, which should be consistent with the

20 Mail & Guardian "How cops and crooks can 'grab' your cellphone - and you" (27 November 2015) (accessible at http://mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-cellphone-and-you).
21 MyBroadband "Here are the leaked e-mails from SARS spy unit to Hacking Team" (10 July 2015) (accessible at http://mybroadband.co.za/news/security/131780-here-are-the-leaked-e-mails-from-sars-spy-unit-to-hacking-team.html).
22 Matthews Commission report (p 17).

Constitutional Court jurisprudence on the right to privacy. From this, the Matthews Commission report extrapolated various proposed safeguards for the use of intrusive methods, including:[23]

- The use of intrusive measures should be limited to situations where there are reasonable grounds to believe that (a) a serious criminal offence has been, is being or is likely to be committed; (b) other investigative methods will not enable the intelligence services to obtain the necessary intelligence; and (c) the gathering of the intelligence is essential for the services to fulfil their functions as defined in law;

- Intrusive methods should only be permitted as a matter of last resort; and

- The intelligence services should delete within specified periods (a) private information about a person who is not the subject of investigation where the information is acquired incidentally through the use of intrusive methods; (b) private information about a targeted person that is unrelated to the commission or planning of a serious criminal offence; and (c) all information about a targeted person or organisation if the investigation yields no evidence of the commission or planning of a serious offence.

35. Importantly, the use of intrusive measures should always require the authorisation of a judge. Any underpinning legislation should prescribe the information that the applicant must present in writing and on oath or affirmation to the judge, and the application should provide sufficient detail to enable the judge to determine whether the circumstances warrant resort to intrusive measures. This would be in line with the recommendation of the United Nations Human Rights Committee, which stated that "[t]he State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization".

36. In our view, we submit that hacking can never be a legitimate component of state surveillance. However, should it take place, this should only be tolerated in circumstances that are very narrowly defined, with the strictest safeguards and under vigorous oversight.

*Use of "grabbers" or "IMSI catchers"*

37. 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. "IMSI catchers" are devices that mimic the operation of a cell tower device in order to entice a user's mobile phone to surrender personally identifiable data such as the SIM card number. In

23 Matthews Commission report (pp 17-18).

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.

38. RICA does not regulate this specific type of technology and it is not clear if the police apply for an 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 Parliamentary Joint Standing Committee on Intelligence (JSCI) 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."[24] We would urge that the government be called upon to indicate what steps, if any, have been taken in this regard, and what future steps it intends to take.

*Surveillance of journalists and civil society activists*

39. There are ongoing concerns of journalists and civil society activists being under surveillance, and being monitored and harassed by state authorities. Various of these are documented in R2K's publication "Big Brother exposed".[25] Moreover, we are aware of at least three prominent journalists – Mzilikazi wa Afrika and Stephan Hofstatter at the Sunday Times, and Sam Sole at amaBungane – who have received confirmed of interception orders being granted against them.[26] In the case relating to the Sunday Times journalists, a former crime intelligence official stands accused of giving false information to a judge to obtain a warrant under RICA.

40. These instances highlight the propensity of RICA to be abused by the authorities, and the urgent need for there to be both reform of the regulatory framework and better oversight of the security and intelligence services. We turn next to examine the issue of oversight in more detail.

***(b) The oversight mechanisms***

41. Although several oversight mechanisms are presently in place, these are neither sufficient nor properly implemented.

42. For instance, the Inspector General of Intelligence, this being the oversight body for the intelligence services, is a position that has stood vacant since March 2015, 18 months at the time of this submission. It remains unclear what steps are being taken to fill this vacancy, but certainly this has not been treated with the necessary level of urgency that it deserves. However, notwithstanding the failure to make the appointment, there

24 Accessible at http://www.parliament.gov.za/live/content.php?Item_ID=8495.
25 R2K "Big Brother exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements" (accessible at bigbrother.r2k.org.za).
26 See R2K "Statement – Sunday Times surveillance case in Pretoria court" (6 May 2016) (accessible at www.r2k.org.za/2016/05/05/6594/).

are additional concerns that the Inspector General of Intelligence is not sufficiently independent from the executive, lacks the necessary resources, and does not release its reports publicly. In order to properly perform its functions, the Office of the Inspector General of Intelligence should have an independent organisations status that allows it to be functionally, financially and administratively independent from those who it is mandated to oversee.

43. Some of the recommendations made in the Matthews Commission report with regard to the Office of the Inspector General of Intelligence included:[27]

    - The budget of the Office of the Inspector General of Intelligence should be substantially increased;

    - The Office of the Inspector General of Intelligence should have an independent organisational status, allowing it to receive and manage its budget independent of the National Intelligence Agency;

    - The Office of the Inspector General of Intelligence should have a higher public profile, including a website that provides contact details and described its functions, activities and findings.

44. Furthermore, South Africa's reports on interception orders are threadbare, and the information provided falls short of the reporting obligations needed for effective public oversight. It is impossible to discern from these reports, including the report of the designated judge, the extent to which surveillance is taking place in the country, and the effectiveness with which it is being monitored and safeguards are being implemented. The JSCI – tasked with exercising oversight over the intelligence agencies – moreover conducts its hearings in secret, and the public is deprived access to these deliberations, notwithstanding the keen public interest of the content of the discussions. A special schedule of rules governs sittings of the JSCI to ensure that its meetings are closed by default and may only be opened by special resolution of the JSCI's members. This is in keeping with the generalised trend of secrecy in the intelligence structures which the Matthews Commission criticised, noting that "[s]ecrecy should therefore be regarded as an exception which in every case demands a convincing justification."[28]

45. We therefore urge that the South African government be called upon to account for the pernicious veil of secrecy in terms of which the intelligence and security services operate, and the low level of implementation of the oversight mechanisms that ought to be in place. We note in this regard that the United Nations Human Rights Committee specifically recommended that "[t]he State party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies."

27 Matthews Commission report (pp 13-14).
28 Matthews Commission report (p 259).

### *(c) Data protection*

*The Information Regulator*

46. In September 2016, following significant delays, South Africa appointed its first Information Regulator. It remains unclear, however, when the office will be fully operationalised, or – importantly – when the conditions for the lawful processing of personal information under POPI will be brought into force. While appreciating that the South African institutions need adequate time and have competing priorities, POPI provides for a minimum one-year grace period for compliance. The longer the delay in fully implementing POPI, the longer it will be before members of the public have recourse to an independent mechanism to monitor and enforce their rights to data protection.

*SIM card registration*

47. The lack of implementation of the data protection law is of particular concern given the requirements imposed by RICA on telecommunications service providers to retain communication data and mandatory SIM card registration. SIM card registration, in particular, violates privacy in that it limits the ability of citizens to communicate anonymously. It also facilitates the tracking and monitoring of all users by law enforcement and intelligence agencies. Research shows that SIM card registration is not a useful measure to combat criminal activity, but actually fuels the growth of identity-related crime and black markets to those wishing to remain anonymous.[29]

*Closed-circuit television*

48. There appears to be growing investment by the government with regard to the use of closed-circuit television (CCTV), with the stated intention of it aiding in crime prevention.[30] However, there is a lack of a clear and consistent regulatory framework for the collection, use and storage of such footage. Through an access to information request, the Ekurhuleni Metropolitan Police Department (EMPD), for instance, made available its CCTV Street Surveillance Policy and the related codes of practice;[31] however, in general the policies are not readily accessible or available to the public. Although the EMPD's policy makes provision for members of the public to complain of privacy infringements, this is only relevant if the person knows of the existence of the CCTV to begin with. There is need for a clear and uniform regulatory framework in this regard that properly protects the right to privacy.

29 KP Donovan and AK Martin "The rise of African SIM registration: Mobility, identity, surveillance and resistance", Information Systems and Innovation Group Working Paper No. 186, London School of Economics and Political Science, London.

30 ENCA "CCTV helps fight crime in CPT" (13 October 2013) (accessible at https://www.enca.com/south-africa/cctv-helps-fight-crime-cpt).

31 Ekurhuleni Metropolitan Police Department "CCTV street surveillance policy" (undated) (accessible at http://protestinfo.org.za/download/policies/empd/PAIA-Disclosure-EMPD-CCTV-Surveillance-Policy-and-Code-of-Practice-26-August-2016.pdf).

*Biometrics*

49. Biometric information is increasingly being collected, most notably through the latest iteration of South African passports and identity cards. The Department of Home Affairs stored information in the Home Affairs National Identification System (HANIS); other government departments making use of biometrics include the police, transport, correctional services, justice and social welfare.[32] Through a joint initiative of the Department of Home Affairs and the South African Banking Risk Identification Centre (SABCRIC), called the Online Fingerprint Verification System, banks are able to access HANIS to verify the identity of prospective and current clients using their fingerprints.[33]

### *(d) Proposed legislation*

*Draft Cybercrime and Cybersecurity Bill*

50. In August 2015, the government published a draft Cybercrimes and Cybersecurity Bill. The 128-page draft 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. Particular concerns include:

- The lack of any defence for disclosure of information on public interest grounds and the overbroad definition of "national critical information infrastructure", which could further reduce transparency and access to information of government activities;

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

- The lack of user notification after a warrant has been issued, and the strict prohibition of disclosure of information, applicable also to communication service providers, which carries a penalty of conviction or a fine (section 39);

- The provisions which make service providers – even if somewhat indirectly – responsible for monitoring the behaviour of users (chapter 9), which could encourage service providers to interfere with users' rights to privacy.

32 IT Web "Biometrics commonplace in SA" (15 September 2014) (accessible at http://www.itweb.co.za/index.php?option=com_content&view=article&id=137674:Biometrics-commonplace-in-SA&catid=234).

33 IT Web "Biometrics save banks millions" (14 March 2016) (accessible at http://www.itweb.co.za/index.php?option=com_content&view=article&id=150678:Biometrics-saving-banks-millions&catid=355); see also: http://www.gov.za/services/verify-identity-online

*Protection of State Information Bill*

51. As mentioned above, POSIB was of key concern during the previous review. POSIB applies primarily to the state security services, although it further empowers the Minister of State Security to extend all classification provisions "to any organ of state or part thereof"; this has the potential to throw a blanket of secrecy over a wide array of government documents and activities, which would have a chilling effect on whistleblowers and journalists, and further impede the ability to hold government to account.

52. While President Zuma referred POSIB back to Parliament in September 2013, mainly to correct typographical errors, we have noted above that many of the substantive concerns have not as yet been addressed. POSIB has now been before President Zuma since November 2013. To our knowledge, the government has neither abandoned nor amended POSIB, notwithstanding the recommendations, all of which were noted by the government, from the previous review. This uncertainty is of deep concern, particularly given that, in the meantime, the apartheid-era Protection of Information Act 84 of 1982 (together with the Minimum Information Security Standards, a government policy adopted in 1996) is the applicable legislation for the classification of information.

53. Accordingly, we would urge that clarity be sought during the coming review, and that the state be requested to provide information both about its compliance with the previous recommendations as well as about its intentions for POSIB going forward.

## VI. Proposed recommendations

54. Based on these observations, PI and R2K propose that the following recommendations be made to the South African government:

- To take all necessary measures to ensure that its surveillance activities, both within and outside South Africa, conform to its obligations under domestic and international law; 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.

- To review all laws that impact the right to privacy, both existing and proposed, including RICA, the Cybercrime and Cybersecurity Bill and POSIB, to ensure that it is consistent with protections in the Constitution and reflect the highest threshold in accordance with international law and best practice.

- To ensure that RICA covers all forms of interception, retention and analysis of personal data for surveillance purposes, and that interception of communications (including communications data) by law enforcement and security services are only carried out on the basis of judicial authorisation.

- To provide that the person whose communications are being intercepted is informed about the interception order, unless failing to do so would seriously jeopardise the purpose for which the interception is authorised.

- To require that a person must be informed about applications for interception directions that are unsuccessful.

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

- To develop a legislative framework for the activities and mandate of the NCC in a way that is compliant with the Constitution and international law.

- To end mass surveillance, and adequately and transparently regulate information sharing with intelligence partners.

- To publicly avow the surveillance technologies capacities of law enforcement and security services, to 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), and to ensure that

the use of technologies such as "grabbers" or "IMSI catchers" are properly regulated and overseen by independent authorities to prevent arbitrary use.

- To ensure that state officials found guilty of illegal monitoring and surveillance are dismissed and prosecuted according to the law.

- To increase the transparency of its surveillance policy and speedily establish strong, independent oversight mechanisms of the intelligence services to prevent abuses and ensure that individuals have access to effective remedies.

- To establish a task team to consider the recommendations of the Matthews Commission report with a view to implementation of those recommendations, and to engage in a simultaneous process of consultation in this regard.

- To provide for oversight and transparency of the JSCI, including by permitting public access to the meetings revising the reporting practices to ensure that the reports provide meaningful information to the public.

- To ensure that the appointment of the Inspector General of Intelligence is dealt with as a matter of urgency, and that the Office of the Inspector General of Intelligence is structurally and functionally independent.

- To expedite the process of fully operationalising the Protection of Personal Information Act and the establishment of the Information Regulator.

- To develop clear, transparent and comprehensive policies regarding the collection, use, sharing and storage of CCTV footage and biometric information.