IPPR

MARCH 2024

NO PRIVACY, GUARANTEED

Namibia's mass surveillance framework is flawed and prone to abuse

COMPILED BY FREDERICO LINKS

EXECUTIVE SUMMARY

On 9 November 2023, which was the last day of its 77th ordinary session, held at Arusha, Tanzania, the African Commission on Human and Peoples' Rights (ACHPR) issued Resolution 573.

With Resolution 573, "on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa", the Commission expressed concern at "the unrestrained acquisition of communication surveillance technologies by State actors without adequate regulation" and the "lack of adequate national frameworks on privacy, communication surveillance and the protection of personal data".

The Commission also expressed concern "about the prevalence of mass surveillance and unlawful targeted communication surveillance that does not conform with international human rights law and standards, and the disproportionate targeting of journalists, human rights defenders, civil society organizations, whistleblowers and opposition political activists, without appropriate safeguards for privacy rights".

The resolution calls on states to take steps to adequately regulate communications surveillance by introducing measures and mechanisms that conform with the guidance provided by the Declaration of Principles on Freedom of Expression and Access to Information in Africa (the Declaration), as well as international human rights law and best practice.

In the wake of the adoption of Resolution 573, the Media Institute for Southern Africa (MISA) hailed it as a wake-up call and noted that state surveillance was "a massive threat to freedom of expression in the region" and that governments "must be more transparent in deploying surveillance equipment and the information they seek".

Similarly, the Centre for Human Rights, at the University of Pretoria, welcomed Resolution 573 as a "landmark resolution" that was "a significant step by the African Commission in recognising the importance of human rights protection in an increasingly interconnected world, particularly the need to safeguard privacy rights in the face of evolving technological advancements".

The adoption of Resolution 573 comes literally on the eve of Namibia implementing its own mass surveillance facilitating framework via regulations bringing into force Part 6 of Chapter V of the Communications Act 8 of 2009. The resolution thus presented an opportunity to benchmark the emerging Namibian communications surveillance framework against the 5-point call of Resolution 573, which derive from the Declaration of Principles on Freedom of Expression and Access to Information in Africa, as well as international human rights law and best practice.

This benchmarking clearly shows that the Namibian communications surveillance framework is substantially flawed and does not meet the standards set by the Declaration, nor international human rights law and/or best practice, whether on the African continent or elsewhere.

Given this, the imposition of the Namibian communications surveillance framework – which comes into full force on 1 April 2024 – on society heightens serious and urgent human rights concerns, specifically around the nature of the threat posed to the constitutionally enshrined right to privacy (Article 13), as well as free expression and media freedom, and by extension and implication also the maintenance of democracy.

Ultimately, given the graveness of the emergent threat, this brief recommends that Namibia change course and proposes pathways for such a course correction.

This brief 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 (grant no. GP/400069), through the College of Social and Political Sciences at the University of Glasgow.

INTRODUCTION

On 1 April 2024, enhancements to Namibia's communications surveillance framework come into full effect.

These enhancements come about through mandatory SIM card registration regulations gazetted in March 2021 and mandatory data retention regulations gazetted in April 2022 by the Minister of Information, Communication and Technology (MICT). The regulations bring into force Part 6 of Chapter V of the Communications Act 8 of 2009. Part 6 of Chapter V of the law deals specifically with the interception and monitoring of digital communications of all sorts.

These regulations not only bring into force Part 6 of the Communications Act, but also constitute the legal basis for mass or bulk communications surveillance.

What is mass surveillance?

Mass surveillance is indiscriminate surveillance. Mass surveillance uses systems or technologies that collect, analyse, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing. Under currently available forms of mass surveillance, governments can capture virtually all aspects of our lives.

– Mass Surveillance, Privacy International

The Namibian communications surveillance framework consists of the Namibia Central Intelligence Service Act 10 of 1997 and the Communications Act 8 of 2009, and its regulations.

It needs spotlighting that the new reality of perpetual mass communications surveillance that will be in force as from April 2024 will have a tremendous impact on the right to privacy – and associated human rights – and heralds a critical era for Namibian democracy.

It is against this backdrop that the African Commission on Human and Peoples' Rights (ACHPR) Resolution 573, on "the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa", and which comes at an opportune moment for Namibia, is used in this briefing paper to assess to what extent the emergent Namibian mass communications surveillance dispensation constitutes a threat to human rights in the Namibian context. Resolution 573 draws significantly from and rests on the Declaration of Principles on Freedom of Expression and Access to Information in Africa (the Declaration).

To be clear, this brief, as illustrated in the following sections, clearly asks to what extent the Namibian communications surveillance framework aligns specifically with the guidance provided in Principle 41 (Privacy and communication surveillance) of the Declaration. Other principles directly and indirectly implicated by Resolution 573 are principles 20, 25 and 40.

The 5-point call of Resolution 573 of the African Commission on Human and Peoples' Rights (ACHPR)

The African Commission calls on States Parties to:

1. Ensure that all restrictions on the rights to privacy and other fundamental freedoms, such as freedom of expression, freedom of association and freedom of assembly, are necessary and proportionate, and in line with the provisions of international human rights law and standards;
2. Align approaches on the regulation of communication surveillance with relevant international human rights law and standards, considering safeguards such as the requirement for prior authorization by an independent and impartial judicial authority and the need for effective monitoring and regular review by independent oversight mechanisms;
3. Only engage in targeted communication surveillance that is authorized by law, that conforms with international human rights law and standards, and premised on reasonable suspicion that a serious crime has been or is being carried out;
4. Promote and encourage the use of privacy-enhancing technologies and desist from adopting laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localization requirements, unless such measures are justifiable and compatible with international human rights law and standards;
5. Ensure that victims of violations arising from arbitrary surveillance measures have access to effective remedies and take specific measures to investigate and prosecute cases of illegal and indiscriminate surveillance.

Done in Arusha, Tanzania, 09 November 2023

DOES THE NAMIBIAN COMMUNICATIONS SURVEILLANCE FRAMEWORK ALIGN WITH THE AFRICAN COMMISSION DECLARATION AND RESOLUTION 573?

The responses to the questions in the following sections are taken verbatim from an unpublished report of an assessment of the Namibian communications surveillance framework conducted by South Africa based ALT Advisory, a public interest advisory firm, in October 2022 for the Institute for Public Policy Research (IPPR).

Does the Namibian framework ensure that all restrictions on the rights to privacy and other fundamental freedoms, such as freedom of expression, freedom of association and freedom of assembly, are necessary and proportionate, and in line with the provisions of international human rights law and standards?

No, it does not.

Best practice dictates that the privacy violations inherent to communication surveillance demand that these powers be exercised only when necessary to responding to the most severe crimes and threats to safety and security, and only where less intrusive measures have failed. These elements are lacking or at best inconsistently applied in the Namibian framework.

The Namibia Central Intelligence Service Act establishes that the grounds for a judge to authorise interception are that: "the gathering of information concerning a threat or potential threat to the security of Namibia is necessary to enable the Service to properly investigate such threat or potential threat *or* to effectively perform its functions in terms of section 5 of this Act or any other law…" (Emphasis added.)

In respect of the first clause, it is notable that the NCIS may seek to use interception in respect of any threat or potential threat, where the principle of proportionality suggests that more intrusive measures should be reserved only for serious or imminent threats. The deficiency is deepened in the second clause, which also gives grounds for the Service to use interception to effectively perform any of its broader functions, outlined in section 5 of the Act, which are not confined to combating serious or imminent security threats.

Regarding access to communications data, the Regulations do not restrict this avenue to investigations of more serious offences or security threats, suggesting that data may be sought even for minor offences. The Regulations also require only that the information be "relevant" to an investigation, rather than necessary, and only that it would not be "expedient" to seek the information through other means.

Does the Namibian framework align approaches on the regulation of communication surveillance with relevant international human rights law and standards, considering safeguards such as the requirement for prior authorization by an independent and impartial judicial authority and the need for effective monitoring and regular review by independent oversight mechanisms?

Only partially.

On the issue of safeguards "such as the requirement for prior authorization by an independent and impartial judicial authority":

The Regulations make provision for the Namibian Police Force to access customer information without court authorisation in urgent situations. Regulation 5(7) of the 2021 Regulations provide that:

> "An authorised officer must also provide stored information if he or she is requested to provide stored information by a member of the Namibian Police Force if the authorised officer on reasonable grounds belief *[sic]* that information is required urgently and the delay in obtaining a request referred to in sub-regulation (1) *[namely, for judicial authorisation]* would defeat the purpose for which the request is made and that a request would have been granted if it had been made."

Though the Regulations do not define "authorised officer", this is understood in context to mean an "authorised staff member", which the Regulations define as an employee of a telecommunications service provider who is delegated to liaise with law enforcement and intelligence agencies' requests for customer information or communication data. The Regulations define "stored information" to mean customer information that the service provider collects when registering a SIM card, which does not include communications-related information.

The approach outlined in the regulations presents several problems. First, it is unusual in that it places the decision-making responsibility on the telecommunications service provider, or more specifically on a specific staff member of the service provider, to decide if an urgent request for customer information meets the necessary conditions. This is a significant power to delegate to a private individual of unknown training or qualifications. The regulations provide that service providers designate which staff members who will function as "authorised staff members", either individually or by virtue of their position

in the organisation, and the service provider must share their names and particulars with the Communications Regulatory Authority of Namibia (CRAN).

However, there are no further criteria for the qualifications, training, or competency of authorised staff members. As employees of private companies, they are also not subject to the statutory or public accountability mechanisms that would ordinarily apply to members of the police, judicial officers, or other government officials. These combine to create poor safeguards for privacy, and limited recourse and accountability if the power is misused.

Second, irrespective of where the authority is delegated, the provision for warrantless access to customer information creates its own inherent risks which must be addressed. These include that the provision undermines the authority of the courts and creates an avenue for law enforcement agencies to access sensitive information without the important safeguard of judicial authorisation. Even if the decision-making power were delegated to a higher authority, such as a more senior police official or the service provider's in-house legal counsel, the grounds for sidestepping court authorisation lack a key element of proportionality. Namely, while it is provided that the information must be required urgently, it is not provided that the request must be of suitable *importance* to justify a deviation from the usual safeguards, such as emergency police action to prevent loss of life or serious injury.

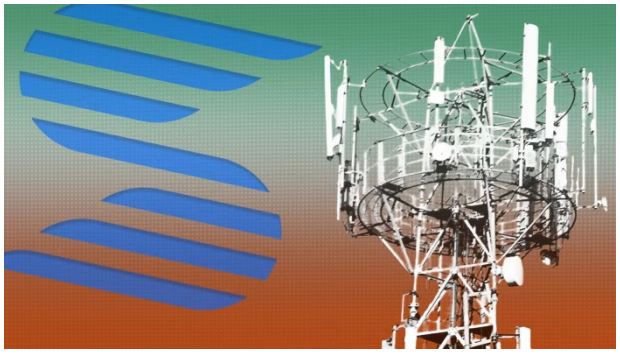
Third, the provision lacks additional safeguards to limit misuse. These may include a requirement that any emergency request to access customer information must be followed by a formal notice to the relevant judicial body which provides all details of the request, so that any use of the provision is at least subject to scrutiny after the fact and any misuse can be subject to appropriate action. It is recommended that this reporting duty should apply to both parties, to offset any risk of under-reporting.

On the issue of "the need for effective monitoring and regular review by independent oversight mechanisms":

While the general requirement for a judge to authorise interceptions and metadata access should be welcomed, the framework lacks several key provisions for robust and independent oversight.

For example, the framework does not make provision for specialist judges or courts to oversee these decisions, which would help ensure judicial oversight that is conversant in the specific legal and technical questions related to communications surveillance and human rights, and adequately resourced for this function.

The oversight falls short of the test, established by the South African courts in *amaBhungane,* for decisions that afford the right to a fair trial. In those proceedings, the court found that the South African Parliament must amend the law to account for the one-sided nature of interception decisions, which may call for the introduction of a 'public advocate', a panel of judges, or other safeguards.



Does the Namibian framework ensure that the state only engage in targeted communication surveillance that is authorized by law, that conforms with international human rights law and standards, and premised on reasonable suspicion that a serious crime has been or is being carried out?

No, it does not.

The regulations of Part 6 of Chapter V of the Communications Act 8 of 2009 are intended to facilitate mass communications surveillance through mandatory SIM card registration and data retention.

Regarding access to communications data, the regulations do not restrict this avenue to investigations of more serious offences or security threats, suggesting that data may be sought even for minor offences. The regulations also require only that the information be "relevant" to an investigation, rather than necessary, and only that it would not be "expedient" to seek the information through other means.

The framework requires mandatory registration of SIM cards. Despite its prevalence in many parts of the Global South, this policy trend has been subject to robust criticism from human rights groups and other expert bodies. While the dominant rationale for SIM registration is that it assists in detecting and investigating crimes and security threats related to the use of ICTs, there is no clear empirical evidence that SIM registration policies lead to a reduction in crime.

On the other hand, privacy advocates link SIM registration policies to an increased risk of identity theft, both by requiring the collection of detailed identity-related information for millions of communications users and by incentivising professional criminals to secure fraudulently registered SIM cards. Mandatory SIM registration also impacts communication privacy, by mandating that a person's identity is linked to their communication; this raises special implications for groups who are considered more vulnerable to communications surveillance or who have a particular need for confidential or anonymous communications, such as journalists or whistleblowers.

SIM registration policies are also considered to be harmful to digital inclusion, as they create an additional barrier to connecting people to ICTs, especially in more marginal communities that are less likely to have access to identity documentation. As SIM registration policies also create

costly obligations for communications service providers, including the cost of additional staff and systems for registration and record-keeping costs, these policies are also linked to likely increases in the costs of communication, and other economic harms.

In sum, SIM registration policies are linked to a range of harms while there is significant doubt that they fulfil their central policy objective of combatting crime. The absence of clear necessity and proportionality calls into question the rationality of mandatory SIM registration for Namibia.

Does the Namibian framework promote and encourage the use of privacy-enhancing technologies and desist from adopting laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and data localization requirements, unless such measures are justifiable and compatible with international human rights law and standards?

No, it does not.

In fact, the stated aim of the regulations is to undermine privacy and anonymity online and in communications. This was explicitly and clearly articulated in a media release issued by the Ministry of Information, Communication and Technology (MICT) on 26 October 2021, which stated that the benefit of the regulations on SIM card registration was that "it eradicates anonymity of communications".

Also, the Namibian framework mistakenly assumes that communications data is less sensitive than the content of communications, and accordingly provides fewer protections and safeguards for its access. This is out of keeping with international best practice, which call for all forms of communication data to be subject to the same rigorous protections and safeguards against access.

The harm is magnified by the extraordinary *length* for which communications data must be stored in terms of the Namibian framework – it mandates the storage of communications data for five years.

Does the Namibian framework ensure that victims of violations arising from arbitrary surveillance measures have access to effective remedies and take specific measures to investigate and prosecute cases of illegal and indiscriminate surveillance?

No, it does not.

Namibia's interceptions framework lacks user notification, which provides that any person whose communications and communication data is intercepted or accessed is generally notified after the fact, except where the notification must be delayed to preserve an ongoing investigation. User notification is a key safeguard established in the Declaration of Principles on Freedom of Expression and Access to Information in Africa, the international Necessary and Proportionate principles, and many international jurisdictions, including South Africa following the Constitutional Court's judgment in *amaBhungane*

The Namibian framework lacks other important transparency and oversight measures, for example, a requirement for law enforcement and intelligence agencies, and judicial bodies, to submit regular, detailed, public reporting on their activities relating to interception and access to communication data, including statistical breakdowns of how many interception and access decisions are requested, authorised, refused, and renewed; across which agencies; and for what purposes and investigations. This form of reporting is regarded as a key enabler of public and legislative oversight of surveillance operations and can be accomplished without harming sensitive investigations.

There is also a notable lack of other oversight measures and ombudsman offices with the power and mandate to receive and investigate citizens' complaints of surveillance abuses and other abuses of power within the intelligence and law enforcement agencies, such as a body of Parliament, or a civilian intelligence ombud.

RECOMMENDATIONS

The following recommendations are taken verbatim from the unpublished report mentioned earlier and compiled for the Institute for Public Policy Research (IPPR) by ALT Advisory, a South Africa-based public interest advisory firm.

Considering the significant gaps and challenges in Namibia's framework for communications surveillance, a full reform process is recommended to provide better protections and safeguards for communications and communication data, drawing on developing guidance, standards and best practice internationally and in the region:

- The framework must be subject to clearer standards of necessity and proportionality, so that communications surveillance may only be conducted on narrowly defined grounds, where necessary for investigations of serious offences and imminent threats to national security or human life, and where less intrusive measures have failed or are not possible;
- The framework should ensure robust and independent judicial oversight of surveillance powers, by providing for specialist judges, with adequate independence and resourcing to fulfil their mandate. The process of judicial oversight must also provide due process for targets of surveillance, in the context of ex parte hearings;
- The framework must provide for user notification, in order for people whose communications or communications data are intercepted or accessed are informed of any potential infringement of their rights so that they can seek recourse;
- The framework must provide for transparency measures across all agencies, oversight bodies, and industry stakeholders involved in communications surveillance, including the publishing of regular transparency reports which disclose statistical information about interceptions and access to communication data;
- All standards and safeguards that apply to the interception of communications, inclusive of the recommended reforms, must apply to all forms of communication data, including historical data;
- Policies relating to the storage of communications data and mandatory SIM registration should be withdrawn and reviewed in their entirety, and subject to an evidence-based approach that considers any privacy and data protection risks, the cost of the policy and its impact on digital innovation and connectivity, the capacity and needs of law enforcement, and appropriate safeguards and oversight measures; and
- These recommendations necessitate wide-ranging amendments to Part 6 of the Communications Act, sections 24-28 of the Namibia Central Intelligence Act, and the relevant Regulations issued under the Communications Act.

About the Author

Frederico Links

Frederico Links is a Namibian journalist, researcher, trainer and freedom of expression advocate. As a researcher he is mostly affiliated with Namibia's leading independent think-tank, the Institute for Public Policy Research (IPPR), where he coordinates a number of projects. In both his journalism and research, Links has a strong focus on good governance, human rights (including digital rights), state surveillance, corruption, rule of law, and transparency and accountability.

About the Institute for Public Policy Research (IPPR)

The Institute for Public Policy Research (IPPR) was founded in 2001 as a not-for-profit organisation with a mission to deliver, independent, analytical, critical yet constructive research on social, political and economic issues that affect development Namibia. The IPPR was established in the belief that development is best promoted through free and critical debate informed by quality research.

The IPPR is independent of government, political parties, business, trade unions and other interest groups.

Anyone can receive the IPPR's research free of charge by contacting the IPPR at the contact details below. Publications can also be downloaded from the IPPR website.

Institute for Public Policy Research (IPPR)
House of Democracy
70-72 Frans Indongo Street
PO Box 6566
Windhoek, Namibia
info@ippr.org.na
http://www.ippr.org.na

Incorporated Association Not for Gain Registration Number 21/2000/468
Directors: M M C Koep (Chairperson), D Motinga, A. Du Pisani, J Ellis, G Hopwood (ex-officio)