Statute Law Review, 2024, **45**, hmae018
https://doi.org/10.1093/slr/hmae018
Advance access publication 16 March 2024
Article

OXFORD

An Analysis of the Legislative Protection for Journalists and Lawyers Under Zimbabwe's Interception of Communications Act

Brian Hungwe[*], Allen Munoriyarwa[**]

ABSTRACT

This paper provides a legal analysis that interrogates the Information Communication Act (ICA) in Zimbabwe. Its purpose is to examine the extent to which the ICA protects journalists and lawyers privileges, critical constituencies in any democratic state. The ICA, passed in 2007, has remained a heavily contested legislation in the country. On the one hand, it is understood to be security minded legislation, yet, other critics have argued that it interferes with the journalist's source privilege, and lawyer–client confidentiality. In this paper, we are concerned about whether the Act provides adequate safeguards where the subject of surveillance is a practising journalist or lawyer. Thus we ask; to what extent does the ICA provides adequate legal safeguards to lawyers and journalists? Through a qualitative textual analysis of the law, the paper determines the constitutional implications of the main provisions of the Act on whether they reflect constitutional norms that safeguard the legal privileges accorded to the professions. We note that the ICA does not provide adequate safeguards for the protection of lawyers and journalists. We, therefore, argue that ICA is a weaponized legislation meant to emasculate these two communities of practice. As such, we call for the Act's alignment with the current broadened constitutional provisions. South Africa's Constitutional Court has invalidated unconstitutional provisions within its surveillance and interception laws, likewise identical provisions within its neighbouring state, Zimbabwe should follow the same. Both countries share common historical, political and economic ties.

1. BACKGROUND AND CONTEXT

The Interception of Communications Act [Chapter 11:04] (hereinafter 'the Act' and or 'ICA') was enacted in 2007 and is still to be aligned with the current 2013 Constitution of Zimbabwe. The old Lancaster House Constitution, a post-liberation war document that was drafted after a

[*] PhD Candidate with the School of Law, University of Witwatersrand, South Africa and Fellow of the Association of Arbitrators (Southern Africa) NPC. Email: hungwebrian@gmail.com
[**] Senior Lecturer of Media Studies at the University of Botswana and a non-resident Senior Research Associate at the University of Johannesburg's Department of Communication and Media. He is the coordinator of the British Academy funded Project titled 'Watching the Watchers: Strengthening Public Oversight of Intelligence Driven Surveillance'. Email: allenmunoriyarwa@gmail.com

1979 constitutional conference was amended 19 times in 30 years and regrettably did not specifically provide for the right to privacy unlike the present constitution.[1] However, the adoption of the ICA in Zimbabwe gave the country a membership card to the club of nations that acknowledge the necessity of national security and the concomitant need to restrict fundamental rights and freedoms to protect national security related imperatives. The Act must be understood in the context of various political developments with impact and implications on national security in Zimbabwe since the turn of the millennia. Since 2000, a year synonymous with the violent land reform programme and attendant state sanctioned human rights abuses, Zimbabwe has witnessed violent demonstrations, riots, mass protests, vicious electoral contestations and other acts of political and economic subterfuge.[2] To some, the increase in state security related legislation has followed the degeneration in internal political dynamics, characterized by fierce political contestations between the governing ZANU PF party, opposition political parties and other civil society movements.[3]

Zimbabwe is going through some economic turbulence, dating back to the 2000s politically motivated seizures of white-owned commercial farmlands. The resultant economic downturn has put some severe pressures on the government, which has since tightened its grip on power amid fears of a Western-sponsored regime change agenda.[4] The economic crisis was often accompanied by state sponsored gross human and property violations, accompanied by corruption and abysmal monetary policies.[5] The Heritage Foundation reported that, 'Zimbabwe's economic freedom score is 39.0, making its economy the 172nd freest in the 2023 Index. … [It] is ranked 46th out of 47 countries in the Sub-Saharan Africa region and is one of the least free economies ranked in the 2023 Index.'[6] Furthermore, it reports that the economy is 'characterized by instability and policy volatility, which are hallmarks of excessive government interference and mismanagement.'[7]

To manage public dissent, the government has previously from the early 1980s to late-1990s, maintained state monopoly on the telephone business using a parastatal, the Posts and Telecommunications Corporation (PTC), and arbitrarily and effectively barred the introduction of cellphones for a prolonged period.[8] In circumstances where private players sought to venture into the telecommunications business, the government used state security and fought legally to bar them.[9] Scholars find this approach tyrannical and against modernization.[10] At present, there are two state owned mobile phone operators and one privately owned. However, all Internet Service Providers (ISPs) and mobile phone companies are licensed and regulated by the state owned telecommunications regulatory body, POTRAZ.[11] Notwithstanding, establishing ISPs and mobile phones is difficult due to exorbitant application and operating

[1] J Mapuva, 'The Trials and Tribulations of Constitutionalism and the Constitution Making Process in Zimbabwe', 2(3) Int J Public Law Policy 123 (2010).
[2] E V Masunungure, 'Zimbabwe's Militarized, Electoral Authoritarianism', 65(1) J Int Affairs, 54 (2011). See also A Munoriyarwa 'So, Who is Responsible? A Framing Analysis of Newspaper Coverage of Electoral Violence in Zimbabwe', 12(1) J African Media Stud 61–63 (2020).
[3] J Makumbe, 'Theft by Numbers: ZEC's Role in the 2008 Elections' in E Masunungure (ed) 'Defying the Winds of Change: The 2008 Elections in Zimbabwe' 119–125 Weaver Press: Harare (2008).
[4] G Cain, 'Bad Governance in Zimbabwe and Its Negative Consequences', 2(1) Downtown Rev. 1 (2015).
[5] Ibid.
[6] The Heritage Foundation 'Zimbabwe 2023 Index of Economic Freedom' (2023) <https://www.heritage.org/index/pages/country-pages/zimbabwe> accessed 5 February 2023.
[7] Ibid.
[8] See R S Velamuri and J Mitchell, 'Resisting Political Corruption: Econet Wireless Zimbabwe' (2004) <http://dx.doi.org/10.2139/ssrn.1008498> accessed 5 February 2024. See also G Cain 'Bad Governance in Zimbabwe and Its Negative Consequences', 2(1) Downtown Rev. 3–4 (2015).
[9] See R S Velamuri and J Mitchell, 'Resisting Political Corruption: Econet Wireless Zimbabwe' (2004) <http://dx.doi.org/10.2139/ssrn.1008498> accessed 5 February 2024
[10] Ibid.
[11] Freedom House 'Zimbabwe, Freedom on the Net 2012' <https://freedomhouse.org/sites/default/files/Zimbabwe%202012.pdf> accessed 5 February 2024

fees.[12] Nonetheless, a significant section of the population had a total of 14.08 million cellular mobile connections in early 2023, representing about 85.4 percent of the total population.[13] The last census statistics reveal that the country's total population is 16.49 million. There were about 6 million Internet users in Zimbabwe at the start of 2023, with 1, 5 million social media users.[14] The government is mulling plans to increase Internet penetration to above 75% by 2025.[15]

Insights into Zimbabwe's state security surveillance operations were disclosed in 2014 by the former Minister of State for National Security in charge of state intelligence between 2005 and 2009, Didymus Mutasa who indicated that the government, 'sees everything … We have our means of seeing things these days; we just see things through our system. So no-one can hide from us in this country.'[16] The former speaker of parliament, who also was the former ruling Zanu PF party secretary for administration warned Zimbabweans to, '[b]e careful not to denigrate our president [;] we will visit your bedrooms and expose what you will be doing.'[17] Subsequently in 2015 after he had left government, Mutasa said, 'Your phones are listened to a lot. The CIO is huge and it produces many reports'.[18] It is important to note that these statements have not been refuted by the state to date. There are several noteworthy provisions of the Act which since 2007 have become contentious and subject to legal contestations. In this paper, we provide a qualitative analysis of selected provisions of the ICA, particularly those that deal with surveillance practices. Our aim is to provide a critic of the extent to which these provisions protect vulnerable communities of practice. We purposively chose lawyers and journalists as some of the most vulnerable for several reasons.

Firstly, since ZANU PF' authoritarianism started intensely hardening in the post- 2000 period, specific communities have been targeted.[19] These include journalists[20]and lawyers,[21] at the centre of targeted surveillance. While research is growing on how these communities of practice have been targeted, there is very little research at the intersection of these professions and their exposure to legalized form of surveillance. This legal analysis makes an attempt to close this gap by providing an analysis of a specific law and how it affects journalists and lawyers quotidian practices. Methodologically, we utilize qualitative textual analysis. This is a qualitative method that allows us to examine the structure, content and meaning of a legal instrument, and how it relates to the historical, political, economic, social, and cultural contexts of its production. Often, this method had been used to provide analysis of legislations.

The article is organized as follows. In the next section, we provide a brief synopsis of international legal standards of surveillance. This is important if we are to determine the extent to

[12] Ibid at 6. The fees for IAPs and ISPs range from US$2–4 million, depending on the type of service to be provided. This is in addition to the 3.5 percent of annual gross income that the provider must pay to POTRAZ.

[13] Simon Kemp, 'Digital 2023 Zimbabwe' *Digital Zimbabwe* 11 February 2023 <https://datareportal.com/reports/digital-2023-zimbabwe> accessed 5 February 2024.

[14] Ibid.

[15] Stanley Karombo, 'Zimbabwe Targets 75% Internet Penetration by 2025' ItWeb, 20 March 2023 <https://itweb.africa/content/O2rQGqAEJl3qd1ea> accessed 5 February 2024.

[16] NewZimbabwe.com "CIO watching your bedrooms, Mutasa warns critics," *New Zimbabwe*, 10 June 2014 in The Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe, the International Human Rights Clinic 'Stakeholder Report Universal Periodic Review 26th Session—Zimbabwe The Right to Privacy in Zimbabwe' 2016, Harvard Law School, and Privacy International, March 2016. <https://humanrightsclinic.law.harvard.edu/wp-content/uploads/2022/10/zimbabwe_upr2016.pdf> accessed 18 August 2023.

[17] Ibid.

[18] Richard Chidza, 'I am ready for jail: Mutasa' *NewsDay*, 1 July 2015, <https://www.newsday.co.zw/2015/07/01/i-am-ready-for-jail-mutasa/> accessed 19 August 2023.

[19] Masunungure (n 4) 55; See also P Zamchiya 'Inside Competitive Electoral Authoritarianism in Zimbabwe, 2008–2018', in Miles Tendi, JoAnn McGregor, and Jocelyn Alexander (eds), The Oxford Handbook of Zimbabwean Politics (online edn, Oxford Academic, 9 July 2020) https://doi.org/10.1093/oxfordhb/9780198805472.013.9 accessed 18 August 2023.

[20] A Munoriyarwa and S H Chiumbu, 'Big Brother is Watching: Surveillance Regulation and Its Effects on Journalistic Practices in Zimbabwe', 40(3), African J Stud P.26–41 (2019).

[21] A LeBas, A and N Munemo, 'Elite Conflict, Compromise, and Enduring Authoritarianism: Polarization in Zimbabwe, 1980–2008', 681(1) The Ann Am Acad Polit Social Sci 209–226 (2019). https://doi.org/10.1177/0002716218813897 accessed 18 August 2023.

which current domestic legislation meets the international barometers set on domestic surveillance. We follow that section with an analysis of how it affects journalists, before we analyse how it impacts on lawyer–client privilege. We then draw South Africa's tested constitutional parameters of Regulations of Interceptions of Communications Act (RICA) to reveal existing deficiencies of the ICA. We then conclude the article by assessing important deficiencies of this constitutional provision.

2. GLOBAL STANDARDS OF SURVEILLANCE REGULATION

Surveillance in the digital age has stirred controversy and contestation at a global level.[22] The central question has been: how can surveillance be practiced in such a manner that it is used to combat crime or provide early warning information against serious criminal activities like terrorism, drug syndicates, but at the same time, protect privacy and safeguard all other associated rights? There are no easy answers to this. The lack of answers emanate from three main factors. Firstly, the human rights regime itself is contested. The discourse of human rights has divided states and fermented confrontations amongst states.[23] Secondly, security threats differ, and they mutate frequently. This makes it hard to pinpoint with certainty how much surveillance and what kind of surveillance would a particular state need. Thirdly, the technologies of surveillance keep changing.[24] It is incredibly hard to legislate for or against specific technologies when a few months or years down the line they are overtaken by yet another technology requiring its own set of laws and legislation. Despite these, global resolutions have been promulgated through the United Nations (UN) to protect human rights from digital surveillance.[25]

The most recent resolution on the right to privacy in the digital age was adopted by the Human Rights Council in September 2019.[26] The resolution, among other issues, states that no citizen should be subjected to arbitrary and unlawful interference with privacy, family, home and correspondence. Additionally, the resolution guarantees equal protection before the law and further right to privacy guarantees. The resolution provides that,

> States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality. It affirms that the same rights that people have offline must also be protected online, including the right to privacy; and it acknowledges that the use, deployment and further development of new and emerging technologies, such as artificial intelligence, can impact the enjoyment of the right to privacy and other human rights.[27]

[22] See A Nishnianidze, 'Surveillance in the Digital Age', 24 Eur Scient J 80 (2023). See also The Annual report of the United Nations High Commissioner for Human Rights 'The right to privacy in the digital age' (2014) A/HRC/27/37, para 47: It reported that: 'International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data. Practices in many States have, however, revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.'

[23] See C Clyde Ferguson, 'Global Human Rights: Challenges and Prospects', 8 Denv. J. Int'l L. & Pol'y 367 (1979) . See also Eric Posner 'The case against human rights' *The Guardian*, 4 December 2014 <https://www.theguardian.com/news/2014/dec/04/-sp-case-against-human-rights> accessed 5 February 2024.

[24] M Padden, 'The Transformation of Surveillance in the Digitalisation Discourse of the OECD: A Brief Genealogy', 12(3) Internet Policy Review, [online] (2023) <https://policyreview.info/articles/analysis/transformation-of-surveillance-in-digitalisation-discourse> accessed 5 February 2024. See also Gordon Corera, 'Pegasus Scandal: Are We All Becoming Unknowing Spies?', BBC 21 July 2021 <https://www.bbc.com/news/technology-57910355> accessed 5 February 2024.

[25] See Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa—ACHPR/Res.573 (LXXVII) 2023. See also Resolution adopted by the General Assembly on 18 December 2013, The report of the Third Committee (A/68/456/Add.2) 68/167 'The right to privacy in the digital age'.

[26] See Human Rights Council Forty-second session 9–27 September 2019 Agenda item 3 Resolution adopted by the Human Rights Council on 26 September 2019 <https://www.ohchr.org/en/press-releases/2019/09/human-rights-council-hold-its-forty-second-regular-session-9-27-september> accessed on 18 August 2023.

[27] Ibid.

There are four major surveillance practices yardsticks that have been adopted as representing best practice in surveillance. In liberal democracies, there is, firstly, an acknowledgement that best surveillance practices would need judicial oversight.[28] This is healthy in a democracy to ensure that the institutions that exercise surveillance are subjected to checks and balances to avoid human rights violations. Secondly, there is also an agreement that surveillance should strictly be crime related to avoid political actors using it against legitimate opposition and other actors. Thirdly, the protection or proper disposition of individual data post-surveillance is a key principle of surveillance. Lastly, post-surveillance notification is an important practice—where targets are informed post-fact for transparency.

3. ZIMBABWE'S ICA LEGISLATION

States have crafted surveillance laws that either respect the resolutions, or in some instances defy the resolution. In both cases, the justification has been security of the state and its citizens. The same has been the case with Zimbabwe. For instance, under the Act, surveillance can only be instituted under section 6 in relation to serious offences. Section 6(1) provides that:

A warrant shall be issued by the Minister to an authorized 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 organized 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.[29]

Circumstances may arise where the target of surveillance is either a practising journalist and or lawyer. The Act is silent on how such surveillance should be carried in these two respective professions whose members' rights are both guaranteed and protected under the constitution and common law. An identical surveillance legal and political parameters also existed under the Rhodesian colonial government. In colonial Zimbabwe, the judiciary had been an important institution that protected white minority rule.[30] In post-colonial Zimbabwe, the state has been notorious for the politicization of the judiciary as well.[31] Throughout history, both journalism and law as professions have been systematic targets of repressive laws of Rhodesian colonial governments due to their extent of influence in information dissemination[32] protecting the rule of law and their broader influence on a country's democratic process. The judiciary was used to protect the political interests of the colonial establishment through narrow legal interpretations that leaned towards entrenchment of their vested parochial interests.[33] The colonial government using the State of emergency powers legitimized the decision of the authoritarian

[28] J Duncan, *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (New York: University Press, 2018).
[29] The Interception of Communications Act [Chapter 11:04] section 6.
[30] C Palley, 'The Judicial Process: U.D.I. and the Southern Rhodesian Judiciary', 30 Modern Law Rev 283–267 (1967).
[31] S Verheul, *Performing Power in Zimbabwe: Politics, Law, and the Courts Since 2000* (Cambridge University Press, 2021).
[32] Rhodesian journalist Peter Niesewand. On 20 February 1973 he was arrested and spent 73 days in solitary confinement for his criticism of conditions under Ian Smith's government and his coverage of the guerrilla war. His sentence of two years hard labour for revealing official secrets was commuted on appeal after an international outcry. He was deported on release from prison. <https://en.wikipedia.org/wiki/Peter_Niesewand> accessed 18 July 2021. See also British House of Commons, HC Deb 17 May 1973 vol 856 Ql. Mr. Edward Lyons asked the Prime Minister Edward Heath, whether he will now seek to meet Mr. Ian Smith. <https://api.parliament.uk/historic-hansard/commons/1973/may/17/mr-ian-smith> accessed 18 July 2021.
[33] *See* John F. Burns, 'Rhodesia is severe in 'terrorism' cases' *New York Times* 12 February 1978.<https://www.nytimes.com/1978/02/12/archives/rhodesia-is-severe-in-terrorism-cases-blacks-found-guilty-of.html> accessed 18 July 2021. Chief Justice McDonald sentenced a black villager sentenced to 15 years in prisons for failing to report presence of African freedom

regime to broaden the role of the intelligence services within the state security apparatus and to marginalize the legislative and judicial arms of the government.[34] After the 1980 independence, scholars observe that the African nationalist regime led by Zimbabwean president Robert Mugabe was faced with the challenge that every regime must undertake to define the role and structure of the state security apparatus and to determine how that apparatus will reflect the character of the state.[35]The dilemma faced by the new governing party, the Zimbabwe African National Union (ZANU) was that it:

> inherited an authoritarian repressive state supported by a powerful state security apparatus [...] The Mugabe regime was faced with the options to reform or restructure or transform the state security apparatus, including its ethical paradigm. Mugabe, based on the perceived threat to the survival of his regime retained the existing Rhodesian state of emergency as well as restructured and broadened the state security apparatus. The result was continued marginalization of the legislative and judicial branches of government, not unlike the apartheid regime he had so recently supplanted. From the standpoint of intelligence ethics, the transition from Smith's apartheid regime to Mugabe's postcolonial regime did not lead to a change in the behaviour of the intelligence services within the state security apparatus only to the identification of new targets of state repression.[36]

Conceivably, this explains why Zimbabwe's post-independence legislative framework was largely based on political survival and maintenance of state security than broad based progressive human rights considerations especially in the protection of journalists and lawyers privileges.

(A) Journalists Privilege

The Constitution's broadened Bill of Rights specifically protects the journalists' right to the doctrine of silence in relation to non-disclosure of sources of legitimate public interest information. Section 61(1) and (2) of the Constitution under freedom of expression and of the media provides that:

Every person has the right to freedom of expression, which includes;

a) Freedom to seek, receive and communicate ideas and other information;
b) Freedom of artistic expression and scientific research and creativity; and
(2) Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists' sources of information.[37]

The protection of journalists' sources of information is part of the focus of this contribution. Previously, the Lancaster House Constitution did specifically provide for media freedom which was however indirectly sheltered under the freedom of expression.[38] Despite this constitutional

fighter. "The sentence was characteristic of the harsh punishment meted out by Rhodesian courts to blacks found guilty of what are termed terrorist offenses. Several times a week a panel of three white wigged judges confirms death sentences and heavy prison terms for those who support or acquiesce in the guerrilla cause...Critics of the High Court, which is in the same building as Parliament and only a block from the closely guarded office of Prime Minister Ian D. Smith, say that the proximity is more than geographical. "I don't think there is really any clear distinction between the judiciary and the other branches of government anymore," a prominent attorney commented. "After all, the judges are all white and they're caught up in this war like everybody else."

[34] C Courville, 'Intelligence Ethics: The African Authoritarian State Security Apparatus', 3(2) Int J Intell Ethics (2012) I Fall I Winter 2012.

[35] Ibid.

[36] Ibid.

[37] Constitution of Zimbabwe, 2013.

[38] Lancaster House Constitution section 20 Protection of freedom of expression.

> (1) Except with his own consent or by way of parental discipline, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence.

omission, statutes and precedents provided scope for journalists' sources protection under public interest considerations. In *Shamuyarira v Zimbabwe Newspapers (1980) Ltd & Another*, the High Court upheld this right.

> Unless our courts are seen to be prepared to lean over backwards to protect, in the public interest, a journalist's source where the journalist has publicly uncovered corruption or some other form of iniquity on the part of those holding high office, whether in government or elsewhere, the courts will be guilty of a grave disservice to Zimbabwean society and to the principles of democracy upon which that society is founded.[39]

It is important to note that sections'113C and 232 of the Criminal Procedure and Evidence Act allows the court to subpoena a witness.[40] The Act further states that no witnesses shall be compelled to give evidence on account of public policy and or public interest considerations. This is legal latitude that could be exploited by the media to protect their sources of information. The privilege for non-disclosure is founded on persuasive considerations under freedom of expression and the media ccaptured by Gubbay CJ, as he was then, in *Chavhunduka v Minister of Home Affairs*, wherein he stated that:

freedom of expression has four broad special objectives to serve:

(i) it helps an individual to obtain self-fulfilment;
(ii) it assists in the discovery of truth, and in promoting political and social participation;
(iii) it strengthens the capacity of an individual to participate in decision making; and,
(iv) it provides a mechanism by which it would be possible to establish a reasonable balance between stability and social change.[41]

The dangers in not providing legal frameworks that protect the confidential sources of journalism are that public interest information may never be delivered as sources may never be forthcoming because of predictable reprisal fears. Studies demonstrate that legal frameworks for protection of sources of confidential information are under threat in the digital age, and there is therefore need to reinforce them.[42] Surveillance of citizens has become more sophisticated because of the new technological advancements that give states around the world scope to eavesdrop and pry on private information.[43] Mature democracies have been implicated in espionage and gross interference with the privacy of its citizens, external allies and strategic institutions.[44] India's government, running one of the fastest growing economies in the world is accused of using a spyware called Pegasus, which targets journalists, human rights activists and opposition politicians. The software apparently secretly unlocks the contents of a target's mobile phone and transforms it into a listening device.[45] In South Africa, evidence

[39] *Shamuyarira v Zimbabwe Newspapers* (1980) Ltd 1994 (1) ZLR 445 (H) at 843
[40] Sections' 113C and 232 of the Criminal Procedure and Evidence Act [9:07] (CPEA).
[41] *Chavunduka and others v Minister of Home Affairs and another* [2000] JOL 6540 (ZS).
[42] See UNESCO 'Protecting Journalism Sources in the digital age' UNESCO series on Internet Freedom <http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/images/Themes/Freedom_of_expression/safety_of_journalists/Protecting_Journalism_Sources_in_Digital_Age_UNESCO_Flye.pdf> accessed on 17 July 2021.
[43] Simon Allison, 'South African phones targeted by notorious 'governments only spyware' *Mail&Guardian*, 2 October 2018. https://mg.co.za/article/2018-10-02-south-african-phones-targeted-by-notorious-governments-only-spyware/ accessed 17 July 2021.
[44] See E Snowden, *Permanent Record Hardcover* (2020) Picador Paper. See also G Greenwald 'No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State' 2015 Picador.
[45] See Joanna Slater and Niha Masih, 'PM Imran's number among those targeted for surveillance by India using Israeli spyware' *The Washington Post* 19 July 2021. <https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/> accessed 20 July 2021. See also: Reuters/AFP'PM Imran's number among those targeted for surveillance by India using Israeli spyware: report' *The Dawn*, July 20, 2021. <https://www.dawn.com/news/1636010/india-among-countries-using-israeli-software-to-spy-on-journalists-report> accessed 20 July 2021.

of surveillance and snooping of practising journalists is supported by uncontroverted court records that implicated its government.[46] In that jurisdiction, there are growing concerns around organized hits targeting whistle-blowers.[47] Axiomatically, pre-publication exposure of journalistic investigations to intrusive politically motivated and unregulated surveillance will only expose the media to intimidation, cover-ups and repercussions to legitimate sources resulting in self-censorship. The reference of the media as the Fourth Estate arises because of the media's capacity for advocacy, providing checks and balances framing political issues, restoring or entrenching accountability mechanisms with the state.[48] Though journalism is not formally recognized as a part of a political system, it wields enormous direct and indirect social influence in the public sphere in its role to disseminate news. The merit of the democratic system is that it gives freedom of expression space to each individual and in most instances, through the media.

(B) Lawyer–Client Privilege

Unlike in journalism, the lawyer client privilege is not specifically protected under the present and old constitution. Its privilege is guaranteed under common law despite having been in force for centuries. The rule is also often referred to as attorney–client privilege. The evidentiary privilege protects communications between an attorney and or a law firm and the client, and such information may never be disclosed and is deemed fundamental to the proper functioning of our system of justice.[49] The privilege in jurisdictions such as the United States is governed by statute. Regardless, the rationale and policy behind it is to provide unfettered legal scope for a:

> full and frank communication between attorneys and their clients... [to] thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that sound legal advice or advocacy serves public ends, and that such advice or advocacy depends upon the lawyer's being fully informed by the client.[50]

The lawyer client privilege considerations were confirmed by South Africa's Constitutional Court in *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others*, where it held that,

> [t]he right to legal professional privilege is a general rule of our common law which states that communications between a legal advisor and his or her client are protected from disclosure, provided that certain requirements are met. The requirements are
>
> (i) the legal advisor must have been acting in a professional capacity at the time;
> (ii) the advisor must have been consulted in confidence;

[46] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2021 (3) SA 246 (CC) at paras 5-37-38-39.

[47] Reitumetse Makwea ,'Tembisa Hospital tenders: 'Find the 'big dogs' – Out' *The Citizen* 29 August 2022 <https://www.citizen.co.za/news/south-africa/tembisa-hospital-tenders-find-the-big-dogs-outa/> accessed 19 August 2023.

[48] T Carlyle, *On Heroes, Hero Worship, and the Heroic in History* (1841) 141. He writes that: 'Burke said there were Three Estates in Parliament; but, in the Reporters' Gallery yonder, there sat a Fourth Estate more important far than they all. It is not a figure of speech, or a witty saying; it is a literal fact … Printing … is equivalent to Democracy … Whoever can speak, speaking now to the whole nation, becomes a power, a branch of government, with inalienable weight in law-making, in all acts of authority. It matters not what rank he has, what revenues or garnitures: the requisite thing is that he have a tongue which others will listen to; this and nothing more is requisite.'

[49] E Mark, 'Legal Ethics: The Client-Attorney Privilege', Nat Business Ellis Law Group, LLP (2017) <https://www.law.com/dailyreportonline/2023/09/01/legaledge-safeguarding-the-attorney-client-privilege/> accessed 17 July 2021.

[50] Ibid. And also statute: 449 U.S. at 389; Restatement (3rd) *Law Governing Lawyers* section 68, comment (c).

(iii) the communication must have been made for the purpose of obtaining legal advice;
(iv) the advice must not facilitate the commission of a crime or fraud; and
(v) the privilege must be claimed.[51]

The doctrine is not mere rule of evidence as its confidential functionality is necessary for the proper administration of justice. This logic is captured in *Baker v Campbel,* which precedent is believed to provide a 'compendious and most useful international survey of the pertinent jurisprudence on the history and development of the rule.'[52] The description by Sir Gordon Slynn in the *A M & S Europe Ltd v Commission of the European Communities* case has eminently flowed in various precedents in Southern Africa as it captures the modern expression of the philosophy reinforcing the rule and the premium that society attach to it.[53] Slynn opines that:

> Whether it is described as the right of the client or the duty of the lawyer, this principle has nothing to do with the protection or privilege of the lawyer. It springs essentially from the basic need of a man in a civilised society to be able to turn to his lawyer for advice and help, and if proceedings begin, for representation; it springs no less from the advantages to a society which evolves complex law reaching into all the business affairs of persons, real and legal, that they should be able to know what they can do under the law, what is forbidden, where they must tread circumspectly, where they run risks.[54]

The privilege if applicable in its four corners is absolute, and suffices in both civil and criminal proceedings. The protection of journalists' sources of information and the lawyer client privileges are both under threat of the ICA provisions, whose surveillance framework is intrusive, lacking judicial oversight and interference, and not subject to proper information safeguards.

4. THE CONSTITUTIONAL DEFECTS OF ICA

As a constitutional democracy, Zimbabwe attaches value to the supremacy of the Constitution under its founding values and principles.[55] Further, section 2(1) specifically states that: 'This Constitution is the supreme law of Zimbabwe and any law, practice, custom or conduct inconsistent with it is invalid to the extent of the inconsistency.' The obligations for the protection bind, 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.'[56] The problematic aspects of the Act are that it does not specifically shield either journalists or lawyers from the dragnet surveillance scanning mechanism. As such, there is potential for gross unrestricted interference with the afforested rights and privileges applicable to practicing journalists and lawyers which undoubtedly protect public interest and promote rule of law standards respectively.

The Act is unconstitutional in various respects. Among others, is its failure to prescribe a procedure for notifying the subject of the interception. Without a delineated procedure to notify

[51] *Thint (Pty) Ltd v National Director of Public Prosecutions and Others; Zuma and Another v NDPP and Others* 2009 (1) SA 1 (CC).
[52] *Baker v Campbell* [1983] HCA 39; 153 CLR 52.
[53] *AM & S Europe Limited v Commission of the European Communities. Legal privilege. Case 155/79.* European Court Reports 1982 -01575.
[54] *Baker v Campbell* [1983] HCA 39; 153 CLR 52.
[55] Constitution of Zimbabwe, section 3(1) (a).
[56] Ibid at section 2(2).

a journalist and or lawyer of the interception, the Act provides cate Blanche for authorities to surreptitiously walk in the dark unaided with a legal guiding torch whose net result is the inadvertent intrusion and violation of rights of the respective parties. A proper procedure generally ensures that the privileges and sources guaranteed and protected under both the constitution and common law are safeguarded. After obtaining the relevant information under surveillance, sections 11(7)(b), 15 (2) of the Act does not prescribe the proper procedure to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing data obtained from interceptions. Importantly, the powers vested under section 5[57] to a prejudiced minister in government to receive and issue warrants, instead of an independent and impartial judicial authority blurs the separation of powers envisaged under section 3 of the Constitution.[58] The Act, in particular sections' 6 and section 6 are inconsistent with the constitution and invalid to the extent that they fail to address expressly the circumstances where a subject of surveillance is either a practising journalist or a lawyer. This failure is compounded by the unlawful provision that allows for unconstitutional bulk surveillance under section 9 of the Act.[59] The bulk surveillance is an automatic dragnet that incorporates journalists and lawyers alike. The ICA does not provide adequate safeguards to protect subjects with a legitimate right to protect sources of information, particularly practising journalists and lawyers having privileged communication with their clients. Key terms in the Act, such as 'monitoring' are not clearly defined creating room for abuse, especially in relation to the collection and analysis of metadata.

(A) Right to Privacy

The ICA provisions invert the right to privacy provisions provided under section 57 of the Constitution.[60] The provisions under the Act are disturbingly overbroad in scope and invasive. This because the scope of the Act allows authorities to retrieve and or monitor the sharing of intimate personal confidences, snoop on private communications between journalists and their sources, and or lawyers and their clients. The bulk surveillance provisions effectively mean there is scope for interception of all communications. This interception does not draw a distinction between journalists' private communications and lawyers and even the broader public's intimate personal communications. Privacy is therefore breached along the entire length and breadth of the interceptions. The violation of privacy invariably violates an individual's cognate right to dignity,[61] a right that permeates all fundamental rights.[62]

[57] The Interception of Communications Act section 5 (1) (2) Authorised persons to apply for warrant of interception (1) An application for the lawful interception of any communication may be made by the following persons, (2) An application in terms of subsection (1) shall be made by an authorized person to the Minister for the Minister to issue a warrant for the interception of any communication.

[58] Constitution of Zimbabwe, section 3(1)–(2) Founding values and principles. Zimbabwe is founded on respect for the following values and principles—a. Supremacy of the Constitution; b. the rule of law; 2. The principles of good governance, which bind the State and all institutions and agencies of government at every level, include—e. observance of the principle of separation of powers;

[59] Section 9 of the Interception of Communications Act. The Act provides, where necessary, the capacity to implement a number of simultaneous interceptions in order—(i) to allow monitoring by more than one authorized person.

[60] The right to privacy, under section 57 of the constitution, Right to privacy, which includes the right not to have:- [...} (d) the privacy of their communications infringed. See also Article 12 Universal Declaration of Human Rights: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[61] Section 51 of the Constitution of Zimbabwe, Right to human dignity "Every person has inherent dignity in their private and public life, and the right to have that dignity respected and protected."

[62] See O Mezzaro and B Oliveira da Silveira, 'The Principle of the Dignity of Human Person: A Reading of the Effectiveness of Citizenship and Human Rights Through the Challenges Put Forward by Globalization', Rev. Investig. Const. (2018) https://doi.org/10.5380/rinc.v5i1.54099. See also *S v Makwanyane and Another* 1995 (3) SA 391. The right to dignity largely informs the content of the right to life. Human dignity has been referred to as the 'cornerstone' of the South African Constitution, and it is found therein as both a right and a value.

(B) Freedom of Expression and Right to Fair Hearing and Access to Courts

The Constitution under section 61 provides freedom of expression and of the media.[63] Unlawful interceptions and abuse of their private communications imposes a severe restraint upon the constitutionally protected freedom of expression and of the media. Surveillance of journalists constitutes a limitation of the right to freedom of expression and the media under section 61 and that surveillance of a practicing lawyer infringes legal professional privilege. The domino effect of this concomitant violation is the infringement on the right to a fair trial, as the surveillance of lawyers limits the rights to a fair hearing and trial, respectively guaranteed under section 69 of the Constitution.[64] The Act does not expressly provide surveillance circumstances where the target may be a practicing lawyer or journalist. The protection of journalists' sources is guaranteed under the rights to freedom of expression and the media. Equally important is that legal professional privilege is an essential part of the rights to a fair trial and fair hearing. The Court in Thint supra, held:

> The right to legal professional privilege is a general rule of our common law which states that communications between a legal advisor and his or her client are protected from disclosure, provided that certain requirements are met … It is now generally accepted that these communications should be protected in order to facilitate the proper functioning of an adversarial system of justice, because it encourages full and frank disclosure between advisors and clients. This, in turn, promotes fairness in litigation.[65]

Fairness of trial is therefore inextricably linked to protection of lawyer client privilege, which automatically promotes the rule of law. In *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* the court persuasively held that:

> The wholesale interception of lawyer-client communications without any recognition of this legal, indeed constitutional, reality would be at odds with the rule of law. In sum, the confidentiality of lawyer-client communications and journalists' sources is particularly significant in our constitutional dispensation. There is thus a need that special consideration be given to this fact when interception directions are sought and granted. … (the Act) is thus unconstitutional to the extent that, when the intended subject of surveillance is a practising lawyer or a journalist, it fails to provide for additional safeguards calculated to minimise the risk of infringement of the confidentiality of practising lawyer and client communications and journalists' sources.[66]

The ICA provisions affect millions of Zimbabweans who are subscribers of the telecommunications service providers. There are above 12 million mobile phone subscribers in Zimbabwe.[67] As such, journalists and legal practitioners are equally affected. The public interest consideration of surveillance is anchored on the firm belief that interception and surveillance affect many

[63] Constitution of Zimbabwe s 61(1) (2). The right to freedom of expression and the media: (1) Every person has the right to freedom of expression, which includes (a) Freedom to seek, receive and communicate ideas and other information; … (2) Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists' sources of information.'

[64] Constitution of Zimbabwe section 69 (1) Right to a fair hearing 'Every person accused of an offence has the right to a fair and public trial within a reasonable time before an independent and impartial court.'

[65] *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* 2009 (1) SA 1 (CC).

[66] See AmaBhungane Case (n 32).

[67] See The Globaleconomy.com 'Zimbabwe: Mobile phone subscribers' <https://www.theglobaleconomy.com/Zimbabwe/Mobile_phone_subscribers/> accessed 19 August 2023.

Zimbabweans. Therefore, it is important that all interceptions and surveillance be done in accordance with the law.

5. ICA VERSUS INTERNATIONAL STANDARDS OF SURVEILLANCE REGULATION

Furthermore, if we juxtapose ICA to the global standards of surveillance that we had laid out above, it is clear that the law ails from several legislative deficiencies which renders it unconstitutional. These relate to, but not limited to the Act's failure to notify the subject of surveillance, ministerial powers to issue a warrant and bulk communication surveillance.

(A) Failure to Notify Subject of Surveillance

According to international human rights standards, every person who is subject to interception and or surveillance should be notified of the decision authorizing surveillance. Delays may be justified only in limited circumstances such as when notification would seriously jeopardize the purpose of the surveillance and for a limited time usually until the reason for the delay no longer exists.[68] While ICA allows individuals to appeal a decision to the Administrative Court once they have been 'notified or becom[e] aware' of a warrant, the Act itself does not require authorities to notify individuals that they are or have been the subject of an interception warrant and renewal proceedings.[69] The Act also does not provide for notification of subject before and importantly after interception. While it may not be contestable that prior notification can be problematic in compromising the gathering evidence by the law enforcement authorities, there are constitutional concerns around failure to notify the subject after the interception and especially where no evidence of illegalities has been obtained. Section 18 (1) of the Act states that, 'Any person who is aggrieved by a warrant, … may appeal to the Administrative Court within one month of being notified or becoming aware of it, as the case may be.' This is a serious infraction of the right to privacy under section 57 of the constitution, in which the subject is never notified after an investigation has been completed, and the interception direction has lapsed. The subject has no way of knowing if the investigation was lawful or not, and the nature and form of the interception direction. This approach inverts the constitutional principle of open justice, promoting night covert justice in which the right of privacy is impinged.

(B) Ministerial Powers to Issues a Warrant

There is lack of judicial oversight in the application and issuance of the warrant. The international human rights standards articulated in the International Principles on the Application of Human Rights to Communications Surveillance, provides that determinations concerning communications surveillance must be made by a competent judicial authority that is independent and impartial.[70] Under the Act, it is not possible for the subject under interception to appear before the minister, or even after the fact. Importantly, what is in issue is the impartiality of the minister to preside over the application by the authorized persons envisaged under section 5(1) of the Act. A minister is a member of the executive, whose duties may overlap subordinating the authorized persons to him. As such, the degree of the minister's independence to act fairly in the adjudication of the facts surrounding the application before him or her is contentious. The Act

[68] See 'User Notification' in 'Necessary & proportionate - International principles on the application of human rights to communications surveillance' at 9. <https://necessaryandproportionate.org/files/en_principles_2014.pdf> accessed 19 August 2023.

[69] Interception of Communications Act, section 18(1). The right to administrative justice is guaranteed under s 68 of the Constitution of Zimbabwe; the Administrative Justice Act [Chapter 10:28] 'provide[s] for the right to administrative action and decisions that are lawful, reasonable and procedurally fair.'

[70] See 'Competent Judicial Authority' in International Principles on the Application of Human Rights to Communications Surveillance, 2014 (n 54).

violates these standards because the warrant regime is controlled by members of the executive and precludes independent and impartial judicial scrutiny. In 2014, using powers granted to him under the constitution, President Mugabe assigned the Act's administration to the Office of the President and Cabinet (OPC).[71] Further, there is obvious lack of an adversarial process in the interception and monitoring of the subject under ICA.

(C) Bulk Communication Surveillance

Bulk surveillance involves the state's monitoring and targeting of a huge section of the population on a continuous basis using digital technology. It also takes many varying digital forms, which may include the bulk retention of data, and bulk hacking.[72] Another comparable definition entails the use of bulk communications data techniques, and large-scale collection, retention and subsequent analysis of communications data.[73] Under analysis is the mass targeting of the population through bulk surveillance under section 9 of the Act, which as shall be argued is unconstitutional per se.[74] States and their national intelligence services are however keen to retain such contentious interception/surveillance powers under national security grounds that they help them pre-empt or prevent human rights violations that may occur, as a result of national security breaches.[75] This notwithstanding the impact such a law has on inverting the right to privacy, fair trial and freedom of expression. Often, states argue bulk surveillance is targeted against potential or real foreign threats, but conducting bulk interception using high capacity fibre optic cables that carry the world's internet communications between countries can easily target individuals within the same jurisdiction using social media messaging apps, such as WhatsApp, or Facebook.[76] There are international human rights law benchmarks that have been

[71] Statutory Instrument 19 of 2014, Assignment of Functions (Office of the President and Cabinet). The Statutory Instrument states that functions were assigned "in terms of s 104(1) of the Constitution, as read with s 37(2) of the Interpretation Act."

[72] J Duncan, 'The Future of Interception of Digital Communication' *Intelwatch, Policy Briefs*, 4 (2024) <https://intelwatch.org.za/wp-content/uploads/2024/01/the_future_of_bulk_interception_of_digital_communication_v4.pdf> accessed 5 February 2024.

[73] D Murray and P Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data', 52(1) Israel Law Rev at 31–60 (2019).

[74] Interception of Communications Act section 9 Assistance by service providers

(1) A service provider must ensure that—

(a) its postal or telecommunications systems are technically capable of supporting lawful interceptions at all times in accordance with section 12;
(b) it installs hardware and software facilities and devices to enable interception of communications at all times or when so required, as the case may be;
(c) its services are capable of rendering real-time and full-time monitoring facilities for the interception of communications;
(d) all call-related information is provided in real-time or as soon as possible upon call termination;
(e) it provides one or more interfaces from which the intercepted communication shall be transmitted to the monitoring centre;
(f) intercepted communications are transmitted to the monitoring centre via fixed or switched connections, as may be specified by the agency;
(g) it provides access to all interception subjects operating temporarily or permanently within their communications systems, and, where the interception subject may be using features to divert calls to other service providers or terminal equipment, access to such other providers or equipment;
(h) it provides, where necessary, the capacity to implement a number of simultaneous interceptions in order—
(i) to allow monitoring by more than one authorized person;

(2)(ii) to safeguard the identities of monitoring agents and ensure the confidentiality of the investigations;

(b) all interceptions are implemented in such a manner that neither the interception target nor any other unauthorized person is aware of any changes made to fulfil the warrant.

(1) A service provider who fails to give assistance in terms of this section shall be guilty of an offence and liable to a fine not exceeding level twelve or to imprisonment for a period not exceeding three years or to both such fine and such imprisonment.

[75] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 1.7. See from D Murray and P Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data', 52(1) Israel Law Rev 2019.

[76] Ibid D Murray and P Fussey at 5.

created to evaluate the constitutionality or legitimacy of statutory surveillance measures. The common three-step approach is widely recognized, and provides as follows:

> 'First, does a legal basis exist under domestic law, and is this legal basis of sufficient quality to protect against arbitrary interference with the rights of individuals? Second, does surveillance pursue a legitimate aim? Third, is the surveillance necessary in a democratic society –that is, does it answer a pressing social need and is it proportionate to the legitimate aim pursued?'[77]

In the Amabhungane case, a similar approach was followed by the apex court in invalidating bulk surveillance.[78] The court noted that there was no law providing for bulk surveillance, and thus invalidated the secretive conduct.[79] While section 9 of the Act might be providing such a framework for the conduct, it is not of sufficient quality to protect against arbitrary interference with the rights of citizens in that it is broad, undefined, and is a dragnet without a specific illustrated aim. The national security considerations may provide a legitimate aim, for a country not a war and peace with its citizens there is need to device a more appropriate legal framework. The uncontested political statements by erstwhile former Zimbabwe government ministers revealing the dark use of unlawful surveillance techniques on citizens have revealed more sinister politically motivated intentions that operate outside legitimate national security contemplations. From the foregoing, the three-test approach in testing the legitimacy of surveillance provisions becomes relevant. The test is also identical to the proportionality test[80] propounded in the *Chimakure v Attorney General* case.[81] The current section 9 Act lacks clear, coherent, precise terms for the bulk surveillance. Moreso, it does not provide the manner, circumstances or duration of the collection, gathering, evaluation and analysis of information gathered.

Nevertheless, investigating and holding the state to account for surveillance activities is a test in endurance, and it has been observed that in general it takes significant amount of pressure to shed a light on these practices, including taking governments to court, if considerations are had to the challenges faced by United States whistle-blower, Edward Snowden who revealed mass surveillance programmes in his country and the United Kingdom.[82] The South African government did not deny the net effect of bulk surveillance, which entailed intercepting internet traffic

[77] Ibid. Scholars Murray and Fussey note that this approach is broadly similar to the test established in relation to the International Convention on Civil and Political Rights (ICCPR) ((entered into force 23 March 1976) 999 UNTS 171) and the American Convention on Human Rights (Pact of San José, Costa Rica (entered into force 18 July 1978) 1144 UNTS 123). In these treaties reference is made to necessity and proportionality, but not always to the test of necessity 'in a democratic society'. See, for instance, the discussion of necessity in UN Human Rights Committee, General Comment No 34, Article 19: Freedoms of Opinion and Expression (12 September 2011), UN Doc CCPR/C/GC/34.

[78] *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) (3) SA 246 (CC).

[79] Ibid at para. 135.

[80] *Chimakure and Ors v The Attorney General Zimbabwe* SC 14–13 (A decision of the Supreme Court of Zimbabwe) 21–22, it provides that: 'The applicants must establish the following facts arising from the application of the three criteria of the proportionality test:

(a) That there is no rational connection between the restriction on the exercise of the right to freedom of expression and the objective sought to be achieved by the provisions of the statute.

(a) That even if there is a rational connection between the restriction on the exercise of freedom of expression and the objective pursued the means used to effect the connection do not impair the right to freedom of expression as little as possible. That would mean that there are other less intrusive means available which the legislature could have used to restrict the exercise of the right to freedom of expression to achieve the same objective.
(b) That the effects of the restrictive measure so severely trench on the right to freedom of expression that the legislative objective sought to be achieved is outweighed by the restriction on freedom of expression.'

[81] Ibid.

[82] News & Analysis 'South African Constitutional Court declares bulk surveillance powers unlawful' *PrivacyInternational.com*, 4 February 2021 <https://privacyinternational.org/news-analysis/4416/south-african-constitutional-court-declares-bulk-surveillance-powers-unlawful> accessed 20 August 2023.

without a warrant or suspicion about the people whose communications are intercepted.[83] To give a context to the impact and implications of the state's surveillance operations, it is important to assess the extent of Zimbabwe's population interaction with the Internet and digital technologies accessible to the state's surreptitious intrusions. Information made available from the GSMA Intelligence shows that in 2023 there were 14.08 million cellular mobile connections in Zimbabwe, representing 85.4 percent of the total population.[84] In the same period there are 5.74 million internet users in Zimbabwe, with about 1.50 million social media users equating to 9.1 percent of population.[85] Digital trends and behaviours are evolving, increasing scope for the state interest in the activities of its own citizens whose census figures totals 16.4 million. Half or more of the entire population can be subjected to massive ongoing interception, monitoring and or surveillance by the state.

It is submitted that there is no lawful basis for conducting bulk interceptions or monitoring of communications, especially where no suspicion of illegalities is in existence. Moreover, there is not any justification and or law of general application that can allow for such massive surveillance. Monitoring of communications constitutes exercise of public power, which must conform to constitutional parameters. Furthermore, the principle of legality requires that any exercise of public power must have a basis in some law, which therefore entails that bulk surveillance must be anchored on some legal basis or justification. The principle provides 'a mechanism to ensure that the state, its organs and its officials do not consider themselves to be above the law in the exercise of their functions but remain subject to it.'[86] Against this legal standpoint, bulk surveillance is being conducted without judicial authorization. Therefore, section 9 of ICA is inconsistent with the Constitution and invalid to the extent that they fail to regulate properly or at all bulk surveillance.

6. LIMITATION OF RIGHTS

It is common cause that state surveillance under the Act limit the right to privacy, fair trial and freedom of expression and the media. While it can be argued that the purpose and importance of state surveillance render surveillance under ICA reasonable and justifiable in the provided circumstances to combat serious crime, and guarantee national security, the overreaching scope of the surveillance is unreasonably intrusive rendering the limitation unjustifiable. Adoption of constitutional procedures and safeguards of intercepted communications in the surveillance can help ensure that issuance and execution of the warrants are done within acceptable constitutional parameters. The search and seizure warrants under section 49 of the Criminal Procedure and Evidence Act, provides procedural considerations to be followed in its execution. In *Mistry v Interim Medical and Dental Council of South Africa and Others,* the court persuasively held that: 'The existence of safeguards to regulate the way in which state officials may enter the private domains of ordinary citizens is one of the features that distinguish a constitutional democracy from a police state.'[87] The limitations provided to ICA are not permissible, having regard to the requirements of section 86 of the Constitution. There are available a range of less restrictive means that can be used to properly balance the legitimate interests of the state in pursuing surveillance when necessary on the one hand and the rights of members of the public on the other hand. The failure to make use of these less restrictive means without any proper explanation renders ICA unconstitutional in many respects.

[83] AmaBhungane Case (n 32) para 129.
[84] Simon Kemp 'Digital 2023: Zimbabwe' *Datareportal,* 14 February 2023. <https://datareportal.com/reports/digital-2023-zimbabwe#:~:text=Mobile%20connections%20in%20Zimbabwe%20in,total%20population%20in%20January%202023> accessed 20 August 2023.
[85] Ibid.
[86] C R Snyman, Crim Law (2008) 36.
[87] *Mistry v Interim Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC).

7. COMPARATIVE ANALYSIS WITH SOUTH AFRICA

The South African *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* case largely informed the constitutional parameters that should help define a progressive interception law in this contribution. It was thus used as a benchmark to illuminate the extent to which Zimbabwe's ICA corresponds with best global surveillance or interception practice. The most telling insights arises in the introduction to the Amabhungane case judgment, in which the court propounded the Constitution's provision that: '[n]ational security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life.'[88] This was informed by the colonial and post-apartheid government approach to surveillance laws whose,

> historical backdrop [... was}in [...] in pursuit of a skewed notion of national security [which] was weaponised and calculated to subvert the dignity of the majority of South Africans. As part of this pursuit, law enforcement involved searches of people, their homes, and their belongings. Over the years, law enforcement evolved to include the surveillance of people, their homes, their movements, and their communications. Today technology enables law enforcement agencies to not only physically – as opposed to electronically – invade the "intimate personal sphere" of people's lives, but also to maintain and cement its presence there, continuously gathering, retaining and – where deemed necessary – using information.

The *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* judgment is hailed as the court's powerful rejection of years of secret and unchecked surveillance by South African authorities against millions of people—irrespective of whether they reside in South Africa.[89] The court held that provisions of Regulation of Interception of Communications Act of 2002 (RICA) and the National Strategic Intelligence Act 39 of 1994 (NSIA) violated the right to privacy. Some of South Africa's surveillance legislative framework mirrored the apartheid government in violating the right to privacy and accompanying cognitive right dignity.[90]The Constitution guarantees the right to privacy[91] and dignity.[92] South Africa's apex court has previously in several precedents sought to draw the line between the past and present, helping shape and preventing recurrence of similar historical infringements.[93] Zimbabwe is not an exception in this transitional development from colonialism to independence carrying statutes and behavioural patterns that grossly invaded the right to privacy and freedom of the media. In *Gaertner v Minister of Finance,* the Constitutional Court draw parallels between pre and post-apartheid South Africa in respect for the right to privacy and dignity.

[88] AmaBhungane Case (n 32) para 1.
[89] Privacyinternational.com (n 54).
[90] W Nortje, 'Warrantless Search and Seizures by the South African Police Service: Weighing up the Right to Privacy versus the Prevention of Crime', (24) PER/PELJ 2021 http://dx.doi.org/10.17159/1727- 3781/2021/v24i0a8153
[91] Section 14 of the Constitution of the Republic of South Africa protects the right to privacy. Data protection laws: The Protection of Personal Information, Act 4 of 2013 (POPI) is the primary instrument regulating data protection in South Africa. See Currie and De Waal Bill of Rights Handbook 295–297.
[92] Section 10 of the Constitution of the Republic of South Africa provides for the right to human dignity: "Everyone has inherent dignity and the right to have their dignity respected and protected". Human dignity is a central value of the objective, normative value system established by the Constitution.
[93] See Amabhungane (n 32) para. 1. See also See R Madlalate 'Dismantling Apartheid Geography: Transformation and the Limits of Law', 9 Constitut Court Rev (2019) 195–217. <https://www.saflii.org/za/journals/CCR/2019/8.pdf>. See *Mazibuko & Others v City of Johannesburg & Others* [2009] ZACC 28, 2010 (4) SA 1 (CC). See also *Minister of Finance and Other v Van Heerden* 2004 (6) SA 121 (CC).

> many of the egregious searches were conducted at the dead of night: a time of relaxation; sleep; intimacy; reckless abandon even; and when some, if not most, would be flimsily dressed. The sense of violation and degradation that the victims must have experienced is manifest.[94]

Scholars observe that the 'horrors of the Apartheid regime are, however, still manifesting themselves in the post-democratic South Africa. The police are regularly faced with civil liability claims due to police brutality.'[95] Yet section 14 of the Constitution provides:

Everyone has the right to privacy, which includes the right not to have –

(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed.

The constitution has created and insulated the right to privacy from intrusions and interference by the state and others.[96] However, subsidiary legislation in the form of RICA created room for the gross interference with the right to privacy, and the right to freedom of expression and the media.[97] Prior to RICA's amendments it was identical to Zimbabwe's ICA in many respects. Both legislations failed to create safeguards for the protection of information collected from surveillance, did not provide judicial oversight into the issuance of warrants and offer specific safeguards against interference with privileges offered to practising journalists and lawyers in protecting sources of information and lawyer-client information. The *Amabhungane* judgment invalidated provisions that were inconsistent with the Constitution to the extent that they failed to provide safeguards referred to in the foregoing.[98] The court's interference with spying legislation that had all the hallmarks of an apartheid government is progressive given the court's reasoning in the Mistry case supra.

> When it came to racially discriminatory laws and security legislation, vast and often unrestricted discretionary powers were conferred on officials and police. Generations of systematised and egregious violations of personal privacy established norms of disrespect for citizens that seeped generally into the public administration and promoted amongst a great many officials habits and practices inconsistent with the standards of conduct now required by the Bill of Rights. [The right to privacy] accordingly requires us to repudiate the past practices that were repugnant to the new constitutional values, while at the same time re-affirming and building on those that were consistent with these values.[99]

When compared to the South African case we outline above, it is clear that Zimbabwe's ICA is inherently defective in its inability to protect these two communities of practice- lawyers and journalists. We have provided an outline of these failures in the preceding discussion. However, we should point out that even when compared to global standards of surveillance that we have outlined, the ICA is still a constitutionally defective legal instrument that is both inadequate in

[94] *Gaertner v Minister of Finance* 2014 1 SA 442 (CC) para. 49.
[95] W Nortje, 'Warrantless Search and Seizures by the South African Police Service: Weighing up the Right to Privacy versus the Prevention of Crime', (24) PER/PELJ (2021) <http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812021000100002>
[96] *Gaertner v Minister of Finance* 2014 (1) SA 442 (CC) para. 47.
[97] Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.
[98] AmaBhungane Case (n 32).
[99] *Mistry v Interim Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC).

its measures of protection and hopelessly anachronistic. Post-surveillance notification, for example, reflects transparency of surveillance practices, and should be an in-built measure within any surveillance law in countries that pronounce themselves as democracies. In the European Union, for example, R (87) 15 of the Council of Europe provides for post- notification measures. Post-notification measures, furthermore, adds respect to any justification of the necessity of surveillance. Judicial oversight is also important as a safeguard against the abuse of powers by agencies tasked with exercising surveillance. Judicial oversight ensures that these agencies are held to account, and also provides remedies and relief to individuals injured by these agencies. In other words, judicial oversight fences off fundamental rights from encroachment and violations by these agencies. Judicial oversight ensures the proportionality of surveillance by ensuring that these agencies are held to account for their actions. Furthermore, judicial oversight fences off fundamental rights and privileges of individuals from abuse by state institutions. Additionally judicial oversight ensures proper remedies for aggrieved lawyers and journalists.

Proper disposition of data post-surveillance is another fundamental flaw of Zimbabwe's ICA. In that vein, its absence means that surveillance in Zimbabwe operates as an aviation flight 'Blackbox'. No one knows what exactly is in it until crucial moments. ICA is weak in all these issues, making it a piece of law that can be weaponized. There is evidence to this day that it is already being used against opponents of the ruling party on the country. There are no measures of redress, constitutionally in-built in ICA as buffers of protection for lawyers and journalists, disastrously concluding that the institutions of surveillance are beyond reproach and incapable of exercising redress after an egregious injury to their rights.

7. CONCLUSION

The ICA is a repressive and restrictive legislation used to act against journalists, lawyers and ordinary citizens. While the Act severely interferes with the rights to privacy, freedom of expression and the media, fair trial and dignity, there are serious international implications in having such a law in its current form including requirements and Zimbabwe's obligations under international and regional human rights law. The freedom of expression and right to privacy are enshrined in various persuasive international instruments and protocols. Countries and state parties to these instruments are mandated to take positive steps towards the realization of such rights. There is scope for invalidating unconstitutional sections highlighted in this contribution and adequate measures to amend or repeal the Act, and safeguard against the arbitrary use of the interception powers against citizens require political will. This will provide room for a new act, or the amended one to align with global standards of surveillance as we outlined them in this paper. This takes the form of either repealing, and or emending ICA aligning it with the fairly democratic Constitution whose progressive teleological scope is informed by the need to break from the repressive historical past. Should ICA be repealed: a delineated, coherent, certain and precise surveillance law that conforms to best practice giving citizens circumstances and conditions in which public officers are authorized to carry out interceptions must be enacted.