DECLARATION OF THE RIGHT 2 KNOW & PRIVACY INTERNATIONAL

27th UPR PRE-SESSION ON SOUTH AFRICA GENEVA, 07 APRIL 2017

1- Presentation of the Organisation

This statement is delivered on behalf of the Right to Know Campaign (R2K) and Privacy International (PI).

2- Plan of the Statement

The statement addresses and urges for a broadening of issues related to the protection and promotion of the right to privacy in South Africa. Four areas, which require consideration in this regard, are raised: (1) communication surveillance, (2) oversight mechanisms (3) data protection, and (4) proposed legislation.

3- Statement

I. The Protection of State Information Bill and expanding review on the right to privacy.

A. Follow-up to the first review

At the last review, little mention was made of the right to privacy in the National Report submitted by South Africa or the report of the Working Group, except as it related to the Protection of State Information Bill (POSIB). The gap in addressing this in previous reviews makes it urgent and appropriate for these matters to be given due regard in the upcoming review. As a fundamental human right, the right to privacy is enshrined in numerous international human rights instruments.

The most recent resolution adopted by the Human Rights Council for the first time recognises that any interference with the right to privacy needs to comply with the principles of legality, necessity and proportionality. It is therefore important to integrate this issue within the UPR to maintain the momentum at the UN to address the right to privacy.

B. New developments since the first review

The extent to which the state party has meaningfully taken on the recommendations on Protection of State Information Bill has been limited. Meanwhile, the have been developments in data collection technological capabilities and documented violations of fundamental privacy and related rights in South Africa

i.) Communications Surveillance

The legal framework for the interception of communications is set out in the 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA). However, there are a number of weaknesses which leave the law open to abuse. Right2Know has documented cases of surveillance of prominent journalists and human

rights activists and NGO's[1]. These cases and further research reveal three specific areas where RICA falls short – (i) the low burden of proof required for a warrant for lawful interception, (ii) the lack of user notification, and (iii) the retention of data imposed by RICA not meeting the necessity and proportionality test. In April 2016, The United Nations Human Rights Committee (UNHRC) in their observations on South Africa expressed concern about the relatively low threshold for conducting surveillance and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy.[2]

The National Communication Centre (NCC), the state's mass surveillance capacity and intrusive technologies[3] were found by the 2008 report of the Ministerial Review Commission on Intelligence titled "Intelligence in a constitutional democracy", to be happening outside any legal framework[4].

Recommendations*:*

- Ensure that RICA covers all forms of interception, retention and analysis of personal data for surveillance purposes.
- Develop a legislative framework for the activities and mandate of the NCC in a way that is compliant with the Constitution and international law.
- Take all measures necessary to ensure that South Africa's surveillance activities conform to its obligations under the Covenant, including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality, regardless of the nationality or location of the individuals whose communications are under surveillance.
- To prevent arbitrary use the surveillance technologies capacities of law enforcement and security services, publicly disclose and independently regulate the export of surveillance technologies by private companies based in South Africa,
- Establish a task team to consider the recommendations of the Matthews Commission report with a view to implementation of those recommendations.

ii.) Oversight Mechanisms

There are several oversight mechanisms in place, but neither sufficiently or properly implemented. We welcome the recent appointment of the Inspector General of Intelligence (IGI), where a non-appointment for two years led to a serious oversight gap and delay in complainants receiving recourse. However, even with the appointment, the Office of the IGI is not (i) sufficiently independent from the executive (ii) lacks resources and (iii) does not release its reports publically.

---

[1] Right2Know Handbook " Stop the Surveillance! Activist guide to Rica and state surveillance in SA" (accessible at http://www.r2k.org.za/wp-content/uploads/R2K-Handbook-Rica-Surveilance-2017.pdf)

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

[3] Known technologies are what is called "grabbers" or "IMSI catchers", used by the South African police, and recent investigation by South African journalists confirms use of hacking technology FinSpy – see in particular: Heidi Swart "Cyberspying: The Ghost in Your Machine" (accessible at https://www.dailymaverick.co.za/article/2017-02-21-cyberspying-the-ghost-in-your-machine/#.WOJ3yxJ96LI)

[4] 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).

The lack of transparent functioning of Parliament's Joint Standing Committee on Intelligence (JSCI), and reporting on interception orders fall short of the reporting obligations needed for effective public oversight. The United Nations Human Rights Committee specifically recommended that South Africa 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.

Recommendations:

- We urge that numerous complaints filed prior and during the absence of the IGI are finalised and released to complainants.
- Greater oversight and transparency, including by permitting public access to the meetings of the JSCI, revising the reporting practices to ensure that the reports provide meaningful information to the public, and the removal of the restriction clauses in RICA[5] which preclude telecommunications service providers public disclosing aggregated reports on the number of interception orders requested by the government.

iii.) Data Protection

We welcome the recent appointments at the Office of the Information Regulator (IR) as an important step in fully implementing the Protection of Personal Information Act (POPI), 2013. However the IR is yet to fully operationalise POPI, meaning members of the public are yet to have recourse to an independent mechanism to monitor and enforce their rights to data protection. This is crucial for protecting other rights - for example, the socio-economic rights of millions of social welfare beneficiaries in South Africa have been violated where biometric information was collected and traded (unlawfully), in many instances leading to illegal cash deductions[6]. Other areas which data protection is of concern, is in the current mandatory process of sim card registration under RICA and the increasing use of Closed Circuit Television by local government and private companies which, remains wholly unregulated.

Recommendations:

- To expedite the process of fully operationalising the Protection of Personal Information Act, including consultations with civil society in this regard.
- End mandatory sim card registrations.
- Develop clear, transparent and comprehensive policies regarding the collection, use, sharing and storage of CCTV footage, biometric information and other data held by the state

[5] (section 42 of RICA)

[6] See analysis in GroundUp on abuses of biometric data used to deprive poor of social grant money. Erin Tokelsen *"Deductions from social grants: how it all works"* http://www.groundup.org.za/article/deductions-social-grants-how-it-works/. In March 2017, Constitutional Court after an approach by civil society, Black Sash, ruled than personal data of grant beneficiaries should be protected, due to the grave and unlawful abuses - *Black Sash Trust v Minister of Social Development and Others (Freedom Under Law NPC Intervening)* (CCT48/17) [2017] ZACC 8 (17 March 2017)

iv.) Proposed Legislation

In August 2015, the government published a draft Cybercrimes and Cybersecurity Bill, and after consultation, has made numerous amendments. However, the latest draft tabled before Parliament this year still 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.

Finally, POSIB was of key concern during the previous review. To date, 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.

Recommendations:

- 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.
- We 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.

I thank you for your time.