Photo: Graham van de Ruit
Graphic design: Wilna Combrinck

POLICY BRIEF

THE FUTURE OF BULK INTERCEPTION OF DIGITAL COMMUNICATION

Issues and policy options

JANE DUNCAN, JANUARY 2024

INTEL WATCH

TABLE OF CONTENTS

This policy brief was prepared by Jane Duncan, Professor of Digital Society, School of Social and Political Sciences, University of Glasgow. It is an output of an eight-country surveillance research project titled 'Public oversight of digital surveillance for intelligence purposes: a comparative case study analysis of oversight practices in southern Africa'. This research project is supported by the British Academy's Global Professorship Programme, through the School of Social and Political Sciences at the University of Glasgow, and Jane Duncan is the holder of the Global Professorship. The policy brief also draws on the work, produced over several years, of the Media Policy and Democracy Project, which was a joint project of the Department of Communication and Media, University of Johannesburg and the Department of Communication Science, University of South Africa.

EXECUTIVE SUMMARY

This policy brief examines the issues around bulk interception of digital electronic signals, especially communication signals, in South Africa and sets out the policy options for improving regulation and oversight of these incredibly powerful spying capabilities. In 2021, the South African Constitutional Court required the State Security Agency to halt the bulk surveillance activities of its signals intelligence agency, the National Communications Centre, as it found that bulk surveillance is unlawful and unconstitutional in the absence of a law authorising this practice. Parliament is now required to pass a law to address this gap. The Presidency has responded by including clauses in the General Intelligence Laws Amendment Bill, providing for the establishment of the Centre, and its powers and functions. This Presidency intended for the Bill is to address a longstanding controversy around the lack of regulation of this Centre, which the Agency is meant to use to conduct surveillance outside the borders of South Africa to protect the country from national security threats.

Despite the Agency having claimed that it benchmarked the Bill internationally, its benchmarking is highly selective and shows little appreciation of the issues around bulk interception as a form of surveillance. There have been major disagreements internationally on whether bulk surveillance, including bulk interception, should ever be permissible in democracies. Parliament needs to decide whether it wants the Agency to have these powers or not. If it decides that it does, then there are reform options. Other countries have improved regulation and oversight of these capabilities by limiting them in various ways, and some of these are set out in this policy brief. However, largely the Presidency has not considered these options. These gaps mean that the Bill falls short of the Court's requirement to provide more detail on the circumstances or duration of surveillance, and how the information obtained from the surveillance will be treated. If Parliament decides to deny the Agency the right to practice bulk surveillance because it believes that the country's spies should not enjoy such invasive spying powers, then any foreign-focussed surveillance and cybersecurity functions would need to be assigned to other entities.

INTRODUCTION

In 2023, the Minister in the South African Presidency introduced a draft law, the General Intelligence Laws Amendment Bill, to make changes to the country's existing intelligence laws. They intended to achieve several objectives, including changing the institutional architecture of civilian intelligence by dis-establishing the State Security Agency. It would then revert to the old model that existed before 2009 of having separate foreign and domestic intelligence services with their own directors general.

The Presidency is also using the Bill to provide a legal basis for the Agency's Centre responsible for bulk surveillance, the National Communications Centre. It is doing so to respond to a Constitutional Court ruling that declared the operations of the Centre unconstitutional as it did not have a founding law spelling out its functions and limiting its powers.

The government established the Centre to collect intelligence from foreign digital electronic signals, including communication signals. It is the most powerful digital surveillance tool available to the South African government, through the Agency, which can be used to put large numbers of people, and even whole populations, under surveillance.

If rogue elements in the government misuse this capability (and they have in the past, as explained below), then it can have a massive, negative impact on peoples' right to privacy, freedom of expression and association and other rights.

Even if they didn't misuse it, the idea of bulk surveillance is problematic as it violates peoples' right to privacy on a massive scale.

This policy brief examines what the Bill says about the Centre, the approach the Presidency has taken to address the problems raised by the Constitutional Court, and the various policy options regarding bulk surveillance. This brief should be of use to civil society, social movements, lawyers, and journalists who may want to know more about the Bill ahead of the Parliamentary hearings, and the members of Parliament who will be considering the Bill. Its intention is to present the key issues and policy options around bulk surveillance in a useful, non-academic form to inform decision-making around the Bill.

BULK SURVEILLANCE: BACKGROUND AND CONTROVERSIES

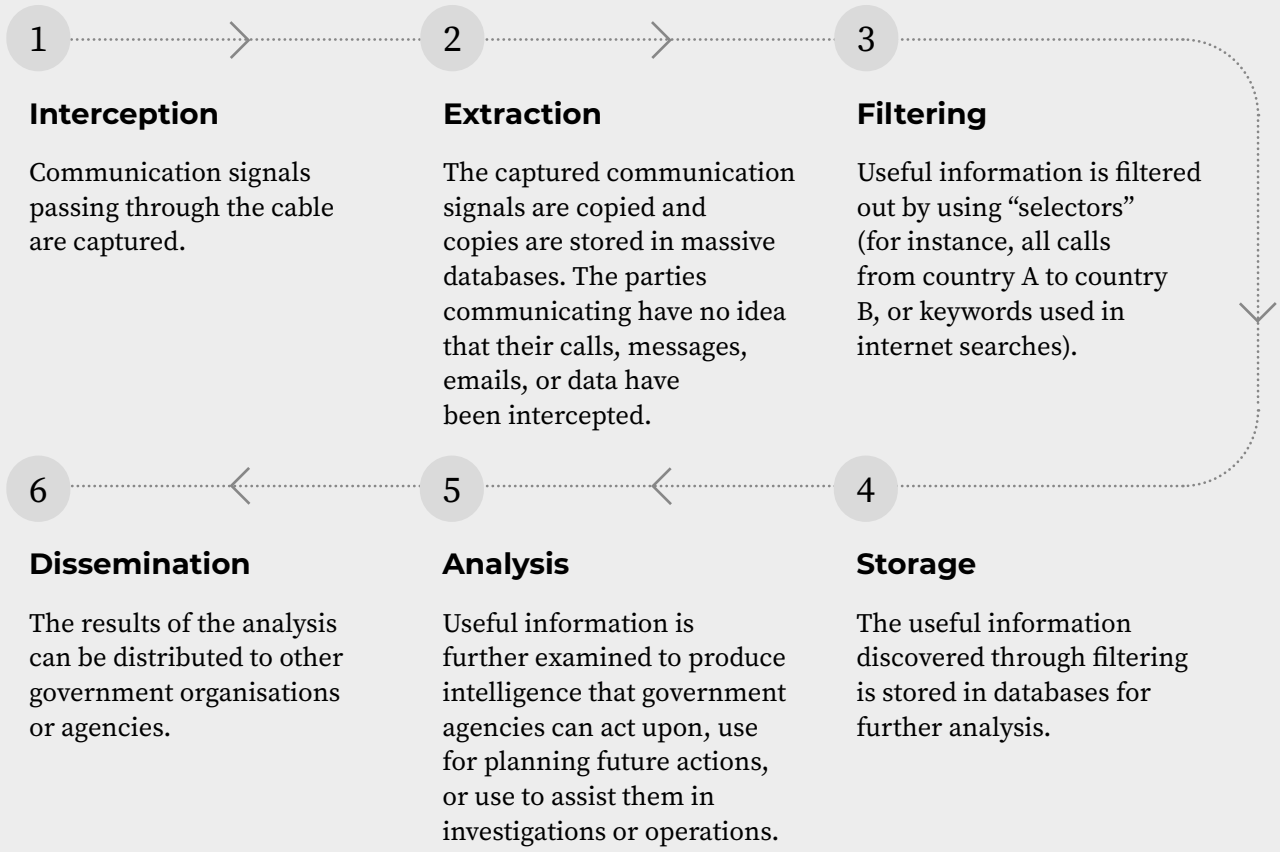
Bulk surveillance can take many forms, such as the bulk interception of communications, the bulk retention of data, and bulk hacking. However, it is unclear whether the Centre undertakes all these forms of bulk surveillance. This policy brief will focus mainly on bulk interception, its regulation and its oversight, as it is clear from the amaBhungane case that at the very least, the Centre will be undertaking this form of surveillance. While a great deal of secrecy surrounds bulk surveillance of foreign signals for intelligence purposes, other countries are known to have similar Centres and capabilities. In the case of bulk interception, they use artificial intelligence and keyword search terms (or selectors) to trawl through masses of communication signals for signs of emerging national security threats (Privacy International 2016). The most powerful known surveillance alliance consists of five countries that pool their signals intelligence capabilities – the United Kingdom, or UK, the United States, or US, Canada, Australia, and New Zealand/ Aotearoa – and is known as the Five Eyes alliance (Farrell 2013). They have also entered into looser alliances and cooperation agreements with other countries to provide them with intelligence. However, these countries claim to use these capabilities to collect foreign intelligence only – a claim which has been proved to be false – and particularly for strategic intelligence where they identify longer-term threats to national security on a forward-looking basis (European Commission for Democracy Through Law 2015). However, due to the nature of internet traffic and how it flows across the globe, it is technically impossible to separate out local from foreign communications (10 Human Rights Organisations 2015).

The rationale intelligence agencies use for collecting foreign intelligence on an untargeted basis is that they do not know what they do not know about looming threats outside their borders, as they lack the investigatory powers that they have domestically. They argue that this problem places them at a major disadvantage in detecting such threats before it is too late. They argue that the possibility of unknown threats means that they need to use the few investigatory methods at their disposal to do so, even if it means collecting huge volumes of information and violating the privacy of large numbers of people, and even whole populations (The United Kingdom 2019).

HOW BULK INTERCEPTION WORKS

Governments conduct bulk interception by tapping high capacity fibre optic cables that carry the world's internet communications between countries. Even if two people in the same country communicate with each other via the internet (for instance, through social media messaging apps), their conversation could still be captured by bulk interception. This is because all communication signals usually cross borders due to the structure of the internet. To boot, foreign governments could be given access to intercepted communications at any stage of a particular country's bulk interception process, since countries can have intelligence-sharing agreements.

The TAT-14, for example, is a transatlantic cable system with a transmission capacity of approximately 34 petabytes per day. To put that number into perspective, 1 petabyte is roughly equivalent to 2 billion cat photos.



Source: Adapted from flow diagram, "How bulk interception works", courtesy of Privacy International.

The problem is that it is practically impossible to regulate these spying powers in ways that respect basic rights and freedoms, such as privacy.

This is because governments set these centres up to collect communications indiscriminately. In other words, they treat everyone outside the country as a potential person of interest, threat actor or criminal suspect. In doing so, these governments adopt a differential approach towards protecting privacy, where those inside their borders are more deserving of privacy than those outside.

In 2013, former National Security Agency contractor, Edward Snowden, leaked classified documents to journalists showing how intelligence agencies conducting bulk surveillance in the US and UK had been abused to spy on citizens that could not reasonably be suspected of being national security threats. Snowden also leaked information showing how the Five Eyes alliance used their bulk surveillance capabilities for reasons that extended far beyond global security.

The documents leaked by Snowden detailed how the alliance spied on African businesspeople, politicians and social movements to gain trade advantages, secure their economic interests on the continent and marginalise African countries even further from the global economy.

In the case of South Africa, the UK government spied on the country's senior officials and politicians during the 2009 G20 summit, as well as technology specialists working for the mobile network operator MTN (De Wet 2013; Staff Writer 2016).

In response to huge public outrage at this massive, unregulated state spying, civil society has pushed the Five Eyes governments to tighten up how these capabilities are regulated.

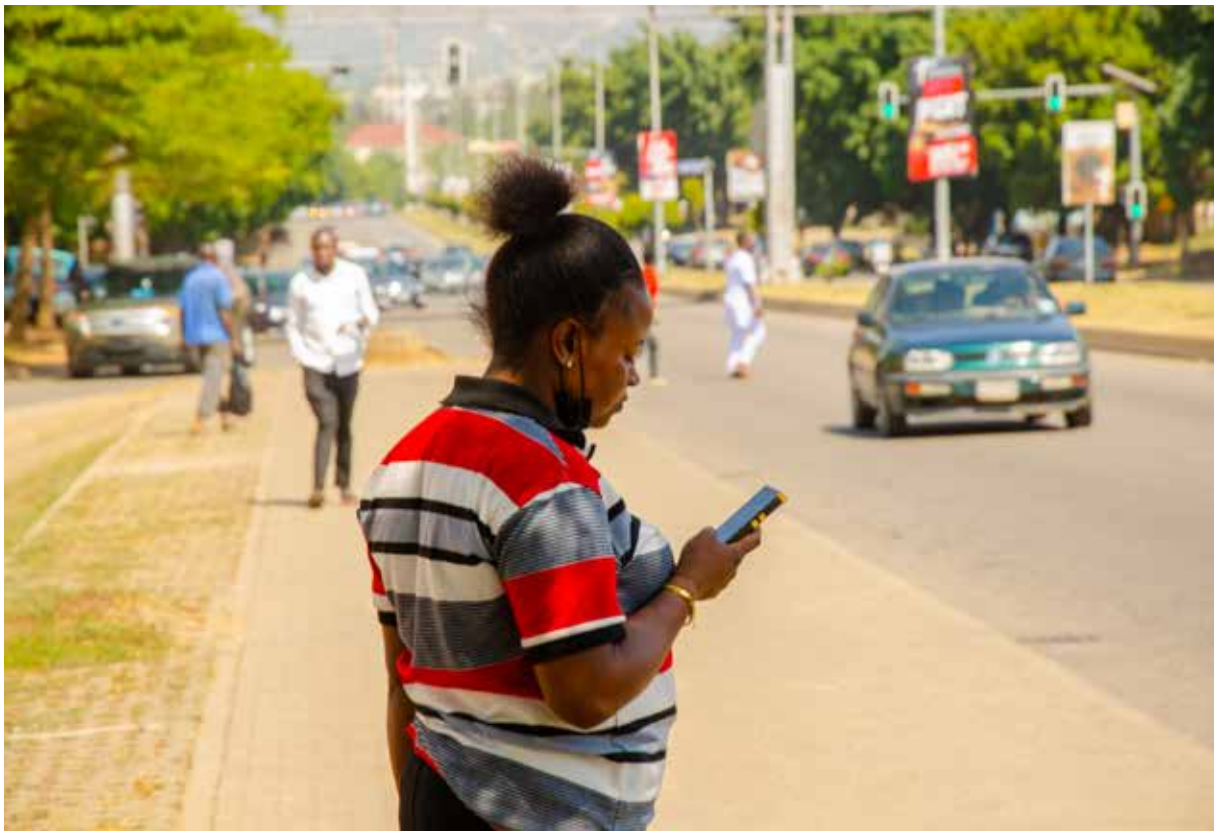


Photo: Ichie Opara

In South Africa, the Centre's role is to provide the government with strategic intelligence derived from foreign signals collection. However, since its establishment, the activities of the Centre have been shrouded in secrecy. From what little is known about it, the Centre collects huge amounts of personal information from electronic networks, including personal communication, to identify potential threats to national security (State Security Agency 2017). The Agency does so on an untargeted basis, which means that it does not need to suspect anyone of a crime or being a threat to national security to scoop this information up in the Centre's dragnet. This means that the dragnet extends to the communications of the innocent and guilty alike.

An affidavit provided to the Court by the Agency's then-Director General, Arthur Fraser, shed more light on how the Centre functions (State Security Agency 2017). The Centre uses what he refers to as an internationally accepted method of monitoring transnational signals to screen them for certain cue words of key phrases suggesting that South Africa may be facing national security threats. The Centre does this by tapping into and recording transnational signals, including from undersea fibre optic cables, suggesting that, at the very least, the Centre undertakes bulk interception. Its capabilities to hack or store bulk datasets are not known publicly.

The Centre operates very differently from the surveillance undertaken in terms of South Africa's main communication surveillance law, Rica (the Regulation of Interception of Communications and Provision of Communication-related Information Act). The Office for Interception Centres undertakes this surveillance on a targeted basis. In other words, individuals are targeted for surveillance, but only if authorities have a reasonable suspicion of serious crimes being planned or committed. In addition, tarteted surveillance as an investigative method can only be used as a last resort when other investigative methods have proven ineffective.

The SSA's bulk interception Centre has been controversial in that rogue elements in the state used it to spy on South African politicians, members of the public service, journalists, and businesspeople in around 2005 (Office of the Inspector General of Intelligence 2006).

A subsequent Commission of Inquiry, held in 2008 (called the Matthews Commission) found that the Centre was most likely operating illegally and unconstitutionally as it did not have a founding law (Matthews, Ginwala and Nathan 2008). However, ever since then, the government has failed to provide legislation to address this problem, until the Constitutional Court judgment compelled it to. It is for these reasons that the amaBhungane Centre for Investigative Journalism decided to include the Centre in its constitutional challenge.

WHAT THE CONSTITUTIONAL COURT SAID

In March 2021, the Constitutional Court found that the Agency was conducting bulk surveillance illegally and unconstitutionally because there was no law authorising the practice, and that they should cease bulk surveillance until there was (amaBhungane Centre for Investigative Journalism and another 2021).

The government maintained that the Centre was covered by the 1994 National Strategic Intelligence Act, which allows the Agency to gather, correlate, evaluate and analyse foreign intelligence to identify any threat or potential national security threat. However, the Court did not accept this argument as it argued that there was no explicit mention of the Centre. The Bill is meant to address this problem and put the Centre on a legal footing, by including a section that establishes the Centre and sets out its basic functions.

The case was based on evidence that emerged during a court case that the amaBhungane Centre for Investigative Journalism's Sam Sole was spied on by the state while communicating with a source in

Photo: Graham van de Ruit

South Africa's National Prosecuting Authority. The journalism centre used this information to challenge the constitutionality of Rica, as well as the constitutionality of the Centre. The court found that the Centre's bulk surveillance activities were unlawful and invalid, as there was no law authorising these practices, and had to be shut down immediately.

In the judgment, the Court gave some indication that it would be looking for a law authorising bulk surveillance that sets out '…the nuts and bolts of the [Centre's] functions', and spells out in '…clear, precise terms the manner, circumstances or duration of the collection, gathering, evaluation and analysis of domestic and foreign intelligence.' It would also be looking for detail on '…how these various types of intelligence must be captured, copied, stored, or distributed.' After the judgment, amaBhungane wrote to the SSA to ask if they had shut down the NCC, and they confirmed that they had (Sole 2021). These are features of a new law that the Court would be looking for.

While the Centre is meant to confine itself to conducting surveillance outside South Africa's borders, in its answering affidavit to the Court, the Agency admitted that it had no way of distinguishing between foreign and local communication signals when it conducted bulk interceptions (State Security Agency 2017). Their admission may be a basis for a future challenge if a law is introduced that assigns weaker protections to foreign communications than local communications.

WHAT THE BILL SAYS

In the memorandum attached to the Bill, the presidency claims that it has complied with the Constitutional Court order by establishing the Centre and providing for its mandate. It clarifies that the Centre shall have two main functions: signals intelligence collection (in other words, bulk surveillance of electronic signals for intelligence purposes) and analysis and information security/ cryptography.

In relation to bulk surveillance, the Bill says that Centre shall gather, correlate, evaluate and analyse relevant intelligence to identify any threat or potential threat to national security; however, it does not clarify which bulk surveillance practices the Centre can use.

Before conducting surveillance, the Centre needs to seek approval for interception applications from a retired judge, assisted by two interception experts appointed by the Minister.

The judge will be appointed by the president. The Bill also says that the Centre should supply relevant intelligence to the national intelligence structures.

In relation to information security/ cryptography, the Bill says that the Centre shall be responsible for identifying and securing critical national information infrastructure, protecting classified information, securing the communications infrastructure of the state, coordinating research and development on electronic communications, and identifying and impeding cybersecurity threats. The Bill exempts the Centre from having to seek broadcasting or electronic communications licences. The head of the Centre shall be appointed by the Minister and its members will be seconded from the Agency.

OTHER COUNTRIES

In preparing the Bill, the presidency claims to have conducted benchmarking studies for the Bill, including on the architecture of the UK, the US, Germany, Israel, Algeria, Zimbabwe and Egypt.

It is useful to look at some of the countries to see how the Bill compares to them. In 2006, the European Court of Human Rights developed a set of principles that have become recognised internationally as the basic standards for strategic surveillance, known as the 'Weber Principles' (European Court of Human Rights 2006). The principles were named after the first applicant in the case, Gabriele Weber, an investigative journalist. She claimed that poorly regulated surveillance made it more difficult for her to investigate stories on issues relating to abuses of national security in Europe and Latin America. This was because governments in these regions would not guarantee the privacy of her communications, and her freedom of expression, since they conducted untargeted bulk surveillance.

The Weber principles state that governments should ensure that warrants are granted for strategic surveillance, and that the warrants should contain the following information:

- The nature of the offences which gave rise to the application for the warrant;
- The categories of people likely to have their communications intercepted;
- Limits on the duration of interception;
- The procedures to be used for examining, using and storing information;
- The precautions to be taken when communicating intercepted information to third parties; and
- The circumstances in which information may be erased or records destroyed.

These principles ensure that strategic surveillance is not completely open-ended. More recently, the European Court of Human Rights has recognised that these principles are not completely applicable to bulk interception as technological advancements have made surveillance at scale much more possible than it was when the Weber Principles were developed. Consequently, in 2021, it adapted these principles to make them more applicable to large bulk surveillance programmes. They require a domestic legal framework to provide what they refer to as 'end-to-end' safeguards covering all stages of the bulk interception, and define clearly the following:

- The grounds on which bulk interception may be authorised;
- The circumstances in which an individual's communications may be intercepted;
- The procedure to be followed for granting authorisation;
- The procedures to be followed for selecting, examining and using intercept material;
- The precautions to be taken when communicating the material to other parties;
- The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
- The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
- The procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

They require that the bases of surveillance should be spelt out in a law authorising bulk surveillance.

This law should be accessible publicly and the bases for surveillance should not be relegated to secretive, subsidiary regulations.

Decisions about strategic surveillance should be taken by an independent body, preferably a judge, who should issue warrants, even if they were not targeted at specific individuals and authorised bulk surveillance of categories of individuals (members of an organisation suspected of serious crimes, for instance). The law must state that the duration of the operations should be limited, although bulk surveillance is typically of longer duration than surveillance targeted at individuals.

One of the countries the presidency claimed to have looked at in benchmarking the Bill is Germany. However, they have ignored important recent developments around the regulation and oversight of bulk surveillance in that country.

In 2020, the German Constitutional Court dismissed the argument often used to justify bulk surveillance that foreigners should be granted weaker privacy protections than nationals.

It ordered the government there to revise the law governing the foreign intelligence service, BND, and its bulk surveillance capabilities, to respect the privacy rights of non-nationals (Bundesverfassungsgericht 2020). It also found that the grounds for bulk collection were not specific enough, which made proper oversight impossible, and special safeguards for the communications of journalists and lawyers were lacking.

The German Constitutional Court set out six areas the government needed to reform (Bundesverfassungsgericht 2020). These were as follows:

- Restricting the volume of data they intercepted and the geographical area covered by surveillance;
- Restricting the transfer of this data to other entities, such as foreign governments;
- Retaining data for not more than six months;
- Providing special protections for professional groups that require confidentiality of communications, such as journalists and lawyers;
- Deleting data referring to the highly personal domain; and
- Documenting these deletions to allow an independent oversight body to assess if they are minimising the data they are storing.

Photo: Ichie Opara

Other safeguards under discussion globally include legislation insisting on warrants containing information on the following (Wetzling and Vieth 2018):

- The fibre-optic cables that are going to be intercepted;
- The expiration dates for particular intelligence operations;
- The private entities that will be involved in assisting (if any);
- The search terms or selectors to be used, or if they cannot all be identified in advance, after-the-fact notification of the judge (a feature of the Swedish system);
- Notification of surveillance subjects when individuals become targets (also a feature of the Swedish system and now a requirement in South Africa for Rica intercepts, which sets a higher standard for communication intercepts);
- Limitations on the number of people who have been in direct communication with the surveillance target, or the number of hops out from the target (Bradley 2014);
- The geographical zones or organisations or groups of people to be placed under surveillance;
- Issuing different warrants for the different stages of the bulk surveillance process;
- Setting quotas for methods used to collect data in order to prevent overuse of the most invasive methods.

THE OPTION OF REFORMING BULK SURVEILLANCE

Despite the Agency having claimed that it benchmarked the Bill internationally, this benchmarking is highly selective and shows no appreciation of the issues around bulk surveillance, its regulation, and its oversight.

In the wake of the Edward Snowden revelations, there have been major disagreements internationally on whether bulk surveillance should ever be legally permissible. Gradually, however, more judgments are emerging that recognise bulk collection as a viable intelligence method (Bundesverfassungsgericht 2020), including the German judgment on the BND Act.

Parliament needs to decide whether it wants the Agency to have these powers or not. If it decides that it does want the Agency to have these powers, then there are reform options that are available such as the ones mentioned above.

On a positive note, the Bill does provide for a judge to authorise bulk surveillance (not always the case in other countries), supported by interception experts appointed by the Minister. In contrast, in the UK, warrants are authorised by the executive. However, the Bill does not provide details on the bases the judge will use to make decisions.

The Bill gives little detail on the Centre's mandate, powers and functions, and there is no real evidence of the Presidency having considered safeguards such as the ones mentioned above.

In fact, all the Presidency has done is taken that clause on the strategic intelligence mandate of the Agency from the National Strategic Intelligence Act – the very clause the Constitutional Court had criticised for being too vague – and copied it into the new Bill, subject to the caveats around the judge and experts.

This is a concern, as the judge is a Presidential appointment. This is remarkable, since the Constitutional Court criticised executive involvement in the appointment of the Rica judge. Thus, presumably, the same standard should apply to the bulk interception judge. A judge that takes decisions on even more invasive capabilities than what Rica provides for, should be at least as, and preferably even more, independent than the Rica judge.

The appointments of experts to assist the judge does not address the 'ex parte' problem, which the Constitutional Court identified as a major weakness of Rica, namely that the judge only gets to hear the applicant's side of the story.

In contrast, in the Swedish system (European Court of Human Rights 2018), their foreign signals intelligence court has a Privacy Protection Representative.

In the case of the US, the signals intelligence court (known as the Foreign Intelligence Surveillance Court) includes a friend of the court, or amicus curiae, to assist the judges on novel legal or technological issues. However, this position is not ideal when compared to that of the public advocate, in that this person does not necessarily act as a public representative. It is also left to the discretion of the judge to appoint one or not, rather than being a permanent fixture of the court.

Ideally, a public advocate should be included in all applications and be granted security clearance to protect the security of the process, in line with well recognised processes elsewhere involving 'cleared counsel', or lawyers with security clearance, which allows them to access secret evidence the state is relying on as evidence in proceedings against individuals (Cole and Vladeck 2014, pg. 162).

While the introduction of a public advocate introduces risks into the process, these are outweighed by the risks (which have been proven to be considerable) of not having one. If the advocate is provided with all information held by the applicant on the surveillance subject, then they will be put on the same footing as the applicant. This will allow them to interrogate the case beyond what is provided for in the application (although the advocate would need to be forbidden from communicating with excluded parties without authorisation once they are served with closed evidence) (Jackson 2019, pg. 126).

The Bill also amends basic definitions to broaden the scope for intelligence, to the point where intelligence risks losing its distinctiveness when compared to other forms of information collection, research, and policymaking.

All manner of issues could potentially be handled by the Agency if certain definitions are broadened, leading to a dangerous and secretive intelligence overreach into more and more areas of open government. This risk is made worse by the fact that the only limitation placed on the type of foreign intelligence the Centre should collect is that it should be relevant.

For instance, the Bill defines foreign intelligence – which the Centre is meant to confine itself to – as '…any external threat or opportunity or potential opportunity or threat or potential threat to national security.' The inclusion of opportunities, in addition to threats, is so broad and covers so many areas of policy – whether related to national security or not – that intelligence risks becoming everything and nothing.

This overbreadth is repeated in the definitions of domestic intelligence, national security intelligence, and intelligence collection. Once intelligence mandates include opportunities and interests, including economic interests, then all manner of abuses become possible and, in fact, likely. Mandates broadened in this way have become major drivers of global espionage and spying for profit. For instance, companies attempting to obtain decision advantages over their competitors can try and bribe spies for intelligence.

The upshot of these broad definitions, and weak controls and oversight, is that the Presidency will have the most powerful spying capability in existence at its disposal with few meaningful checks and balances.

Photo: Ichie Opara

THE OPTION OF ENDING BULK SURVEILLANCE

Bulk surveillance rests on the ability of intelligence agencies to prove that what their signals intelligence agencies are collecting is, in fact, foreign and not local communication. Otherwise, they would not be able sustain the argument for such invasive powers.

But how does one separate foreign and domestic communications in an era of globally connected communications, when people send, store and receive communications on foreign servers all the time?

Yet, as stated above, in its answering affidavit, the Agency_admitted that it had no way of distinguishing between foreign and local signals when it conducted bulk surveillance (State Security Agency 2017). In other words, on the Agency's own admission, there is no basis for a law to assign weaker protections to foreign communications than local communications. This is precisely what the Bill is attempting to do relative to Rica, which governs targeted interceptions of communications inside South Africa.

There is also a basic democratic decision that Parliament needs to take about what powers it wants the Agency to have.

Can it ever be acceptable for a government to have a spying capability where no one can have a reasonable expectation of privacy at any point, which risks destroying so much of our social fabric?

The essence of the right to privacy involves people being able to exchange information in spaces that are beyond the reach of other members of society, and bulk surveillance violates this essence, and does so in ways that constitute a disproportionate response to the level of threat (Privacy International 2019, pg. 8).

Insisting that government should use its surveillance powers only if there is individualised, reasonable suspicion of serious criminality or threats to national security will resolve this dilemma, but it does mean that it will lack the capabilities that other governments have and may miss national security threats it does not know about.

However, governments cannot adopt whatever measures they see fit to fight national security threats. The Agency may still be able to make an operational case for bulk surveillance in time to come, but not everything that is useful to an intelligence service should be permissible in a democratic society.

As the Snowden disclosures showed, the Five Eyes has used bulk surveillance for reasons that stretch far beyond protecting national security and into economic espionage, diplomatic manipulation, and social control, including of former colonial countries.

If South Africa took a position that no democracy should tolerate blanket indiscriminate surveillance and committed to rolling back these powers globally, then it would be exercising thought leadership on these issues and reducing the scope for global espionage. South Africa is already contributing to preventing destabilising accumulations of weapons through the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies, which covers bulk internet surveillance. Taking this decision would be consistent with South Africa's international commitment to disarmaments, given that bulk surveillance is an offensive weapon that comes out of a military environment. If Parliament decided to keep the Centre shut, then any foreign-focussed surveillance would need to be dealt with through the Rica process and defensive cybersecurity functions would need to be assigned to another entity.

REFERENCES AND FURTHER READING

10 Human Rights Organisations v United Kingdom, Grand Chamber, European Court of Human Rights. [Online]. [Accessed 28 November 2023]. Available from: https://privacyinternational.org/legal-action/10-human-rights-organisations-v-united-kingdom.

AmaBhungane Centre for Investigative Journalism and another v Minister of Justice and others, CCT278/19 & CCT279/19 [2021] ZACC 03. [Online]. [Accessed 28 November 2023]. Available from: https://www.concourt.org.za/index.php/judgement/383-amabhungane-centre-for-investigative-journalism-npc-and-another-v-minister-of-justice-and-correctional-services-and-others-minister--of-police-v-amabhungane-centre-for-investigative-journalism-npc-and-others-cct278-19-cct279-19#:~:text=The%20Court%20declared%20RICA%20unconstitutional,independent%20judicial%20authorisation%20of%20interception.

Bradley, T. 2014. NSA reform: what President Obama said, and what he didn't. Forbes, 17 January. [Online]. [Accessed 30 October 2023]. Available from: https://www.forbes.com/sites/tonybradley/2014/01/17/nsa-reform-what-president-obama-said-and-what-he-didnt/#28046375de6c.

Bundesverfassungsgericht. 2020. In their current form, the Federal Intelligence Service's powers to conduct surveillance of foreign telecommunications violate fundamental rights of the Basic Law (press release). [Online]. [Accessed 30 October 2023]. Available from: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html.

Cole, D. and S.I Vladeck. 2014. Navigating the shoals of secrecy: a comparative analysis of the use of secret evidence and "cleared counsel" in the United States, the United Kingdom and Canada. In Liora, L; McCrudden, C and Bowles, N.eds. *Reasoning rights: comparative judicial engagement*. London: Hart Publishing. [Online]. [Accessed 30 October 2023]. Available from: http://dx.doi.org/10.5040/9781849468466.

De Wet, P. 2013. Spy wars – South Africa is not innocent. Mail & Guardian. [Online]. [Accessed 30 October 2023]. Available from: https://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent/.

European Commission for Democracy Through Law. 2015. Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies. Strasbourg: European Commission for Democracy Through Law. [Online]. [Accessed 30 October 2023]. Available from: https://www.statewatch.org/media/documents/news/2015/apr/coe-venice-commission-oversight-intelligence%20agencies-sigint-update-2015.pdf.

European Court of Human Rights. 2006. Weber and another v Germany (App No 55878/00). [Online]. [Accessed 30 October 2023]. Available from: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-77888%22]}.

European Court of Human Rights. 2018. Centrum för Rättvisa v Sweden (App No 35252/08). [Online]. [Accessed 30 October 2023]. Available from: https://www.statewatch.org/media/documents/news/2018/jun/echr-sweden-Judgment-bulk-interception-communications-FULL.pdf.

European Court of Human Rights, 2019. Big Brother Watch and others v United Kingdom (Apps No 58170/13, 62322/14 and 24960/15). [Online]. [Accessed 30 November 2023]. Available from: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}.

Farrell, P. 2013. History of Five Eyes – explainer, 2 December. [Online]. [Accessed 30 October 2023. Available from: https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

Jackson, J.D. 2019. In a world of their own: security-cleared counsel, best practice and procedural tradition. *Journal of Law and Society*. 46(1), pp. s115-135.

Matthews, J; Ginwala, F and Nathan, L. 2008. Intelligence in a constitutional democracy. [Online]. [Accessed 30 October 2023]. Available from: https:/www.lse.ac.uk/international-development/Assets/Documents/PDFs/csrc-background-papers/Intelligence-In-a-Constitutional-Democracy.pdf.

Office of the Inspector general of Intelligence. 2006. Executive summary of the final report on the findings of an investigation into the legality of the surveillance operations carried out by the NIA on Mr. S Macozoma. [Online]. [Accessed 30 October 2023]. Available from: https://www.gov.za/sites/default/files/gcis_document/201409/igreport0.pdf.

Privacy International. 2016. How bulk interception works. [Online]. [Accessed 28 November 2023]. Available from: https://privacyinternational.org/long-read/827/how-bulk-interception-works.

Privacy International. 2019. Intervention before the Federal Constitutional Court in the case 2 BvR 1850/18. [Online]. [Accessed 30 November 2023]. Available from: https://privacyinternational.org/sites/default/files/2019-09/BVerfG_Statement_PI_Trojans_Sept2019_EN.pdf.

Sole, S. 2021. State Security Agency confirms suspension of "bulk surveillance" following amaBhungane ConCourt victory. Daily Maverick. [Online]. [Accessed 30 October 202]. Available from: https://www.dailymaverick.co.za/article/2021-02-25-state-security-agency-confirms-suspension-of-bulk-surveillance-following-amabhungane-concourt-victory/.

Staff Writer. Britain spied on MTN – Snowden leaks. MyBroadband. [Online]. [Accessed 30 October 2023. Available from: https://mybroadband.co.za/news/security/191186-britain-spied-on-mtn-snowden-leaks.html.

State Security Agency. 2017. Answering affidavit. AmaBhungane Centre for Investigative Journalism and others vs Minister of Justice and Correctional Services and others. [Online]. [Accessed 30 October 2o23. Available from: https://www.anchoredinlaw.net/wp-content/uploads/2019/09/Answering-Affidavit-DG-State-Security-Agency.pdf.

The United Kingdom. 2019. The United Kingdom's observations on the Grand Chamber's questions to the parties. Big Brother Watch and others v the United Kingdom and others. [Online]. [Accessed 30 October 2023]. Available from: https:/privacyinternational.org/sites/default/files/2019-07/UK Gov Obs - Revised Version - May 2019.PDF.

Wetzling, T. and Vieth, K. 2018. Upping the ante on bulk surveillance: an international compendium of good legal safeguards and oversight innovations. Berlin: Heinrich Boll Stiftung. [Online]. [Accessed 30 October 2023]. Available from: https://www.stiftung-nv.de/sites/default/files/upping_the_ante_on_bulk_surveillance_v2.pdf.