15 February 2019

Submission to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: The Surveillance Industry and Human Rights

This submission is made jointly by ALT Advisory and the Right2Know Campaign, with specific reference to South Africa.

For further information, please contact:

ALT Advisory
c/o Avani Singh
avani@altadvisory.africa

Right2Know Campaign
c/o Murray Hunter
murray@r2k.org.za

INTRODUCTION

1. This submission is made jointly by ALT Advisory[1] and the Right2Know Campaign[2] (R2K), both based in South Africa, in response to the call for submissions regarding state and business responsibilities to limit the export and use of surveillance technologies to undermine fundamental rights. This submission focuses specifically on South Africa, including the applicable regulatory framework, key actors, and incidences that have occurred within the South African context. In line with the call for submissions, responses are provided to the following questions: A.1; A.2; B.1; and B.3. Furthermore, suggested resources of relevance are highlighted in this submission to provide further information and context.

QUESTION A.1: LAWS THAT REGULATE THE EXPORT, IMPORT AND USE OF SURVEILLANCE TECHNOLOGY

Regulation of the Interception of Communications and Provision of Communication-Related Information Act

2. The Regulation of the Interception of Communications and Provision of Communication-Related Information Act 70 of 2002[3] (RICA) is the primary legislation regarding the interception of communications. This includes establishing a system for law enforcement to apply for judicial authorisation for the interception of communications.

3. RICA has been subject to various criticisms, and is currently subject to an extensive constitutional challenge.[4] This includes that RICA is outdated and no longer fit for purpose; does not contain adequate safeguards; and constitutes a violation of constitutional rights, including the right to privacy. For a discussion of the shortcomings and concerns regarding RICA, please see the following resources:

[1] ALT Advisory is a legal consultancy that offers advisory, research, training and innovation services across four practice areas: (i) information rights; (ii) data privacy; (iii) emergent technology; and (iv) public law. ALT Advisory strives, in all instances, to act in the public interest, and has the protection and promotion of fundamental rights as its overarching aim. For more about ALT Advisory, please visit: https://altadvisory.africa/. ALT Advisory works in association with Power Singh Inc., a duly registered law firm, to offer litigation services to our clients within our practice areas.

[2] R2K is a movement centred on freedom of expression and access to information. It is a democratic, activist-driven campaign that strengthens and unites citizens to raise public awareness, mobilise communities and undertake research and targeted advocacy. One of R2K's core focus areas is 'Stop secrecy', in which it aims to ensure that security legislation and the conduct of security agencies – in particular the policing of gatherings – is aligned to the Constitution of the Republic of South Africa, 1996 (the Constitution) and underlying values. For more about R2K, please visit: https://www.r2k.org.za/.

[3] Accessible here: http://www.justice.gov.za/legislation/acts/2002-070.pdf.

[4] The court application is accessible here: https://amabhungane.org/advocacy/advocacy-amab-challenges-snooping-law/.

3.1. R2K, 'The surveillance state: Communications surveillance and privacy in South Africa', (March 2016).[5]
3.2. R2K and Media Policy & Democracy Project, 'New terrains of privacy in South Africa', (December 2016).[6]
3.3. R2K, 'Activist guide to RICA and state surveillance in South Africa', (April 2017).[7]
3.4. R2K, 'Spooked – Surveillance of journalists in South Africa', (June 2018).[8]
3.5. R2K and Privacy International, 'State of privacy: South Africa', (January 2019).[9]

4. Of particular relevance to the present call for submissions, we note the provisions of section 44–46 of RICA. Section 44(1)(a) provides that the Minister of Justice and Correctional Services must, by notice in the Government Gazette, "declare any electronic, electro-magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for purposes of the interception of communications, under the conditions or circumstances specified in the notice, to be listed equipment". In accordance with this section, on 29 December 2009 the Minister published the contemplated list under Government Notice No. R. 1263.[10]

5. Section 45(1) provides further that, subject to sub-section (2) and section 46 of RICA, no person may manufacture, assemble, possess, sell, purchase or advertise any listed equipment. Section 45(1) does not apply to any telecommunication service provider, law enforcement agency or other person who undertakes these activities in respect of listed equipment under the authority of a certificate of exemption issued for that purpose by the Minister under section 46 of RICA.[11] Section 46, in turn, details the conditions under which the Minister may grant such an exemption, including if such an exemption is in the public interest,[12] or if special circumstances exist which justify the exemption.[13]

[5] Accessible here: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf.

[6] Accessible here: https://www.r2k.org.za/privacy-monograph.

[7] Accessible here: https://r2k.org.za/rica-guide.

[8] Accessible here: https://www.r2k.org.za/spooked.

[9] Accessible here: https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa.

[10] Accessible here: http://www.justice.gov.za/legislation/regulations/r2006/REGULATION%20OF%20INTERCEPTION%20OF%20COMMUNICATIONS%20AND%20PROVISION%20O.pdf.

[11] Section 45(2) of RICA.

[12] Section 46(2)(c) of RICA.

[13] Section 46(2)(d) of RICA.

National Conventional Arms Control Act

6. The National Conventional Arms Control Act 41 of 2002[14] (NCACA), as amended by the National Conventional Arms Control Amendment Act 73 of 2008,[15] is intended to be the domestic legislation that gives effect to South Africa's commit under the Wassenaar Arrangement. The NCACA incorporated the 2003 Wassenaar Arrangement at the time of enactment, even though South Africa only formally became a member of the Wassenaar Arrangement in 2006.[16] However, as with RICA, the NCACA has similarly become outdated. Of particular concern, the NCACA does not contain the updated List of Dual-Use Goods and Technologies and Munitions List of the Wassenaar Arrangement that broadened the list in respect of surveillance technology; accordingly, it is apparent that the NCACA does not provide an effective control in respect of the trade in surveillance equipment.

7. The NCACA establishes the National Conventional Arms Control Committee (referred to as 'the Committee' or 'NCACC'),[17] whose functions include authorising or refusing the issue of any permit in terms of the NCACA, ensuring that the conditions under which a permit is issued are complied with, and keeping a register of permits issued and the persons involved in the trade of controlled items.[18] The Committee is required to report annually to the Cabinet and Parliament of South Africa on all transfers of controlled items concluded during the preceding quarter.[19] Concerns have been raised that the Committee has not been responsive to requests for information, and has remained more focused on conventional arms with inadequate attention being paid to surveillance equipment.

---

[14] Accessible here: https://www.gov.za/documents/national-conventional-arms-control-act.

[15] Accessible here: https://www.gov.za/documents/national-conventional-arms-control-amendment-act. The objects of the NCACA are as follows:

> "To establish the National Conventional Arms Control Committee; to ensure compliance with the policy of the Government in respect of arms control; to ensure the implementation of a legitimate, effective and transparent control process; to foster national and international confidence in the control procedures; to provide for an Inspectorate to ensure compliance with the provisions of this Act; to provide for guidelines and criteria to be used when assessing applications for permits made in terms of this Act; to ensure adherence to international treaties and agreements; to ensure proper accountability in the trade in controlled items; to provide for matters connected with the work and conduct of the Committee and its secretariat; and to provide for matters connected therewith."

[16] Department of International Relations and Cooperation, 'Wassenaar Arrangement', accessible here: http://www.dirco.gov.za/foreign/Multilateral/inter/wasse.htm.

[17] Section 2 of the NCACA. The NCACA further establishes a Secretariat to assist in the performance of the functions of the Committee (section 8 of the NCACA); and an Inspectorate – separate from the Secretariat – to ensure compliance with the NCACA and the internal regulatory processes of the Committee (section 9 of the NCACA).

[18] Section 4 of the NCACA.

[19] Section 23 of the NCACA. Section 23 further requires that the Committee report periodically to the Secretary-General of the United Nations and other applicable international treaty bodies.

8. In terms of section 13 of NCACA, no person may trade in or possess the controlled items referred to in the Conventional Arms Control Regulations, 2004[20] (CACR), unless that person is registered with the Secretariat, and in possession of a permit authorised by the Committee and issued by the Secretariat. Although the CACR makes some reference to surveillance technology,[21] this does not include the more recent amendments to the scope of applicable surveillance technology, such as IP-based surveillance, equipment interference and grabbers. Section 14(1) of the NCACA provides that any person who wishes to obtain a permit contemplated in section 13 of the NCACA must apply to the Committee in the prescribed manner.

9. Notably, section 15 of the NCACA sets out the guiding principles and criteria that the Committee must apply when assessing an application for a permit:

> "When considering applications contemplated in section 14 the Committee must –
> (a) assess each application on a case-by-case basis;
> (b) safeguard the national security interests of the Republic and those of its allies;
> (c) **avoid contributing to internal repression, including the systematic violation or suppression of human rights and fundamental freedoms**;
> (d) **avoid transfers of controlled items to governments that systematically violate or suppress human rights and fundamental freedoms**;
> (e) **avoid transfers of controlled items that are likely to contribute to the escalation of regional military conflicts, endanger peace by introducing destabilising military capabilities into a region or otherwise contribute to regional instability**;
> (f) **adhere to international law, norms and practices and the international obligations and commitments of the Republic, including United Nations Security Council arms embargoes**;
> (g) take account of calls for reduced military expenditure in the interests of development and human security;
> (h) avoid contributing to terrorism and crime;
> (i) **consider the conventional arms control system of the recipient country and its record of compliance with end-user certificate undertakings, and avoid the export of conventional arms to a government that has violated an end-user certificate undertaking**;

[20] Accessible here: https://www.gov.za/sites/default/files/gcis_document/201409/26372rg7963gon634.pdf.

[21] This includes, for instance, items ML5(b) and ML11(c) of the Munitions List.

(j) take into account the inherent right of individual and collective self-defence of all sovereign countries in terms of the United Nations Charter; and

(k) **avoid the export of controlled items that may be used for purposes other than the legitimate defence and security needs of the government of the country of import.**"

10. It is apparent from the legal framework that the Committee is required to take into account, amongst other things, the human rights impact that the grant of the permit may have. Section 16 of the NCACA goes further in seeking to ensure accountability, including in respect of requiring stipulated undertakings to be reflected in the end-user certificate.[22] Further in respect of end-user certificates, section 17 of the NCACA provides that, subject to section 16, where controlled items are exported, a person authorised by the government of the country to which the controlled items are exported must issue an end-user certificate, including the details of the end-user and an undertaking that the controlled items will not be transferred or re-exported to any other person or country without the authorisation of the South African government.[23]

Annual report of the NCACC

11. On 7 June 2018, the NCACC presented its annual reports for 2016 and 2017 to the Joint Standing Committee on Defence. The report contained various information that provides insight into the workings and considerations applied by the Committee. For details regarding the report of the Committee, please see the following resources:

    11.1. NCACC, '2017 National Conventional Arms Control Committee (NCACC) Annual Report (January – December 2017)', (March 2018).[24]

[22] Section 16 provides for the following:

- Where controlled items are exported and ownership is transferred, the Committee must satisfy itself that the government of the country of import has given an undertaking, reflected in an end-user certificate, that the controlled items in question will not be transferred, re-sold or re-exported to any other country without the prior approval of the Committee, acting on behalf of the Government of South of Africa.
- Where controlled items are exported and ownership is transferred, the Committee must obtain a letter from the government of the country of import stating that controlled items in question are intended for demonstration or evaluation purposes and whether they will be returned. Alternatively, the Committee must obtain a letter from the applicant stating that the arms in question are being exported for repair or integration only, and will be returned.
- Where there is an undertaking that the controlled items in question are to be returned, the Committee must satisfy itself that the controlled items have been returned in accordance with the undertaking.
- Where the controlled items in question have been expended during demonstration, the Committee must obtain a certificate from the government of the country of import verifying that fact.

[23] Section 6 of the CACR further requires that an end-user certificate must contain a government-issued certificate that the end-user certificate is a legal and valid document that has been properly sealed and signed, unless the end-user certificate contains an apostille stamp.

[24] Accessible here: https://pmg.org.za/committee-meeting/26606/.

11.2. NCACC, 'The 2016 and 2017 NCACC Annual Reports presentation to the Joint Standing Committee on Defence', (March 2018).[25]

11.3. Parliamentary Monitoring Group, 'NCACC Annual Reports: 2016 & 2017, with Ministers of Defence and Energy; Deployment resources funding; Mozambique Channel piracy; Department of Military Veterans status', (June 2018).[26]

12. Discussions regarding the human rights considerations in the grant of permits are apparent from the meeting report (listed at paragraph 11.3 above).[27] It should be noted that lack of transparency has hampered efforts to map the sale of surveillance technology to or from South Africa.[28] For example, Danish state records show the sale of BAE mass surveillance software to South Africa and of a UK-made IMSI catcher in 2014, but the NCACC's reports do not.[29] Separately, the NCACC failed to say whether it approved the export of VASTech surveillance technology to Libya.[30]

---

[25] Accessible here: https://pmg.org.za/files/180607NCACC.pptx.

[26] Accessible here: https://pmg.org.za/committee-meeting/26606/.

[27] For instance, the following discussion is minuted in the report:

> "Mr S Esau (DA) asked if the reasons could be provided as to why permits were denied.
>
> Minister Mapisa-Nqakula said that the DoD was very careful as to who it granted export permits to.
>
> **Mr Esau referred to areas where weapons had been supplied by South Africa, and asked if it had been checked if any human rights abuses had taken place in these countries, and if yes, how had South Africa responded to this.**
>
> Mr Esau said that the Islamic State of Iraq and Syria (ISIS) itself had been armed and trained by the USA and the USA has its own veto rights and also overrides any Security Council. He asked what position South Africa took with regard to the arming of rebels and forces and undermining other forces and governments with regards to the US. **Further, he noted that in Myanmar, there are serious human rights abuses taking place and they imported weapons from South Africa that would assist in the launching of missiles. He wanted a response on the human rights abuses taking place and if these have been properly considered.**
>
> Minister Radebe said the position was **guided by the parameters set by the United Nations Security Council on whether there were sanctions against particular countries especially if there were arms embargoes. Guidance was also provided by information about conflicts and South Africa's own national interest in the country. The track record of certain countries in terms of their human rights situation was also looked at, including the issue of regional dynamics in particular areas like whether there was stability or not. The other area of concern - which was a factor for consideration - was the possibilities of diversion, where arms would be exported and then the country in question would divert the arms to areas that were sanctioned. In all the instances mentioned, arms would be denied. The NCACC would also look at whether countries were signatories to the Non-Proliferation Treaty or not. The Secret Service also provided information that helped when assessing whether arms could be provided to certain countries.**
>
> Minister Mapisa-Nqakula said that if there was a record of a country having committed human rights violations then permits would be denied. If there was conflict in a particular country then permits would be denied. The two countries where permits had been denied recently were Taiwan and Ukraine."
>
> (Emphasis added.)

[28] Jane Duncan, 'Stopping the spies: Constructing and resisting the surveillance state in South Africa', (2018), Wits University Press, p 117.

[29] *Id*., p 121.

[30] See Privacy International, 'Privacy International files complaint with South African export control body regarding export of surveillance tech to Libya', (22 October 2013), accessible here: https://privacyinternational.org/blog/1521/privacy-international-files-complaint-south-african-export-control-body-regarding-export.

QUESTION A.2: REMEDIES AVAILABLE IN THE EVENT OF ILLICIT EXPORT OR USE OF PRIVATE SURVEILLANCE TECHNOLOGY

RICA

13. The offences and penalties under RICA are set out in Chapter 9, specifically sections 49–57 of RICA. In respect of the prohibition on the manufacture, possession and advertising of listed equipment (as contained in section 45(1) of RICA), section 51 provides that any person who contravenes the section is guilty of an offence and liable on conviction to a fine not exceeding R2 million (ZAR) or to imprisonment for a period not exceeding ten years.[31]

NCACA

14. Section 14(3) of the NCACA empowers the Committee to take any of the following measures:

    14.1. Cancel or suspend the permit if any condition of the permit has not been or is not being complied with.
    14.2. Cancel the permit if the person who has been issued the permit is convicted of an offence in terms of the NCACA.
    14.3. Cancel, amend or suspend the permit if it is in the interest of the protection of the security of South Africa.
    14.4. Cancel, amend or suspend the permit if it is in the interest of maintaining and promoting international peace, or avoiding repression and terrorism.

15. Section 24(1)(a)–(j) sets out the offences in terms of the NCACA. Of particular relevance, a person is guilty of an offence if the person engages in trade in contravention of section 13 of the NCACA,[32] or fails to comply with or contravenes any specification or condition stated in a permit or end-user certificate.[33] Any person convicted of the abovementioned offences is liable to a fine or imprisonment not exceeding 25 years, or both.[34] A court may further order seizure of any goods, article, material or substance in respect of which the offence was committed.[35]

---

[31] See, for example, *Okundu v S* [2016] ZAECGHC 131 (22 November 2016), paras 15-21, accessible here: http://www.saflii.org/za/cases/ZAECGHC/2016/131.html. The appellant in the matter had been convicted of possessing listed equipment in contravention of section 45 of RICA. In the alternative to section 45(1) of RICA, the appellant was charged with a similar prohibition contained in section 86(3) of the Electronic Communications and Transactions Act 25 of 2002.

[32] Section 14(1)(a) of the NCACA.

[33] Section 14(1)(b) of the NCACA.

[34] Section 24(2) of the NCACA.

[35] Section 24(3) of the NCACA.

16. Moreover, section 24A(1) of the NCACA provides that, notwithstanding anything to the contrary, the Committee may impose an administrative fine on any person who is alleged to have committed an offence in terms of section 24(1)(b)–(j) of the NCACA, or who fails to keep the prescribed records, minutes registers and financial statements as required by the regulations.

QUESTION B.1: STATE USE OF PRIVATE SURVEILLANCE TECHNOLOGY AGAINST INDIVIDUALS OR CIVIL SOCIETY ORGANISATIONS

17. There have been various reports of individuals in South Africa – including activists, whistle-blowers and journalists – being subject to surveillance. R2K has been engaged in documenting such case studies. For details of these reports, please see the following resources:

    17.1. R2K, 'Big Brother exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements' (April 2015).[36]
    17.2. R2K, 'Spooked - Surveillance of journalists in South Africa' (June 2018).[37] The factual basis for the constitutional challenge to RICA, referred to above, is premised on the surveillance of investigative journalist Sam Sole, whose case study is one of the ten highlighted in this report.

18. It is also a matter of record that the South African Police Services (SAPS), and possibly other security agencies, have access to IMSI catchers or 'grabbers', the use of which appears not to be subject to judicial oversight.[38] While the employment of such devices by SAPS is best documented,[39] in 2018, a local newspaper reported that the Defence Intelligence Division had allegedly procured a mobile surveillance van from a Chinese supplier, which may have included grabber technology.[40] Other instances of the procurement and use of grabbers had been previously reported during November 2015.[41]

[36] Accessible here: https://www.r2k.org.za/bigbrother.

[37] Accessible here: https://www.r2k.org.za/spooked.

[38] See, for example, Designated Judge, 'Annual report on interception of private communications, period 2014/2015' (15 October 2015), accessible here: https://www.parliament.gov.za/storage/app/media/Docs/atc/616481_1.pdf. Following public reports that the devices may be used without judicial authorisation, the Designated Judge reported to Parliament that: "Under [RICA], the devices utilised by various Law Enforcement Agencies do not require the Designated Judge's authorisation. Once authorisation has been obtained to install a listening device, the nature of the device does not require approval of the Designated judge."

[39] See Media Policy & Democracy Project, 'Communications surveillance by the South African Intelligence Services', (February 2016), accessible here: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf.

[40] Rapport, 'Weermag kry spioenasiebus', (26 August 2018), accessible here: https://www.netwerk24.com/Nuus/Algemeen/weermag-kry-spioenasiebus-20180826.

[41] Mail & Guardian, 'How cops and crooks can 'grab' your cellphone – and you', (27 November 2015), accessible here: https://mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-cellphone-and-you.

19. There have been further unconfirmed reports of spyware being used by the state or private actors in South Africa. This includes a report from Citizen Lab of the presence of FinFisher on South African servers in 2013,[42] and Pegasus software in 2018.[43]

20. Following the Hacking Team leaks, the leaked data revealed that several different government departments in South Africa had expressed interest in the firm's surveillance technology.[44] However, the leaked data does not provide any indication of whether any transactions were concluded between the government departments and the Hacking Team.

21. It should be noted further that in June 2015, the Investigatory Powers Tribunal of the United Kingdom made a determination that communications from an email address associated with the Legal Resources Centre – the largest public interest law firms in South Africa – were intercepted and selected for examination by Britain's Government Communications Headquarters (GCHQ).[45]

QUESTION B.3: EXTENT TO WHICH PRIVATE SURVEILLANCE COMPANIES OFFER SERVICES TO STATES AND OTHER ACTORS TO DEPLOY THEIR TECHNOLOGIES

22. A number of South African companies are known to provide surveillance services or software, although the extent of their operations are unknown. As has previously been noted by R2K, this includes:

    22.1. VASTech SA (Pty) Limited, a South African company that designs and sells hardware and software capable of mass surveillance. As previously noted by R2K, while VASTech's full client list is unknown, in 2011 it emerged that VASTech had sold its technology to the Gadaffi regime in Libya. In 2013, research by Privacy International revealed that the South African government had given public funding to VASTech to develop its products, prompting speculation that South Africa may also be a VASTech client. VASTech has also previously been active in Syria.[46]

---

[42] Citizen Lab, 'For their eyes only', (April 2013), accessible here: https://citizenlab.org/2013/04/for-their-eyes-only-2/.

[43] Citizen Lab, 'Hide and seek', (September 2018), accessible here: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[44] IT Web, 'Hacking Team failed to crack SA', (14 July 2015), accessible here: https://www.itweb.co.za/content/nG98YdqLKbJMX2PD.

[45] *American Civil Liberties Union and Others v The Government Communications Headquarters and Others* [2015] UKIPTrib 13_77-H_2 (22 June 2015), paras 11 and 15, accessible here: https://www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf. According to the ruling, while the interception and selection was lawful and proportionate, the procedure laid down by GCHQ's internal policies for selection of the communications for examination was in error not followed in this case.

[46] R2K and Privacy International, above n 9.

22.2. iSolv, a South African company that provides products and services related to "lawful interception" and "targeted monitoring". One product, called CS Intercept, is advertised on the iSolv website as "a versatile, purpose built appliance for the lawful interception and filtering of telecommunication networks". There is also speculation that iSolv has some operational responsibilities at the Office for Interception Centres (OIC), and that the OIC is a client of iSolv.[47]

22.3. A former member of the Crime Intelligence Division of SAPS currently faces criminal charges, which allege that he used state interception resources for private intelligence purposes, and illegally imported and sold an IMSI catcher manufactured by Forensic Telecommunications Services Ltd (FTS) in the United Kingdom.[48]

CONCLUDING REMARKS

23. The surveillance landscape in South Africa – including in respect of the export, import and use of surveillance equipment – is complex and rife with challenges, both in terms of the legal frameworks and the implementation thereof. As set out above, RICA has been subject to ongoing criticism, and is now being directly challenged in court as being unconstitutional. While the NCACA does contain provisions requiring the NCACC to consider potential human rights violations prior to the granting of a permit, there are concerns that it is outdated and does not constitute an effective control of the trade in surveillance equipment. There are further concerns in respect of the level of enforcement, the delayed reporting by the NCACC, and the extent to which end-user certificates are verified.

24. In terms of the private sector, there is little known about the policies of the key actors in South Africa or any stated commitment to human rights. It appears from reports that there is active engagement between the government and the private sector regarding surveillance technology and services, but there is a lack of transparency regarding these engagements or any subsequent procurement that the state may conclude. Both the public and private sector actors should be required to ensure that they are not facilitating human rights infringements either domestically or abroad, and should be held accountable for any failure thereof.

25. Thank you for the opportunity to provide this submission. Please do not hesitate to contact us should you have any questions or require any further information.

[Ends.]

[47] *Id*.

[48] *State v Scheepers*, Belville Specialised Commercial Crimes Court, Case No. SSH7/38/16.