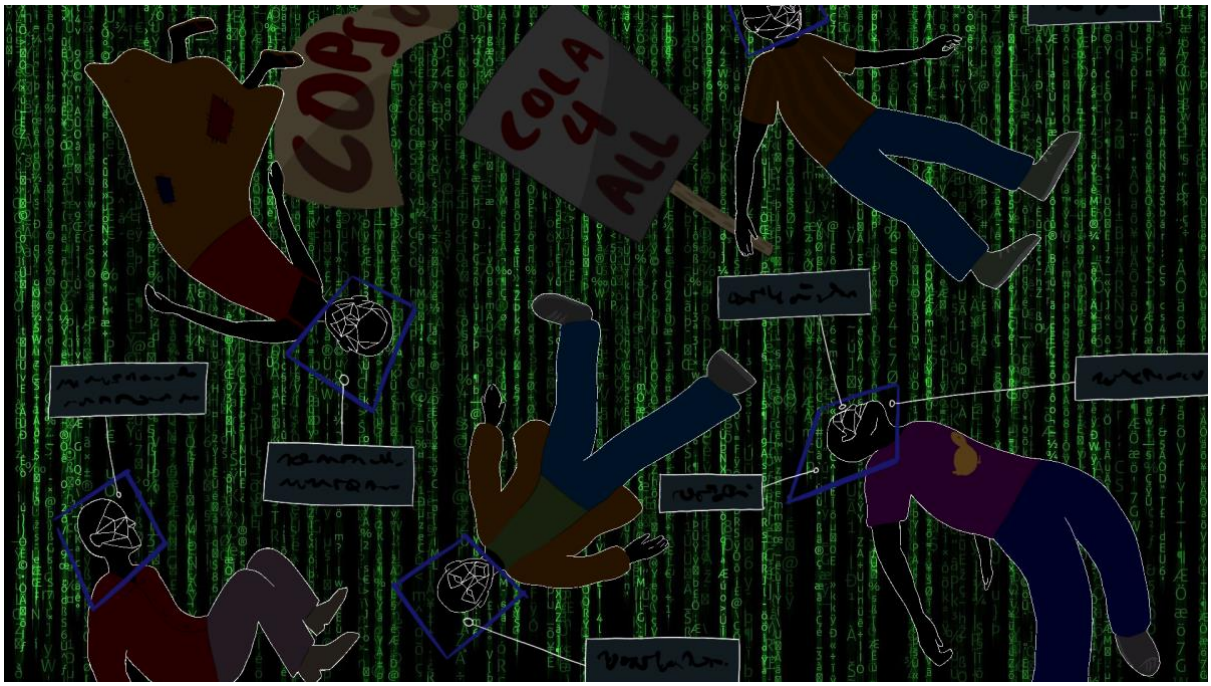
Policy Brief.

Not fit for purpose: Zimbabwe's Interception of Communications Act (ICA).

Allen Munoriyarwa, April 2024.



An emerge showing how dragnet surveillance operate. The image is accessible here**:** **https://images.app.goo.gl/LLqC73JaKrzfi1gy7.**

Table of contents

Dr Allen Munoriyarwa, Senior Lecturer in the Department of Media Studies at the University of Botswana, prepared this policy brief. **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.***

The brief also draws on the work produced over several years by the Media Policy and Democracy Project, a joint project of the Department of Communication and Media at the University of Johannesburg and the Department of Communication Science at the University of South Africa. It also draws on the research published here: https://doi.org/10.1093/slr/hmae018.

Executive summary

This policy brief examines the Interception of Communication Act (ICA) regulation passed by the Zimbabwean parliament in 2007. It outlines the defects of this Act, compares it to globally acceptable surveillance practices, and makes policy recommendations. A major point to note is that the ICA generally favours bulk data collection in the name of state security.

. Another central point to note is that the ICA does not protect specific communities of practice that, in some democratic regimes, are excluded from surveillance for them to undertake their critical roles in society. For instance, there are no proactive mechanisms and regulations that protect important communities of practice like journalists and lawyers from surveillance. Yet, it is common knowledge that when lawyers are wantonly subjected to surveillance and communication interception, the client-attorney privilege practice is compromised, yet this constitutes the central lynchpin of the legal profession.

This is equally true of journalists. They thrive on sources, and certain of their practices, like investigative journalism, depend on confidential sources and whistleblowers. Such sources are integral to journalism, especially in its execution of accountability. Zimbabwe's ICA does not offer such protection in any of its clauses. But this is not the only concern. Several other issues make this law inadequate in its approach to communication interception.

For instance, the law does not clearly define the processing of intercepted data. Every interception act should be premised on principles of transparency and fairness. Also, interception of communication should generally serve the public interest, such as fighting serious organised crime.

The ICA is not fashioned for this, judging by its crucial interception mistakes. What makes this worse is the absence, within the law, of clarity on how the process of interception will

be carried out if surveillance has been carried out the way it was initially set out, and within the confines of human rights like privacy. In other words, ICA lacks built-in mechanisms that ensure that interception is done within the confines of necessity concerning the purpose of interception.

General recommendations

Zimbabwe's Interception of Communications Act (2007) requires substantial redrafting to align with the country's Constitution and global surveillance standards. In its current form, the law is defective on many levels. There is a need for parliament to redirect its effort to reforming the law so that it meets the following, among other issues:

- Establishment of an independent board that oversees surveillance.
- Provide further clarity on how journalists and lawyers should be protected from surveillance.
- Make the sanctions available for abuse of people's data explicitly clear.
- The law should expressly include a surveillance supervisory authority independent of the Executive.
- ICA should quickly be harmonised with the 2013 Constitution and all inconsistent sections of the Act struck off.

Global standards of surveillance and interception

(a). Parliamentary committee oversight

There are many ways of ensuring parliamentary oversight. These include ad-hoc parliamentary committees, plenary debates, and question and answer sessions with the responsible ministers. A generally acceptable way is establishing a parliamentary committee that ensures continuous and comprehensive oversight.

(b). Clarity on the powers of institutions engaged in surveillance. Best practices insist on these powers being explicit within the law.

(c). Specific sanctions for violation. Specific sanctions should be imposed for violating interception regulations. This is often meant to discourage actors from acting in their own interest, in the interest of malicious forces, or in their own malice.

(e). Judicial oversight: Judicial oversight is increasingly becoming a best practice norm in the regulation of interception. In jurisdictions where judicial oversight is exercised, Interception Judges have been appointed to dis/approve applications for interception.

Introduction: Thinking about privacy and interception in Zimbabwe

The Zimbabwe parliament passed the Interception of Communications Act (ICA) in 2007. In 2013, the country passed a new Constitution through a public referendum, with an expanded Bill of Rights. The consultations over the ICA Bill, leading up to the enactment of the law, were acrimonious and controversial. Concerned Civil Society Organisations (CSOs) and Non-Governmental Organisations (NGOs) argued that the process of consultations by the parliamentary committee was superficial and window-dressing. It was not meant to accept opposing views, incorporate them and improve the bill before it became law. The

consultations that were held were often poorly attended and some attendees had the least understanding of the provisions of the bill.

Critical CSOs like Veritas, Zimbabwe Lawyers for Human Rights (ZLHR), MISA and Zimbabwe Union of Journalists (ZUJ) had their submissions taken in but rarely made it in the final piece, which was ascended into law by the then President and low late Robert Mugabe.

Overview of the 2007 Interception of Communication Act

There needs to be faster progress in enacting an interception of communications framework in Zimbabwe relative to other countries. By 2007, when Zimbabwe passed ICA, most countries in the world, especially the WEIRD countries (Western Educated Industrialised, Rich and Democratic), had already passed a plethora of communication interception regulations as a response to the September 11 attacks.

These legislations were, therefore, part of a multi-pronged fightback against terrorism. Against this background, the ICA was also promulgated, even though Zimbabwe joined later than most countries in terms of regulating the interception of (electronic) communication.

The adoption of the ICA in Zimbabwe was an opportunity for the country to join other League of Nations in acknowledging terrorism as a global challenge and in setting clear parameters on issues of national security and preserving the constitutionally guaranteed rights.

What was and is still controversial is the extent to which governments were willing to limit these rights. In the context of Zimbabwe, the Act must be understood in the context of various political developments that have impacted and implications for national security in Zimbabwe since the turn of the millennium.

In 2000, a violent land reform programme gripped the country, led by Zanu PF supporters and former liberation war veterans. The reform programme unleashed a wave of political violence across the country and, with the violence, attendant state-sanctioned human rights abuses.

The violent land reform programme triggered a severe economic crisis characterised by shortages of basic commodities, high inflation, and unemployment. This crisis, in turn, triggered a wave of protests and violent demonstrations, riots, mass protests, vicious electoral contestations, and other acts of political and economic subterfuge.

To some, the increase in state security-related legislation has followed the degeneration of internal political dynamics, characterised by fierce political contestations between the governing Zanu PF party, opposition political parties, and other civil society movements. The law's key provisions include, among others, the following, which we consider to be key and consequential to this law.

Section 6(1) of the ICA provides that:

A warrant shall be issued by the Minister to an authorised person …if there are reasonable grounds for the Minister to believe that:

> *(a) any of the following offences has been or is being or will probably be committed (i) a serious offence by an organised criminal group;*
>
> *(b) … the gathering of information concerning an actual threat to national security or to any compelling national economic interest is necessary;*
>
> *(c) The gathering of information concerning a potential threat to public safety or national security is necessary*[1]*.*

[1] The Interception of Communications Act [Chapter 11:04] section 6.

The legal defects of the ICA clauses

ICA is defective in several ways, especially in treating journalists and lawyers in Zimbabwe. These two communities of practice are mentioned because they are integral to any democracy or to any efforts to build a democratic dispensation through their professions.

In this regard, the Act is defective in the following ways.

(a). Dragnet surveillance: The problem with dragnet surveillance is that it targets people under suspicion and those who are not suspected of any wrong-doing. The overall effect of this is that it turns everyone into a potential criminal.

Dragnet surveillance has been justified in several ways by its advocates. By throwing the net out on everyone, the state/surveillers claim that they are making it hard for rogue criminal or terrorist elements to escape but engage in an egregious violation of privacy. There is also the unproven claim that law enforcement will generally not do anything with your data not unless you do something wrong. This is not true as the intention of dragnet surveillance is not always to fight crime, especially in regimes where political opponents have been persecuted, and where law enforcement are partisan.

(b). Absence of explicit protection for vulnerable communities of practice. The ICA should offer explicit protection for vulnerable communities of practice like journalists and lawyers. The question that should be asked about ICA, which it does not answer include: how are journalists' sources protected from surveillance? How is journalism itself as a central practice in the enjoyment of democracy, protected from intrusive surveillance? How are lawyers as well, protected? ICA is silent about these protections. When a law is silent about how it protects the vulnerable, it actually targets them by its silence.

(c). Absence of jurisdictional boundaries: The fact that dragnet surveillance allows law enforcement to run data queries and information would always be there should worry people about both accessibility and post-use storage. Without a corresponding capability to store the data, citizens run the serious risk of data exposures and criminal-masterminded hacks.

(d). The abrogation of the State's responsibility to protect. The primary responsibility of the State is to protect. The way the ICA is crafted makes it inevitable for the state to abrogate its responsibility to protect. This needs urgent reform in order to make the state responsive to its natural role of protecting citizens. The ICA, in its current form shirks away this responsibility because the State, instead of protecting citizens, exposes them to unmitigated surveillance. Yet, the obligation to protect binds under Section 2(2), 'every person, natural or juristic, including the State and all executive, legislative and judicial institutions and agencies of government at every level, and must be fulfilled by them'[2] . Therefore, the ICA needs to be recrafted to address this glaring inevitability.

Additional recommendations.

ICA should be amended to reflect the following:

(a) Judicial oversight

(b) Effective parliamentary oversight.

(c) Protection and proper disposition of intercepted communication. Currently, the law is silent about this.

(d) Post-surveillance notification is an important practice - where targets are informed post-fact for transparency.

Practical actions that should be considered immediately

- ICA should expressly affirm the rights of data subjects. In its current form, it is too broad in its inclusion of targets and has a chilling effect on journalism and law.
- There is an urgent need for a supervisory authority whose role and responsibilities are included in the law and guaranteed.

[2] Ibid at section 2(2).

- Post-surveillance notification should be included in the process of interception.
- There needs to be more clarity on who within the security agencies can be held responsible in the event of data leaks.
- The law should clarify offences, penalties, and fines in the event of data mismanagement within the security agencies.

Relevant readings

Brayne, S., 2020. *Predict and Surveil: Data, discretion, and the future of policing*. Oxford University Press, USA.

Hungwe, B & Munoriyarwa, A. (2024). An Analysis of the Legislative Protection for Journalists and Lawyers Under Zimbabwe's Interception of Communications Act, *Statute Law Review*, Volume 45, (1). DOI: hmae018, https://doi.org/10.1093/slr/hmae018.

Institute of Public Policy Research. 2021.Not fit for purpose– the Data Protection Bill. Accessible at https://action-namibia.org/https-action-namibia-org-wp-content-uploads-2022-12-data-protection-bill-web-pdf/.

Munoriyarwa, A., 2021. When watchdogs fight back: resisting state surveillance in everyday investigative reporting practices among Zimbabwean journalists. *Journal of Eastern African Studies*, *15*(3), pp.421-441.

Perspectives on Parliament. 2022. Thinking about data. Accessible at: https://ippr.org.na/wp-content/uploads/2023/01/PoP-17-web.pdf.