Comments on Regulation of interception of Communications and Provision of Communicated Related Information Amendment Bill, published in Government Gazette 49189, 25 August 2023

Jane Duncan
Professor of Digital Society
School of Social and Political Sciences
University of Glasgow
Visiting Professor
Department of Communication and Media
University of Johannesburg[1]

27 September 2023

[1] This submission 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 I am the holder of the Global Professorship. The submission 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, and specifically reports by Murray Hunter, Heidi Swart and Catherine Kruyer.

1. Process

The process followed by the Ministry of Justice and Correctional Services in drafting the Bill is inadequate. By this stage, the Bill could have been preceded by a review and a discussion paper setting out a comprehensive policy framework more fitting for the digital era, which would most likely have resulted in the amendments being extended beyond the areas of unconstitutionality identified by the Constitutional Court in the amaBhungane matter[2], as the Act has become dated on numerous levels. Had that review taken place timeously, then there may well not have been the need for the Constitutional Court case as areas of possible unconstitutionality could have been anticipated. Rica is an outdated piece of legislation and no longer fit for purpose, but amendments are being pursued piecemeal: a problem the Department acknowledged publicly as far back as 2017, coupled with a commitment to review Rica (Swart 2017). The fact that the Constitutional Court ruled on five areas of unconstitutionality, and a sixth related area (on the National Communication Centre) does not mean that there are no other problematic and potentially constitutionally offensive issues. Rica needs to be reviewed in a comprehensive fashion and plans in this regard, I believe, should be ventilated at the Committee hearings on the Bill as the need remains despite (somewhat belated) progress on the Bill.

2. Areas of unconstitutionality

According to the Constitutional Court, the declaration of unconstitutionality by the High Court is confirmed only to the extent that the Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (RICA) fails to—
(a) provide for safeguards to ensure that a Judge designated in terms of section 1 is sufficiently independent;
(b) provide for notifying the subject of surveillance of the fact of her or his surveillance as soon as notification can be given without jeopardising the purpose of surveillance after surveillance has been terminated;
(c) adequately provide safeguards to address the fact that interception directions are sought and obtained ex parte;
(d) adequately prescribe procedures to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data; and
(e) provide adequate safeguards where the subject of surveillance is a practising lawyer or journalist.

The declaration of unconstitutionality took effect from the date of the judgment and was suspended for 36 months to afford Parliament an opportunity to cure the defects causing the invalidity. Each section of the Bill will be discussed below and related back to the Constitutional Court judgment and prescripts.

3. Designated judges (15A)

[2] AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC [2021] ZACC 3;2021 (3) SA 246 (CC); 2021 (4) BCLR 349 (CC) ("AmaBhungane").

The requirement for the judge to be independent needs to include independent decision making about the appointment of the judge and security of tenure for the judge, implying a term of office that is longer than one year, even if renewable, but not too long to lead to "case hardening" where the judge "[loses] the qualities of independence and external oversight" (Kruyer 2023, pg. 16). The problem of a lack of independence has been responded to by inserting a requirement for the judge to be appointed by the Minister in consultation with the Chief Justice.

This appointment process is adequate only to the extent that it means that the appointment must be made by the Minister with the concurrence of the Chief Justice, and doing so will mean that there is a properly designated judge. This clarity is necessary to ensure that decision making does not continue to rest with the executive, which opens the door to political interference in the selection process.

However, the new requirements, including the user notification requirement, as well as the proposed requirements to provide reasons to subjects of communication and to monitor s.205 subpoenas for communication-related information or metadata (see below for both), are likely to lead to significant increases in workload. These increases may lead to bottlenecks in the system where only one judge is making decisions, in a situation where speed of decision-making is of the essence. Establishing a panel of judges, rather than having one single judge, may be the most appropriate solution to this problem, and in any event, it appears that Rica envisaged the possibility of there being more than one judge.

Recommendations:

- **The Bill could make it clear that the appointments of the designated judges and review judges should be made with the concurrence of the Chief Justice;**
- **Rather than having one judge, consideration could be given to having a panel of judges.**

4. Review judge (15B)

In terms of the Bill, the review judge has the powers to confirm, vary or set aside any decision made by the designated judge. However, the intention appears to be for the review judge to review all decisions of the deciding judge immediately after the decisions are made. Perhaps a better use of resources would be to build automatic review into the process once surveillance subjects have been notified, and then they can be included in the review if they wish to contest the bases for surveillance, supported by the public advocate (see below). Doing so may make for a much more robust review process that sheds new light on the decision. Otherwise, the review judge may mirror the decisions of the decision-making judge and add little value to the mix. The Bill is also not clear on whether the review judge will have access to remedial powers if is found that decisions were flawed, and as suggested by Adv. Catherine Kruyer, these remedial powers could include making orders, cessation of surveillance, destruction of intercept information or payment for compensation (Kruyer 2023, pg. 28).

The fact that the designated judge and the review judge will enjoy substantial tenure for a non-renewable period not exceeding seven years is welcome. However, while it is clear what the maximum period of their tenure is, it is not clear what the minimum period of their tenure is. This section could be amended to make clear what the terms of their tenure are. To avoid the dangers of judges becoming subject to regulatory capture, it may be better to restrict appointments to a non-renewable term of five years. However, in the same way that one judge may not be enough at the decision stage, one judge is also not likely to be enough at the review stage and the establishment of a Tribunal could be considered.

Recommendations:

- **The Bill could state that the tenure of both judges is for a non-renewal period of five years;**
- **The review judge should be retained but consideration should be given to including more review judges and establishing a Review Tribunal with remedial powers.**

5. Ex parte problem

It is possible that the review judge was introduced as a safeguard to respond to the 'ex-parte' problem identified by the Constitutional Court, where interception directions are granted without informing the affected party, who is consequently unable to defend their rights. No other safeguards are apparent from the draft. Alternatively, it has been introduced to address the issue raised in the Constitutional Court on the lack of automatic review procedures, although they did not make a finding on this. The Constitutional Court left it to Parliament to decide how best to respond to these matters, but with the proviso that its solutions would need to address the inherently one-sided nature of the process.

The purpose of the ex-parte requirement is to ensure that there is an adversarial element introduced into the system as there are real weaknesses in the designated judge having to rely on information provided by the applicants only when interception directions are applied for. As has been shown in the past, an applicant with ill or corrupt intent can lie to mislead a judge into granting a direction, as was the case with respect to two *Sunday Times* journalists in 2011.

The review judge does not satisfy the ex-parte requirement as it is not an adequate or appropriate safeguard and fails to introduce an interrogative element. In such circumstances, there is no reason to believe that two judges operating on an ex-parte basis will be less likely to make incorrect decisions than one, as they will still be making decisions based on the same one-sided secret evidence. Any solution to the problem must address the issue that the judge(s) do not get to hear the other side of the argument, which undermines the *audi alteram partem* (listen to the other side) principle and does not elevate the process from being an inquisitorial one to an adversarial one. It is disappointing that the Bill fails to grapple sufficiently with this problem and the advances made internationally in how to respond to it.

In this regard, what could be considered is for the Bill to make provision for a public advocate to defend the interests of the surveillance subject, appointed using the same procedures as for the designated judge and review judge, ie. by the Minister with the

concurrence of the Chief Justice, and for a duration of five years. The public advocate could 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 applicant on the surveillance subject, then they will be put on same footing as the applicant, to 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). In one case, the advocate was also able to identify inconsistencies in the state's case (Jackson 2019, pg. 125). Further arguments in justification for this recommendation are provided in the research on amendments to Rica which the Media Policy and Democracy Project commissioned (Kruyer 2023, pp. 18-19).

Including an *amicus curiae* in the process, as is the case in the US system, is not ideal as the amicus has an even more remote relationship to the surveillance subject than the special advocate, whose role is tied more directly to the interests of the subject than an amicus (Jackson 2019; pg. 130). With regards to the powers and functions of the public advocate, they could be able to cross-examine the applicants, ensure that all the relevant arguments on the facts and the law are put before the judges, and perform any other function that would assist the judges. They could also be available to surveillance subjects who would like to take decisions on review following post-surveillance notification and they could represent their interests in proceedings. It would be a contradiction in terms for there to be a public advocate, but for that advocate not to be available to the public.

Recommendation:

- **The Bill could make provision for a special advocate to defend the interests of the surveillance subject, appointed in the same manner and for the same duration as the designated judge and review judge, and with the powers to access all information held by the applicant about the subject, cross-examine the applicants and perform any other function that assists the judges to make decisions. The advocate could receive an appropriate level of security clearance. They could operate at decision-making and review levels and be available to surveillance subjects who wish to contest decisions they have been made aware of through post-surveillance notification, and when receiving reasons, they should be provided with sufficient information to be able to defend any rights that may have been infringed.**

6. **Disclosure that person in respect of whom direction, extension of direction or entry warrant is sought is journalist or practising lawyer (23A)**

This section is reproduced from the Constitutional Court judgment for the period of suspension of the judgment. However, the following clause has been omitted from the Bill:

> (2) The designated Judge must grant the direction, extension of a direction or entry warrant referred to in subsection (1) only if satisfied that it is necessary to do so, notwithstanding the fact that the subject is a journalist or practising lawyer.

This means that the protection afforded by the Bill is weaker than the protection afforded by the Constitutional Court for the period of suspension. Requiring the judge to satisfy themselves that the direction is necessary is a high test. To fulfil this requirement, the direction needs to be more than merely convenient and cannot lead to the required result of solving serious crimes or protecting national security using less invasive means and protecting vital interests. Putting journalists and lawyers under surveillance really needs to be an investigative method of last resort, which can be achieved by including the above clause.

Recommendation:

- **Include the following clause in the draft s.23(A):**

  (2) The designated Judge must grant the direction, extension of a direction or entry warrant referred to in subsection (1) only if satisfied that it is necessary to do so, notwithstanding the fact that the subject is a journalist or practising lawyer.

7. Post-surveillance notification (25(A)

This section is largely reproduced from the Constitutional Court judgment for the period of suspension of the judgment, except for the following clause, which has been added:

> (2) If the notification contemplated in subsection (1)—
> …
> (b) has the potential to impact negatively on national security, the designated judge may, upon application by a law enforcement officer, direct that the giving of notification be withheld for such period as may be determined by the designated judge.''.

The addition of this clause is too broadly framed and could lead to an indefinite suspension of the notification requirement. It is overbroad in the sense that the judge merely must satisfy themselves that the notification has the potential to impact negatively on national security. This introduces a speculative element into the decision-making as the impact merely needs to be possible, not imminent or, even for that matter, likely. Also, there does not need to be a requirement to show a threat to national security, merely a possibility of negative impact, which could encompass events or actions that are depressing or unpleasant, but do not necessarily constitute a clear and present danger to national security. The uncertainty could be reduced by specifying the adverse result of the notification, such as death or physical harm to an individual, fleeing prosecution or prevention of evidence tampering or witness intimidation, and the delay should be necessary to prevent these adverse results from occurring, and for no longer than that. The Constitutional Court envisaged that a revised Rica would include an upper time limit on delayed notification, which this provision fails to include.

Furthermore, the notification requirement does not include a requirement for the judge to provide reasons for their decisions. Mere notification in the absence of reasons makes it difficult, if not impossible, to assess the basis for issuing the direction, leaving the subject at somewhat of a loss about how to protect their rights - to the extent that they need to - once they are informed.

Recommendations:

- **The clause on national security should be replaced with a clause that allows for delayed notification in 'life-and-limb' situations and should set an upper limit for the delay;**
- **The Rica judges should give reasons for their decisions, which should form part of the post-surveillance notification as a default;**
- **Consideration could be given to adapting the mechanism for post-surveillance notification prescribed by the High Court, where decisions to delay notification should be referred to the Review Tribunal (see above).**

8. Management of data (37(A))

According to the Constitutional Court, Rica was unconstitutional because the sections '…relating to the management of intercept data gave no clarity or detail on: what must be stored; how and where it must be stored; the security of such storage; precautions around access to the stored data (who may have access and who may not); the purposes for accessing the data; and how and at what point the data may or must be destroyed. Thus, there is a real risk that the private information of individuals may land in wrong hands or, even if in the "right" hands, may be used for purposes other than those envisaged in RICA.'

The applicants in the case made the argument that there are no provisions in Rica with regard to where interception information is stored, who may have access to it and under what conditions, whether any access has to be recorded/ registered, whether copies may be made, whether the fact of the number and distribution of copies has to be recorded in any way, whether access to copies may be shared within the intelligence or security community and if so on what conditions and what documentation of this sharing takes place, whether the material must be or may be destroyed at any time and if so when/ under what conditions, if and how extraneous or irrelevant material that is gathered must be separated and destroyed and whether this is documented.

The Bill responds to these issues by requiring issues relating to the processing, examining, copying, sharing disclosing, sorting through, using, storing, or destroying of any intercept data to be prescribed, presumably in regulations. It then sets out the principles for the safeguarding of data, broadly conforming to the Weber Principles.[3] Including these procedures in regulations without adequate guidance in primary legislation is inadequate in that it delegates the details to a subsidiary process that may well take place without public participation or even in secret.

[3] Weber and Sanravia v Germany, no 54934/00, § 95, ECHR 2008 (Weber).

Some of the issues that could be covered in primary legislation could include the fact that intercept information (including metadata) obtained in terms of Rica should be limited to the minimum that is necessary for the authorised purposes, including limiting the number of persons to whom any of the information is made available, the extent of that disclosure, the extent to which any of the material is copied and the number of copies that are made. The Bill could also require intercept information to be destroyed as soon as there are no longer any grounds for retaining it. Where information is retained and examined for purposes other than the destruction of the material, and it is material that contains confidential journalistic material or identifies a source of journalistic material, then the judge must be informed. Information should not be shared with agencies of other countries under mutual assistance or international cooperation agreements if the human rights protections in the destination country are lower than in South Africa, to afford some level of protection to intercept information obtained locally (Duncan 2020; Investigatory Powers Act 2016). Finer details that are addressed in regulations should be gazetted for public comment.

Recommendations

- **The section around the management of data needs to be reconsidered as it does not provide sufficient detail to meet the requirements of the Constitutional Court judgment;**
- **Where information is retained and examined for purposes other than the destruction of the material, and it is material that contains confidential journalistic material or identifies a source of journalistic material, then the judge must be informed;**
- **Any details not dealt with in primary legislation should be included in regulations that are gazetted and released for public comment.**

9. Issues not dealt with

9.1 Section 205 of the Criminal Procedures Act

In confining itself to the four corners of the Rica judgment, the Bill is missing an opportunity to address possibly the most serious surveillance control and oversight issue, relating to s. 205 of the Criminal Procedures Act. S. 15(1) of Rica allows for the use of other procedures for obtaining real-time or archived communication-related information, and this had led to the preferred option of s. 205 being used extensively for law enforcement purposes. This is even though in 1999, the South African Law Commission recommended that the main surveillance law (at that stage the 1992 Interception of Communications Act) should be the only law authorising requests for call-related information (Swart 2023: 4-5).

Statistics released by successive Rica judges, through their reports to the Joint Standing Committee on Intelligence, as well as by mobile phone operators, demonstrate that s.205 is used far more frequently to obtain call-related information or metadata, than Rica is (Swart 2023). This provides law enforcement and intelligence agencies with a significant loophole as the requirements for a s.205 warrant are far lower than they are in Rica. For instance, applicants for warrants merely must prove that the metadata they are seeking merely must be relevant to a case, and not that it is being used as an investigative method of last resort or that it relates to a serious crime and that there are reasonable grounds to believe that

such crimes have been or are likely to be committed. Oversight arrangements in relation to metadata usage are also lower than they are in relation to Rica.

Metadata can say as much if not more about a person's relationships, interests, and habits as communication content, to the point where the distinction between metadata and content is become increasingly redundant. Mobile phone companies are required in terms of Rica to store metadata for a considerable period (between 3 and 5 years). However, controls over its usage by intelligence and law enforcement agencies are lax and have not kept up with recent developments that recognise the privacy implications of huge amounts of metadata being collected, stored, and analysed. Abuses of metadata resulting from these lax controls have been documented (Hunter 2020: 35; Swart 2023: 11-12). Therefore, it is necessary to address this loophole to prevent further abuses of metadata.

At the same time, information in the public domain points to metadata being of considerable use to law enforcement agencies in the investigation of criminal cases (Hunter 2020). The Law Commission formed its view about s.205 before metadata became as pervasive as it is today, so restricting metadata applications to the Rica judges only may not be practical given the sheer number of requests. Doing so will centralise decision-making in the Rica judge's office and is likely to create major bottlenecks, particularly if the user notification requirement and the provision of written reasons apply. It may make more sense to leave decision-making about s. 205 applications with magistrates and High Court judges, but to make the Rica standards apply to their decisions, including the need to make usage of metadata an investigative method of last resort and to confine the applications to serious crimes. All these objectives could be achieved by making Rica the only law for communication surveillance, including surveillance of real-time and archive related communication.

Recommendation

- **S. 15(1) and s. 59 of Rica should be repealed to make it clear that only Rica should be used for obtaining real-time or archived communication-related information, and that the Rica standards apply to this information, including the need to make usage of metadata an investigative method of last resort, to confine the applications to serious crimes and to provide post-surveillance notification to surveillance subjects combined with written reasons.**

9.2 Reporting requirements

The Rica judge reports to Parliament through the Joint Standing Committee on Intelligence. However, there is insufficient guidance provided on the reporting requirements and what reports should contain. As a result, reports have varied hugely in terms of the amount and type of information, making comparisons across the tenures of several judges difficult. In contrast, in the US criminal justice system, requirements are set as to what the reports should contain. An international civil society document setting out proposed standards for the application of human rights to communication surveillance, known as the Necessary and Proportionate Principles, has set out the following as the bare minimum to be included in a transparency reports:

> States should be transparent about the use and scope of Communications Surveillance laws, regulations, activities, powers, or authorities. They should publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting Communications Surveillance. States should not interfere with service providers in their efforts to publish the procedures they apply when assessing and complying with State requests for Communications Surveillance, adhere to those procedures, and publish records of State requests for Communications Surveillance (Necessary and Proportionate Principles 2014).

These standards could be considered for reporting. Furthermore, there is a potential for conflicts of interest in the judges reporting to Parliament on interceptions, as this is tantamount to the judges marking their own homework. Ideally, reporting should be separated from authorisation, which raises the question of the need for an independent reporting mechanism. Consideration could be given to the Inspector General of Intelligence playing that role, rather than creating an entirely separate reporting mechanism.

Recommendations:

- **The standards for reporting proposed in the Necessary and Proportionate Principles could be considered as the baseline reporting standards for the Rica judges;**
- **Consideration should be given to making the Inspector General of Intelligence responsible for reporting on Rica intercepts to Parliament.**

References

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 20 September 2023]. Available from: http://dx.doi.org/10.5040/9781849468466.

Duncan, J. 2020. The loophole in South Africa's spying laws. *Daily Maverick*, 9 March. [Online]. [Accessed 20 September 2023] Available from: https://www.dailymaverick.co.za/article/2020-03-09-the-loophole-in-south-africas-state-spying-laws/

Hunter, M. 2020. *Cops and call records: policing and metadata in South Africa.* Johannesburg: Media Policy and Democracy Project. [Online]. [Accessed 20 September 2023]. Available from: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/cops_and_call_records_web_masterset_26_march.pdf

Investigatory Powers Act 2016 (UK).

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.

Kruyer, C. 2023. *Reforming communication surveillance in South Africa: recommendations in the wake of the amaBhungane judgment and beyond*. Johannesburg: Intelwatch/ Media Policy and Democracy Project. [Online]. [Accessed 20 September 2023]. Available online: https://intelwatch.org.za/wp-content/uploads/2023/05/Intelwatch_Reforming_communication_surveillance_in_South_Africa_May_2023.pdf

Necessary and Proportionate Principles. 2014. [Online]. [Accessed 20 September 2023]. Available from: https://necessaryandproportionate.org/

Swart, H. 2017. Op-ed: Big brother is watching your phone call records. Daily Maverick, 10 May. [Online]. [Accessed 27 September 2023]. Available from: https://www.dailymaverick.co.za/article/2017-05-10-op-ed-big-brother-is-watching-your-phone-call-records/.

Swart, H. 2023. *Reforming communication surveillance in South Africa: understanding the section 205 'loophole'.* Johannesburg: Media Policy and Democracy Project/ Intelwatch. [Online]. [Accessed 20 September 2023]. Available from: https://intelwatch.org.za/wp-content/uploads/2023/05/Intelwatch_Supplementary_report_Reforming_surveillance_in_South_Africa_May_2023.pdf