London, 6 October 2023

Privacy International's response to the South African Parliamentary Monitoring Group's call for submissions on the on Regulation of interception of Communications and Provision of Communicated Related Informa/on Amendment Bill

Introduction

Privacy International (PI) welcomes the opportunity to provide comments on the Regulation of Interception of Communications and Provision of Communication-related Information Amendment Bill (the Rica Bill), published in Government Gazette 49189, 25 August 2023, as part of a call for comments made by the Portfolio Committee on Justice and Correctional Services.[1]

Privacy International (PI) is a London-based non-profit, non-governmental organisation (Charity Number: 1147471)[2] that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development, the UN Office of the High Commissioner for Human Rights and the UN Refugee Agency.

[1] Regulation of Interception of Communications and Provision of Communication-related Information Amendment Bill, *Call for Comments*, https://pmg.org.za/call-for-comment/1351/
[2] https://privacyinternational.org/

In the context of the *amaBhungane and Sole* challenge,[3] Privacy International together with and Right 2 Know Campaign (R2K) submitted amici curiae to assist the High Court of South Africa in Pretoria and the Constitutional Court of South Africa.[4]

While we acknowledge and welcome the positive changes introduced in the proposed amendments, we wish to provide specific comments that highlight where the amendments fall short or require improvement. Our aim is to enhance the overall framework and address any shortcomings for the betterment of the situation at hand.

In the following pages, we provide comments in relation to post-surveillance notification, judicial independence, protection for journalists and lawyers, closing the Section 205 loophole, and the need for balanced oversight with the inclusion of public defenders. We can summarize the main issues as follows:

1. Post-surveillance notification requirements. We discuss concerns regarding the broad exception of " potential national security risk" in Section 25A (2) of the Rica Amendment, suggesting that it be more precisely defined to prevent arbitrary exceptions. We also advocate for the law to provide for a maximum duration for notification delays to prevent indefinite postponements. Ensuring clear definitions and procedures is essential to prevent violations of privacy. Also, we propose the introduction of a well-defined procedure to guide individuals in addressing grievances effectively.

2. Enhancing the independence and accountability of designated judges: Preserving the independence and integrity of designated judges is crucial. We recommend a joint appointment process by the Minister of Justice and the Chief Justice to emphasize mutual accountability. Additionally, we suggest considering a panel of judges to distribute the workload, ensuring timely and impartial decisions.

3. Closing the section 205 loophole: We point out the need to address the Section 205 loophole, which allows access to sensitive communication data without adequate oversight. We stress the importance of incorporating measures into RICA to eliminate such potential loopholes, ensuring robust safeguards.

[3] Constitutional Court of South Africa, *amaBhungane Centre for Investigative Journalism and Stephen Patrick Sole v. Minister of Justice and Correctional Services, Minister of State Security and others*, Case CCT 278/19, 4 February 2021, https://privacyinternational.org/legal-action/amabhungane-and-sole-case-south-africa
[4] *ibid*.

4. Enhancing safeguards for journalists, lawyers, and civil society: We address the need for additional safeguards for journalists, lawyers, and civil society organizations. We highlight the omission of a crucial clause from the Bill, emphasizing the importance of reinstating it to protect the confidentiality and rights of these individuals. We also argue for enhanced protections for civil society organizations, aligning them with those enjoyed by journalists and lawyers.

5. Addressing the issue of *ex-parte* decision-making in surveillance: We discuss the inadequacy of the presence of only a review judge in addressing *ex-parte* decision-making. We argue that introducing public defenders to represent the interests of individuals subject to surveillance would enhance fairness and transparency. We emphasize that relying on confidential evidence without the opposing side undermines oversight and the principle of *audi alteram partem*.

In the subsequent sections, we will delve into each of these critical issues, offering comprehensive analyses, and detailed recommendations to address the challenges and shortcomings within the proposed amendments to RICA Bill.

1. Post-surveillance notification requirement falls short of international standards

The recent RICA amendment introduces a noteworthy addition at the proposed new section 25A, which outlines a framework for post-surveillance notifications. This shift away from a culture of secrecy is commendable; however, certain crucial aspects require further consideration specifically concerning broad definitions, potential lack of remedies and transparency practices.

a. Broad National Security Exception in Section 25A (2) of RICA Amendment

Section 25A (1) establishes a notification procedure that appears to align with international standards.[5] Nevertheless, Section 25A (2) introduces a provision whereby if the notification under subsection 1(b) has the potential to negatively impact national security, a designated judge may, upon application by a law enforcement officer, delay the notification as determined by the judge. This institutes an exception to the standard notification procedure. Notification requirements are

[5] UN OHCHR, *The right to privacy in the digital age, A/HRC/27/37*, 30 June 2014, para 47; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40* 17 April 2013, para 82; *Joint Declaration on Surveillance Programmes and Their Impact on Freedom of Expression*, 21 June 2013, para 5. For further information: PI, *PI's Guide to International Law and Surveillance*, December 2021, https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf.

necessary to enable individuals who are subjected to secret surveillance measures to challenge unlawful surveillance decisions. The provision is outlined as follows:

> 25 A (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. (emphasis added).

The UN General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, underscores the importance of regulating the right to privacy in a way that "must be publicly accessible, clear, precise, comprehensive and non-discriminatory".[6]

The first concern with this insertion arises from the broad definition of "national security risk." Its expansiveness affords the executive overly broad discretion in respect of the notification requirement, potentially allowing a wide range of scenarios to be classified within the exception regime.

Section 25A(2) also specifies that the impact on national security need only be potential, which allows for various interpretations. In such cases, there is no obligation to prove that the risk to national security must be immediate or specific in order to delay notification.

Whilst notification of surveillance is not an absolute right in the sense that it should operate without restrictions, any restriction on notification should be strictly limited, i.e. it should only be delayed where it would seriously jeopardize the purpose for which the surveillance is authorised, or where there is an imminent threat to human life.[7]

It is suggested that more precise criteria, i.e., it should only be delayed where it would seriously jeopardize the purpose for which the surveillance is authorised, or where there is an imminent threat to human life, be adopted to prevent arbitrary exceptions in the post-surveillance notification regime.

[6] UN Doc, A/RES/72/180, 19 December 2017.

[7] This is consistent with the development of international law and with the comparative experience of a wide range of jurisdictions, including Canada, Germany and Sweden and the United States and it is consistent with the Court's own case law, in particular the requirement that any restriction on the right to privacy or the right to an effective remedy should not impair the very essence of the right. See our comparative analysis on notifications regimes in Council of Europe countries and beyond at: Privacy International, PI intervention in *Pietrzak ao v Poland* case before the European Court of Human Rights (App Nos 72038/17 and 25237/18), October 2020, https://privacyinternational.org/legal-action/pietrzak-and-others-v-poland

Finally, it is worth noting that Section 25A (b) does not specify a maximum duration for withholding notifications based on potential impacts in national security. This omission implies the possibility of an indefinite delay that could turn the notification requirement in fact ineffective**. To enhance accountability and prevent abuse, it is advisable to establish a specific maximum period for notification delays.**

The United Nations Human Rights Committee in its Concluding Observations on the Sixth Periodic Report of Hungary expressed worry about a legal framework that lacked clear definitions. In this case, a lack of clarity could render the post-notification procedure ineffective, potentially leading to arbitrary interferences with no recourse for individuals.[8]

In *Weber* case*,* the European Court of Human Rights (ECtHR) noted that there is "in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".[9]

In its judgment in *Schrems* case, the Court of Justice of the European Union (CJEU) added that:

> [a]ccording to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection.[10]

We do not submit that notification of surveillance is an absolute right in the sense that it should operate without restrictions. Rather, any restriction on notification should be strictly limited, i.e. it should only be delayed where it would seriously jeopardize the purpose for which the surveillance is authorised, or where there is an imminent threat to human life. Any such delay in notification, moreover, must be judicially authorised and subject to continuing judicial oversight. The burden must be on the government to satisfy an independent and impartial tribunal that continued non-notification is both necessary for a legitimate aim and proportionate.

In conclusion, while the inclusion of post-surveillance notification in the RICA amendment is a positive step toward transparency, it is imperative to address the issues related to the broad definition of

[8] UN Human Rights Committee, UN Doc CCPR/C/HUN/CO/6*,* 9 May 2018.
[9] ECtHR, *Weber and Savaria v Germany,* App No 54934/00, 29 June 2006, para 135.
[10] CJEU, *Data Protection Commissioner v Facebook Ireland and Schrems (Schrems II), Case C-311/18*, Judgment, 16 July 2020, para 187, see also CJEU, Joined cases *Tele2 Sverige AB v Post-och telestyrelse*n and *Secretary of State for the Home Department v Tom Watson*, Cases Nos C–203/15 and C–698/15, Judgment, 21 December 2016, para 121.

national security risk, the "potential to impact" criterion, and the absence of a maximum notification delay period. Adherence to international standards and human rights principles is essential in these issues.

b. Addressing the gap: absence of remedies and procedures post-notification grievances

The relevance of the post-notification procedure cannot be overstated, as it significantly contributes to accountability and diminishes the potential for arbitrary interferences, as affirmed by the Court Order in *amaBhungane and Sole* case. It is crucial to highlight that the Court Order also establishes that through notification "the subject of surveillance is afforded an opportunity to assess whether the interception direction was applied for and issued in accordance with the Constitution and RICA. If need be, she or he may seek an effective remedy for the unlawful violation of privacy."[11] This aligns with the principles enshrined in Section 38 of the South African Constitution, which guarantees the right to an effective remedy.

International human rights bodies and experts, including the UN High Commissioner for Human Rights, have repeatedly underlined the significance of notification to ensure effective remedy of violations of the right to privacy.[12] Moreover, the UN Human Rights Committee in its Concluding Observations on the Eighth Periodic Report of Ukraine, regarding the International Covenant on Civil and Political Rights, stated that "The State party should bring its regulations governing data retention and access thereto, surveillance and interception activities into full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality, and necessity. It should ensure that (…) (b) persons affected are notified of surveillance and interception activities, where possible, and have access to effective remedies in cases of abuse".[13]

However, it is regrettably observed that Section 25A does not clearly delineate the procedure that individuals can go through once they have been notified. This is a significant omission, as it leaves individuals uncertain about how to address potential breaches of their rights.

To strike an appropriate balance between safeguarding investigations and ensuring access to effective remedies, **it is imperative to introduce a specific procedure within the new provision. This procedure**

[11] Constitutional Court of South Africa, *amaBhungane Centre for Investigative Journalism NPC and Sole v Minister of Justice and Correctional Services and Others; Minister of Police v amaBhungane Centre for Investigative Journalism NPC and Others [2021] ZACC 3*, para 45.
[12] *The right to privacy in the digital age*, UN Doc. A/HRC/27/37, 30 June 2014, para 47; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/HRC/23/40, 17 April 2013, para 82; Joint Declaration on Surveillance Programmes and Their Impact on Freedom of Expression, 21 June 2013, para. 5.
[13] UN Human Rights Committee, *Concluding Observations on the Eighth Periodic Report of Ukraine,* UN Doc CCPR/C/UKR/CO/8, November 2021.

should outline the steps an individual can take following notification, facilitating their ability to seek redress for any unlawful infringement upon their privacy.

In conclusion, while the new RICA proposed amendment represents progress in terms of transparency and accountability, it falls short in providing clear guidance on how individuals can address grievances once they have been notified. By implementing a well-defined procedure for this purpose, we can establish a framework that appropriately balances the interests of protecting investigations and providing effective remedies, in accordance with international standards.

c. Enhancing clarity and security in notification procedures: defining format and content.

An essential aspect that requires attention within the new RICA amendment is the way individuals will be notified, along with the content of these notifications. Currently, the amendment is lacking in specificity in these crucial areas, which creates uncertainty and potentially exposes individuals to security threats.

To address these issues effectively and ensure consistency and security standards, it is crucial for the law to define the process, format, and content of the notifications. These provisions should be structured in a manner that prioritizes the safeguarding of sensitive information. Neglecting to do so could potentially result in security threats, including the leakage of information and the potential misuse of such sensitive data. Also, these provisions should ensure that individuals are adequately informed of the relevant details.

Regarding the format of notifications, it is essential to be prescribe a standardized, secure, and confidential means of communication. Moreover, defining the content of notifications is equally important. At the very least, notifications should include information allowing individuals to seek remedies in cases of abuse.

In conclusion, addressing the format and content of notifications within the new RICA amendment is imperative to provide clarity and security for all parties involved**. By establishing clear standards and guidelines for notification procedures, we can bolster the effectiveness of the amendment while safeguarding individuals' rights and minimizing potential security threats.**

3. Enhancing the independence and accountability of designated judges: proposals for strengthening safeguards and oversight

Preserving the absolute independence and integrity of the designated judge is of utmost importance, particularly in the context of inherently secretive surveillance processes. Although the proposed amendment has taken steps to introduce certain safeguards to reinforce the independence of this judge, there remains room for further enhancements in the interest of strengthening these protections.

a. Enhancing judicial independence in designation: proposing joint appointment of judges.

Section 15A(b)(2) stipulates that the Minister of Justice must designate a judge as outlined in subsection (1) after consultation with the Chief Justice. While this represents an improvement by moving away from the notion of sole appointment by an executive authority, there is a concern regarding the phrase "in consultation". This wording may imply that the Chief Justice's opinion is merely advisory and not binding. In *Zakharov* case, the European Court referred to approval of authorisation by a non-judicial authority "provided that that authority is sufficiently independent from the executive".[14]

Therefore, **we propose amending the language to state that both the Minister and the Chief Justice shall jointly designate the judge or if suggestion below accepted at the designation of the panel of judges**. This modification would more explicitly emphasize a mutually accountable decision-making process.

b. Workload and independence of designated judges: proposing a panel approach.

The new requirements introduced in the amendment, such as the user notification requirement and the need to provide, along with monitoring subpoenas for communication-related information issued under Section 205 of the Criminal Procedure Act, may potentially result in a significant increase in the workload of the designated judge. This surge in responsibilities could lead to an overload of the system, where a single judge is tasked with making critical decisions in a context where timely decision-making is of utmost importance.

[14] ECtHR, *Zakharov v Russia*, App No 47143/06, Judgment, 4 December 2015, para 260.

In line with international standards, particularly the UN General Assembly Resolution on the Right to Privacy in the Digital Age,[15] it is imperative that the designated judge's office is adequately resourced and staffed to meet these heightened demands. This resolution emphasizes the necessity of establishing or maintaining "independent, effective, adequately resourced, and impartial judicial oversight mechanisms for surveillance" is critical. **Therefore, our proposal is to consider the formation of a panel of judges to distribute the workload, thereby enhancing efficiency while maintaining the required level of independence and impartiality.**

c. Strengthening surveillance oversight: proposals for enhanced transparency and reporting.

To reinforce the independence and accountability of the designated judge(s), it is vital to establish a robust reporting function within RICA. The Bill envisions that all interception requests will be assessed by a single designated judge and appoints a review judge to evaluate each decision made by the Rica judge based on the same set of facts. This approach does not effectively address the issues identified by the court or enhance oversight. This system remains limited in terms of judicial oversight.

The current absence of specific reporting obligations undermines transparency and oversight. The Designated Judge(s) should be subject to explicit transparency obligations. Reports generated by the designated judge(s) should include essential information to shed light on the surveillance process, including:

- The purpose of the warrants issued.
- The number of individuals affected by the warrants.
- The alleged offenses under investigation.
- Details regarding the technology and methods employed in surveillance.
- Statistics on the outcomes of surveillance, including the number of interceptions leading to arrests and convictions.

International law aligns with the necessity for independent and effective oversight. Both the Special Rapporteur and the UN High Commissioner for Human Rights have consistently emphasized that surveillance should only be conducted with proper oversight.

As the UN High Commissioner for Human Rights noted, effective oversight should ensure that:

> Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources.

[15] UN Doc *A/RES/69/166*, 18 December 2014.

> Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance, and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies, and they should be required to keep records of all surveillance measures taken. Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review.[16]

Effective oversight cannot be limited to an automatic and superficial review of the reported interferences, without the ability to review all available information and authority to issue binding decisions.

4. Closing the section 205 loophole: ensuring comprehensive safeguards in surveillance legislation for the protection of human rights

While the recent amendments have made strides in addressing certain systemic flaws with RICA, there remain significant issues that demand attention, pivotal for safeguarding human rights in surveillance cases. These issues, although not explicitly raised by the High Court, bear fundamental importance in ensuring a fair and rights-respecting surveillance framework.

One paramount concern left unaddressed in the proposed amendment is the failure to close the Section 205 loophole. This issue stems from the fact that, in most cases, the state accesses an individual's sensitive communications data through a separate legal avenue, distinct from RICA - namely, Section 205 of the Criminal Procedure Act. Unlike RICA, Section 205 permits access to archived communications data related to any criminal matter without the need for authorization by a designated judge, thereby establishing a lower standard of oversight, just to name some examples. This omission raises legitimate concerns regarding potential law enforcement abuses, as documented by Intel Watch.[17]

[16] UN OHCHR, *Report on the right to privacy in the digital ag*e, UN Doc A/HRC/39/29, 3 August 2018, para 40. See also ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, App No 62540/00, Judgment, 28 June 2007, para 85.

[17] Intel Watch, Reforming Communication Surveillance in South Africa, Understanding the section 205 'loophole' https://intelwatch.org.za/2023/05/30/reforming-communication-surveillance-in-south-africa-in-the-wake-of-amabhungane/

From a right-to-privacy perspective, there exists no fundamental distinction in the manner of accessing communication data. Furthermore, it's imperative to note that the safeguards governing metadata usage are notably less stringent under the Criminal Procedure Act compared to RICA.

Crucially, communications data, including metadata, holds exceptional sensitivity, with its collection constituting a profound invasion of the fundamental right to privacy. Metadata, often overlooked as mere technical information, possesses the capacity to unveil significant facets of an individual's private life.[18] Governments can leverage this information not just for prosecuting specific offenses but also for creating comprehensive profiles of individuals. These concerns resonate with the Court of Justice of the European Union (CJEU), in Tele2/Watson, regarding communications data retention, which concluded that the distinction between content and communications data or traffic data is, in fact, no longer fit for purpose.[19]

To adequately mitigate these risks, it is of utmost importance to guarantee that the legislative framework in question, RICA, incorporates measures that effectively eliminate any potential loopholes that render safeguards under the Act illusory. The objective should be to ensure that the framework with the highest level of safeguards takes precedence, and in this case, that framework is RICA.

5. Enhancing Safeguards for Journalists, Lawyers, and Civil Society: Addressing Gaps

The Constitutional Court ruling declared that RICA was unconstitutional in cases involving practicing lawyers or journalists, as it lacked additional safeguards aimed at minimizing the risk of violating attorney-client confidentiality and journalist-source **confidentiality. The proposed amendment attempts to rectify this deficiency by** introducing some protective measures, albeit with certain weaknesses.

A specific section from the Constitutional Court judgment, pertaining to the suspension period of the judgment, is reproduced in the Bill. The insertion states the following:

[18] PI, *Video explaining Metadat*a, https://www.youtube.com/watch?v=xP_e56DsymA; EFF, Why metadata matters, 7 June 2013, https://www.eff.org/deeplinks/2013/06/why-metadata-matters; PI, How intrusive is communications data?, 21 August 2019, https://privacyinternational.org/long-read/3176/how-intrusive-communications-data.

[19] CJEU, Joined cases *Tele2 Sverige AB v Post-och telestyrelse*n and *Secretary of State for the Home Department v Tom Watson*, Cases Nos C–203/15 and C–698/15, Judgment, 21 December 2016, paras 99-101; CJEU, Joined cases *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others*, Cases Nos C-293/12 and C-594-12, Judgment, 8 April 2014, para 27.

> 23A. (1) Where the person in respect of whom a direction, extension of a direction or entry warrant is sought in terms of section 16, 17, 18, 19, 20, 21, 22 or 23, whichever is applicable, is a journalist or practising lawyer, the application must disclose to the designated judge the fact that the intended subject of the direction, extension of a direction or entry warrant is a journalist or practising lawyer.
>
> (2) If the designated judge issues the direction, extension of a direction or entry warrant, she or he may do so subject to such conditions as may be necessary, in the case of a journalist, to protect the confidentiality of her or his sources, or, in the case of a practising lawyer, to protect the legal professional privilege enjoyed by her or his clients.''.

However, a critical clause has been omitted from the proposed Bill, which significantly impacts the level of protection provided. The Constitutional Court had underlined that:

> (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 practicing lawyer.[20]

The proposed Bill does not provide for such requirement. This omission signifies that the protection afforded by the proposed Bill is less robust than that provided by the Constitutional Court during the suspension period. The requirement for the judge to be satisfied that the direction is necessary sets a high standard for granting such directions.

In conclusion, while the proposed amendment makes efforts to address the concerns related to practicing lawyers and journalists, the omission weakens the protection provided. It is imperative to introduce this clause to ensure that the rights and confidentiality of these individuals are adequately safeguarded in line with constitutional principles.

The Constitutional Court did not address the question of protecting civil society however PI considers that the amendment should also include **enhanced protections for the communications between members of civil society groups and human rights defenders.** The knowledge that intelligence agencies may use their interception powers and capabilities to capture the communications of civil society organisations has a profound chilling effect on their exercise of freedom of expression. It endangers the public watchdog function of civil society organisations by undermining the way in which

[20] Constitutional Court of South Africa*, 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 [2021] ZACC 3*, p 80.

they operate. They report on human rights violations, illegalities, and other wrongdoings, both locally and worldwide. In order to do so, they rely on the willingness of others to pass them information in confidence, sometimes at their risk to their own lives. The knowledge that intelligence services may intercept those communications is bound to diminish that willingness of people in other countries will have to communicate with civil society. As sources of information dry up, civil society organisations are less likely to be able to report on human rights violations and other social issues and consequently, they will be less able to hold governments to account.

In other words, secret surveillance programmes dramatically undermine the protection of organisations' sources and their ability to carry out their work. If civil society organisations are to perform their public watchdog function, which the ECtHR itself has recognized in its jurisprudence,[21] they must be able, like journalists, to guarantee the anonymity of their sources and the confidentiality of their communications. The chilling effect of surveillance measures on the exercise of freedom of expression is not limited to NGOs or journalists.

In summary, it is essential for any surveillance legal framework to include at least special protections for the communications data of civil society organisations, similar to those enjoyed by lawyers and the press. In particular, the collection of these groups' personal data, including content data and metadata, should only be ordered by a judge, and be made subject to stringent requirements as regards access, permitted uses, preservation, retention and destruction of such data.

6. Addressing the issue of *ex-parte* decision-making in surveillance: The need for balanced oversight and the role of public defenders

The amendment bill introduces a review judge into the process. However, it is crucial to note that the presence of a review judge does not fully satisfy the *ex-parte* decision-making problem, as it does not constitute an adequate or suitable safeguard. Furthermore, it fails to introduce an element of inquiry and scrutiny. The Constitutional Court's order that Rica must "adequately provide safeguards to address the fact that interception directions are sought and obtained ex parte". The Constitutional Court found:

[21] ECtHR, *Vides Aizsardzības Klubs v Latvia*, App. No. 57829/00, Judgment, 27 May 2004, para. 42. See also more recently, ECtHR*, Szabó and Vissy v Hungary,* App No 37138/14, Judgment, 12 January 2016, para 38.

> […] the result is that an application for an interception direction that may severely and irreparably infringe the privacy rights of the subject is granted on the basis of information provided only by the state agency requesting the direction. The designated judge is required to issue the direction on the basis of that one-sided information. Save perhaps for relatively obvious shortcomings, inaccuracies or even falsehoods, the designated judge is not in a position meaningfully to interrogate the information.[22]

The problem observed by the judge, as described, appears to be related to a one-sided process that restricts or hinders the concept of oversight. In these circumstances, there is no compelling reason to believe that having two judges operating on an *ex-parte* basis will be less prone to making erroneous decisions than one. This is because both judges will still be relying on the same one-sided, confidential evidence. The core issue that must be addressed is that the judge(s) involved do not have the opportunity to hear the opposing side of the argument. This omission undermines the fundamental principle of *audi alteram partem* which dictates that both sides should be heard and equality of arms which involves a fair balance of power or resources between the parties involved in a legal process.

Moreover, it is important to recognize the significance of having a public defender who can access the information and contribute to a more thorough and balanced assessment of the case by representing the interests of the individual subject to the surveillance measure, different jurisdictions have used this approach in order to ensure the right to a fair hearing in secret or security-related proceedings: these include the European Court of Human Rights, Canada, Hong Kong, New Zealand, Australia, and the United Kingdom.[23]

The presence of a public defender can substantially enhance the fairness and transparency of the process, aligning it more closely with the principles of an adversarial system. Therefore, it is disappointing that the Bill does not adequately grapple with this problem and fails to consider the international progress made in addressing it.

---

[22] [22] Constitutional Court of South Africa*, 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 [2021] ZACC 3*, para 93.

[23] C Kruyer, *Reforming communication surveillance in South Africa: recommendations in the wake of the amaBhungane judgment and beyond,* Johannesburg, Intelwatch & Media Policy and Democracy Project, 2023; H Swart, Supplementary *report: Understanding the section 205 loophole*, Intelwatch, 2023.