Regulation of Digital Surveillance and the Impact on Civil Society in Africa:

Experiences from South Africa

AUGUST 2025

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

Regulation of Digital Surveillance and the Impact on Civil Society in Africa:

Experiences from South Africa

This report was prepared by our consultant Ms. Hlengiwe Dube with support from the International Center for Not-For-Profit Law (ICNL) Africa and digital teams.

Table of Contents

List of abbreviations

ACHPR	African Commission on Human and Peoples' Rights
AfCHPR	African Court on Human and Peoples' Rights
CCTV	Closed-Circuit Television
CJEU	Court of Justice of the European Union
ECtHR	European Court of Human Rights
GDPR	General Data Protection Regulation
GILAB	General Intelligence Laws Amendment Bill
HRDs	Human Rights Defenders
ICCPR	International Covenant on Civil and Political Rights
IMSI	International Mobile Subscriber Identity
IR	South African Information Regulator
NCC	National Communications Centre
NICOC	National Intelligence Co-ordinating Committee
NIS	National Intelligence Services
NHRIs	National Human Rights Institutions
NSIA	National Strategic Intelligence Act 39 of 1994
OECD	Organisation for Economic Co-operation and Development
OIG	Inspector General of Intelligence
POPIA	Protection of Personal Information Act
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
SAPS	South African Police Service
SSA	State Security Agency
UDHR	Universal Declaration of Human Rights
UNHRC	United Nations Human Rights Council

1. Introduction

The regulation of digital surveillance has become an urgent issue across Africa, with profound implications for human rights, particularly for human rights defenders (HRDs), journalists, and activists. In South Africa, digital surveillance intersects with broader concerns about privacy, freedom of expression, and political repression. As civil society increasingly uses digital platforms to challenge government actions and address issues such as corruption and social inequality, they face greater vulnerability to surveillance and harassment. This vulnerability is compounded by the country's political and historical context, which carries the legacy of apartheid-era surveillance, a tool of state repression used to monitor and suppress anti-apartheid activists.[1]

The digital surveillance ecosystem in South Africa is shaped by an interplay between state and non-state actors, with law enforcement agencies and intelligence services at the forefront. These actors, including the South African Police Service (SAPS) and the State Security Agency (SSA), deploy digital surveillance technologies for national security and law enforcement purposes. However, concerns about the transparency and accountability of these agencies have grown, particularly regarding the potential use of surveillance to monitor political opposition, civil society activism, and media practitioners. State surveillance practices are often shrouded in secrecy, leaving the public with limited knowledge of the extent of data collection and its purposes, further undermining trust in the system.

Post-apartheid South Africa initially focused its surveillance efforts on internal threats, but the global context, particularly the aftermath of the 9/11 attacks, led to the expansion of surveillance activities, including financial monitoring and anti-terrorism measures. The 2013 Edward Snowden revelations further heightened awareness of the risks associated with mass digital surveillance, sparking increased academic and civil society interest in the topic. While South Africa's intelligence agencies have evolved since the end of apartheid, challenges persist in ensuring that their surveillance practices align with democratic principles and human rights standards.

Surveillance, broadly defined, refers to the systematic monitoring and collection of data on individuals, groups, or activities, often without the knowledge or consent of those being monitored. It encompasses various forms, including electronic surveillance (monitoring digital communications such as emails, social media activity, and phone calls), mass surveillance (widespread monitoring of large populations), and targeted surveillance (focusing on specific individuals or groups, often based on their perceived threat to national security or political interests). Surveillance can be conducted through different means such as data collection, location tracking, internet monitoring, and physical sur-

1 J Duncan 'Stopping the spies: Constructing and Resisting the Surveillance State in South Africa' (2018) 57-64.

veillance.[2] The increasing use of digital surveillance technologies by state and private entities in South Africa and beyond has created a complex landscape where the tension between ensuring security and protecting individual rights becomes increasingly difficult to navigate. Practices such as mass data collection, location tracking, and online monitoring can lead to surveillance overreach, abuse of power, and a chilling effect on free speech. In a democratic society that enshrines rights to privacy, freedom of expression, and access to information, the challenge lies in ensuring that digital surveillance is conducted in a manner that is proportionate, transparent, and accountable.

South Africa is a signatory to numerous international human rights frameworks, including the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples' Rights (the African Charter). These frameworks obligate the country to uphold fundamental human rights, including the right to privacy, freedoms of expression, association, and association. Any surveillance undertaken should comply with the principles of legality, necessity, and proportionality in conformity with these frameworks. Despite these international commitments, the country's increasing use of digital surveillance technologies has raised significant concerns about its compliance with global human rights standards. The growing reliance on digital surveillance, by state and non-state actors, presents potential risks to individuals' privacy and other fundamental freedoms, complicating the balance between security imperatives and fundamental human rights.

While South Africa's legal framework on surveillance is well-established in certain aspects, it remains insufficient to address the rapidly evolving digital surveillance landscape. The Constitution[3] and other laws such as the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA)[4] and the Protection of Personal Infor-

Forms of digital surveillance

Internet surveillance
Monitoring online activities, including browsing history, social media interactions, and email communications.

Biometric surveillance
Use of biometric data such as fingerprints, facial recognition, and iris scans to monitor and verify identities.

Location tracking
Monitoring of the physical location of individuals through GPS and mobile phone data.

Social media monitoring
Analysis of social media platforms to gather information about public sentiment, trends, and individual behaviors.

Network surveillance monitors
Use of network traffic to detect and prevent unauthorized access, cyber threats, and data breaches.

2 This is a widely accepted understanding of surveillance. It incorporates elements commonly found in academic and legal definitions of surveillance, as well as in privacy and human rights literature. The concepts such as electronic surveillance, mass surveillance, and targeted surveillance are widely discussed in works that focus on privacy, human rights, and surveillance technologies.

3 Constitution of the Republic of South Africa, 1996 https://www.gov.za/documents/constitution/constitution-republic-south-africa-1996-04-feb-1997

4 Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13

mation Act (POPIA)[5] offer some safeguards. However, they fail to adequately address emerging technologies or provide robust protections against excessive surveillance practices. The 2021 Constitutional Court ruling, which declared parts of RICA unconstitutional due to inadequate privacy protections, underscored the need for stronger safeguards, particularly for vulnerable groups such as journalists, HRDs, and activists.[6] This ruling exposed significant gaps in the legal framework, especially regarding judicial oversight and protection against surveillance abuses.

The state's justification for digital surveillance often centres on national security and crime prevention, goals that align with broader global security trends. These objectives, while legitimate, have spurred concerns over the growing scope and impact of surveillance on human rights, especially in a post-apartheid society sensitive to issues of state overreach. Civil society groups and HRDs have raised alarms over the misuse of surveillance technologies, reporting instances of being tracked, harassed, and threatened through digital means, including anonymous messages and phone calls. The pervasive use of technologies such as facial recognition, biometric data, and artificial intelligence (AI)-driven systems has amplified these concerns, as activists face heightened personal risks, with some even relocating for safety.[7] The rise of private surveillance networks, such as Vumacam, which operates over 6,600 cameras in affluent areas, further exacerbates these fears.[8] These networks, often linked to both private security firms and government agencies, employ AI for tasks like license plate recognition, raising alarm over the potential for mass surveillance and its implications for privacy and other human rights.

Civil society groups and human rights defenders have raised alarms over the misuse of surveillance technologies, reporting instances of being tracked, harassed, and threatened through digital means, including anonymous messages and phone calls.

5 Protection of Personal Information Act (POPI Act) https://popia.co.za/section-37-regulator-may-exempt-processing-of-personal-information/

6 *AmaBhungane Centre for Investigative Journalism NPC and Stephen Patrick Sole v. Minister of State Security and Others* (CCT 20/19) [2019] ZACC 33 https://www.saflii.org/za/cases/ZACC/2021/3.html

7 KZN's environmental human rights defenders face murder, threats, intimidation — here are their stories https://www.dailymaverick.co.za/article/2024-12-09-kzn-environmental-human-rights-defenders-deadly-calling/ 09 Dec 2024

8 M Cronje 'South Africa's private surveillance machine is fuelling a digital apartheid' https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/ 19 April 2022

Also, the gaps in strong, independent oversight mechanisms and the failure to implement comprehensive privacy protections leave individuals vulnerable to potential abuses of power. The expansion of private surveillance networks and the increasing sophistication of state surveillance tools necessitate urgent legal reforms to ensure that surveillance practices are both accountable and human rights compliant. A careful and balanced approach is needed to protect the privacy rights of South Africans while addressing legitimate concerns related to national security and crime prevention.

This research examines the state of digital surveillance regulation and practices in South Africa, exploring its implications for civil society, governance, and human rights protection. It aims to highlight the challenges facing South Africa in balancing security concerns with the protection of democratic freedoms, and to propose the necessary steps for developing more effective, transparent, and accountable policies that respect human rights while addressing legitimate security needs.

2. Regulation of Surveillance and Interception of Communications in South Africa

2.1 NATIONAL LEGAL FRAMEWORK AND HUMAN RIGHTS PROTECTIONS

The Constitution

Privacy: Section 14 of the Constitution protects the right to privacy.[9] It recognizes privacy as a fundamental human right that is essential to the individual's autonomy and dignity. The right to privacy includes the right not to have their person, home, or property searched; not to have their possessions seized; and not to have the privacy of their communications infringed upon. This provision ensures that individuals are shielded from unwarranted government interference and from intrusions into their private lives by both state and non-state actors. The right to privacy under Section 14 is considered an important safeguard against arbitrary surveillance and data collection by the government, as well as a protection for personal and intimate aspects of an individual's life. The right to privacy similarly facilitates free expression, guaranteed in the Constitution, for individuals to form opinions, communicate and express themselves freely without fear of surveillance or retaliation.[10] However, Section 36 allows limitations on rights, including the right to privacy, if the limitation is reasonable, justifiable, and necessary in an open and democratic society, considering factors such as the nature of the right, the purpose and extent of the limitation, and whether less restrictive means could achieve the same goal.[11]

Security: The Constitution mandates that the State uphold national security in compliance with the law and international standards, with security services operating transparently and accountably. Parliamentary oversight, as defined by relevant legislation, ensures this. Sections 205-208 outline the establishment, responsibilities, and control of the police, and Sections 209-210 detail the establishment, powers, functions, and oversight of intelligence services.[12]

Protection of Personal Information Act (POPIA)

POPIA regulates the collection, processing, and storage of personal information by public and private bodies, ensuring protection of privacy.[13] Section 37 allows for exceptions

9 Constitution of the Republic of South Africa, 1996, Section 14. https://www.gov.za/documents/constitution/constitution-republic-south-africa-1996-04-feb-1997

10 Section 16 of South Africa's Constitution states that Everyone has the right to freedom of expression, which includes a. freedom of the press and other media; b. freedom to receive or impart information or ideas; c. freedom of artistic creativity; and d. academic freedom and freedom of scientific research.

11 Constitution of the Republic of South Africa, 1996, Section 36. https://www.gov.za/documents/constitution/constitution-republic-south-africa-1996-04-feb-1997

12 Constitution of the Republic of South Africa, 1996, Sections 205-210. https://www.gov.za/documents/constitution/constitution-republic-south-africa-1996-04-feb-1997

13 Protection of Personal Information Act (POPI Act) https://popia.co.za/section-37-regulator-may-exempt-processing-of-personal-information/

to privacy protections where broader societal interests (such as national security or the benefit to the data subject) are deemed to justify the interference with privacy. The Information Regulator is responsible for its implementation and enforcement and is established in terms of section 39 of the Act.[14]

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)

RICA governs interception of communications by state agencies.[15] It requires a designated judge to authorise surveillance and sets out procedures for interception, monitoring, and storing of data. The Act's main objectives are to regulate the interception of specific communications, the monitoring of signals and radio frequencies, and the provision of communication-related data. It also outlines the process for making applications for, and issuing, directions to authorise communication interception and data provision under particular circumstances. It also details the execution of these directions and entry warrants by law enforcement officers, as well as the assistance that postal services, telecommunication providers, and decryption key holders must offer during these operations. RICA further mandates that telecommunication services must be capable of interception, prohibiting those that lack this feature, and it specifies which telecommunication service providers are responsible for certain costs related to these activities. It also establishes interception centres, the Office for Interception Centres, and the Internet Service Providers Assistance Fund. Lastly, the Act prohibits the manufacturing, assembly, possession, sale, purchase, or advertising of certain interception equipment.

RICA has weaknesses that make it susceptible to abuse by intelligence agencies, failing to adequately protect the privacy of journalists, politicians, and citizens from arbitrary surveillance.[16] The vague standards for warrant authorization, based on speculative grounds of potential criminal activity, have led to concerns about infringement on professional confidentiality, particularly for

RICA has weaknesses that make it susceptible to abuse by intelligence agencies, failing to adequately protect the privacy of journalists, politicians, and citizens from arbitrary surveillance.

14 Information Regulator: https://inforegulator.org.za/

15 Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13

16 J Duncan 'The South African government's thinking on surveillance law is regressive' 4 June 2019 The Coversation https://theconversation.com/the-south-african-governments-thinking-on-surveillance-law-is-regressive-118185

journalists. These issues have prompted legal action and public calls for amendments to strengthen privacy protections. In 2021, the Constitutional Court declared some of its provisions unconstitutional due to lack of adequate safeguards on privacy, notification of subjects, and judicial independence.[17]

National Strategic Intelligence Act 39 of 1994 (NSIA)

The Act provides a structured approach to national intelligence, balancing security needs with constitutional compliance, and ensuring that various intelligence and security agencies work together effectively.[18] It outlines the responsibilities of the Agency in gathering, analysing, and correlating both domestic and foreign intelligence to identify and address potential threats to national security, excluding foreign military intelligence. It also covers counterintelligence duties, including supplying intelligence to relevant state departments such as the South African Police Service and the Department of Home Affairs, as well as the coordination of intelligence through the National Intelligence Coordinating Committee (NICOC). The Act also details the vetting process for individuals accessing classified information or national key points and mandates compliance with constitutional safeguards while performing these duties. A designated Minister is tasked with overseeing the efficient functioning of intelligence coordination and advising the President on strategic intelligence matters. The National Strategic Intelligence Act (NSIA) of 1994 was amended by the General Intelligence Laws Amendment Act 11 of 2013, expanding the functions of the State Security Agency (SSA). These amendments introduced new responsibilities related to cryptography, specifically outlined in section 2(2)(b) of the Act. The SSA is now tasked with: (i) identifying, protecting, and securing critical electronic communications and infrastructure from unauthorised access and various related threats; (ii) providing cryptographic and verification services for the security of electronic communications systems, products, and services used by government entities; and (iii) coordinating research and development in the field of electronic communications security and related services.

The Criminal Procedure Act (1977)

The Criminal Procedure Act (1977) allows judges or magistrates to require individuals to provide relevant information about alleged offences, potentially including private details like financial transactions or metadata from ISPs.[19] While this provision supports crime investigations, it must be applied in line with privacy and confidentiality principles, ensuring that information is gathered appropriately without infringing on individual rights.

17 See, AmaBhungane Centre for Investigative Journalism NPC and Stephen Patrick Sole v. Minister of State Security and Others (supra note 6). In that case, the South African Constitutional Court ruled that the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) was unconstitutional in part due to inadequate protection of the right to privacy. The court found that RICA lacked sufficient safeguards against state surveillance, including the lack of notification to individuals targeted for surveillance and insufficient judicial oversight.

18 National Strategic Intelligence Act 39 of 1994 https://www.gov.za/documents/national-strategic-intelligence-act

19 The Criminal Procedure Act (1977) https://www.justice.gov.za/legislation/acts/1977-051.pdf

The Intelligence Services Act of 2002

The Intelligence Services Act of 2002 was enacted to establish the National Intelligence Services, the South African National Academy of Intelligence, and the Intelligence Services Council on Conditions of Service.[20] The Act serves to regulate the operations and functions of these bodies. It also grants the Minister of Intelligence the authority to appoint senior officials, including the Deputy Director-General and Assistant Director-General, as well as to create various chief directorates and directorates within the intelligence services. The Act of 2002 is highly relevant to research on South Africa and digital surveillance as it outlines the legal framework governing the operations of the National Intelligence Service (NIS), which plays a key role in the country's intelligence and surveillance activities. The Act provides the mandate for the Minister of Intelligence to establish key positions and structures within the intelligence services, including roles such as Deputy Director-General and Assistant Director-General, which are critical for overseeing surveillance operations. The establishment of directorates and chief directorates also facilitates specialised functions, including digital surveillance and cybersecurity.

Intelligence Services Oversight Act (ISOA) 40 of 1994

The Act establishes a committee tasked with overseeing intelligence matters in Parliament, known as the Joint Standing Committee on Intelligence. It also provides for the appointment of the Inspector-General of Intelligence (OIGI), who is responsible for ensuring accountability and transparency within the intelligence services.[21]

General Intelligence Laws Amendment Act 11 of 2013

This Amendment Act was passed to revise several key pieces of legislation, including the National Strategic Intelligence Act of 1994, the Intelligence Services Oversight Act of 1994, and the Intelligence Services Act of 2002.[22] The Act also led to the repeal of the Electronic Communications Security (Pty) Ltd Act of 2002 to facilitate the creation of the State Security Agency, which absorbed various government components. The amendments made by this Act aim to address the legal and technical changes resulting from the dissolution of certain government entities and to introduce additional technical adjustments to existing laws.

Key legislative amendments and their human rights compliance

Following the Constitutional Court declaration of unconstitutionality of some provisions of RICA, Parliament amended it. The Department of Justice introduced the amendment over two years after the court's ruling, with the bill focusing mainly on

20 National Intelligence Services Act of 2002 https://www.gov.za/documents/intelligence-services-act

21 Intelligence Services Oversight Act. No. 40 of 1994.

22 General Intelligence Laws Amendment Act 11 of 2013 https://www.gov.za/documents/general-intelligence-laws-amendment-act-0

implementing the court's directives. In addition to the RICA amendment bill, other key amendments are found in the General Intelligence Laws Amendment Bill (GILAB) of 2023.

Legislation	Key points	Concerns/Issues
RICA Amendment Bill[23]	• Introduced by the Department of Justice over two years after the Constitutional Court's ruling. • Focused on post-surveillance notification and enhancing the independence of RICA judges. • Positive changes include post-surveillance notification and more independence for RICA judges.	• The bill's narrow focus mainly implements the court's directives, missing broader concerns. • Fails to address the Section 205 'loophole' in the Criminal Procedure Act, which allows police to access sensitive data with fewer safeguards, impacting journalists and others. • Lack of clarity on the implementation of safeguards (post-surveillance notification, number of judges overseeing decisions). • Weaknesses in the bill could make it prone to abuse, necessitating stronger oversight and clearer implementation mechanisms.
General Intelligence Laws Amendment Bill (GILAB)[24]	• GILAB was expected to address corruption, factionalism, and unlawful practices within the State Security Agency (SSA). • It seems to promote surveillance laws despite the Constitutional Court's ruling on mass surveillance.	• The bill uses the opportunity of the RICA judgement to introduce vague clauses, possibly expanding surveillance without proper oversight. • Potential to expand surveillance powers without adequate oversight, contradicting the intended reforms in the RICA amendment. • Concerns about the SSA leveraging the bill to entrench surveillance without accountability, particularly regarding the unlawful mass surveillance practices of the National Communications Centre (NCC).

2.2 KEY ACTORS IN PRIVACY, DIGITAL SURVEILLANCE AND INTERCEPTION OF COMMUNICATIONS ECOSYSTEM

South Africa's surveillance ecosystem consists of several key players:

The South African Police Service (SAPS)

The role of the SAPS is critical in that this is the entity that deploys digital surveillance technologies for law enforcement purposes. There are concerns about the manner in which they balance the state's obligation of public security and the protection of citizens' privacy rights, particularly in light of previous regulatory gaps. The weaknesses

23 See commentary here: M Hunter 'RICA bill misses the chance for real reform' 20 September 2023 Groundup https://groundup.org.za/article/rica-bill-misses-chance-for-real-reform/

24 See commentary here: Intelwatch: ' The two surveillance bills before Parliament that should give every South African pause for thought' 3 October 2023 https://intelwatch.org.za/2023/10/03/op-ed-the-two-surveillance-bills-before-parliament-that-should-give-every-south-african-pause-for-thought/

in existing legal frameworks, such as the RICA, which was initially designed to regulate the interception of communications and the collection of communication-related data for law enforcement and intelligence purposes, became worrisome particularly regarding inadequate safeguards for privacy, insufficient oversight mechanisms, and gaps in accountability. For instance, loopholes in judicial oversight allowed for the potential abuse and concerns that surveillance was being conducted without sufficient safeguards against abuse, leading to the 2021 court order to amend RICA.

The Information Regulator

Section 37 of RICA allows exceptions to privacy protections for broader societal interests, such as national security or the benefit of the data subject and plays a key role in regulating surveillance. It permits interference with privacy if data collection directly benefits individuals, such as protecting them from harm. The Information Regulator oversees compliance with privacy laws, ensuring that any exceptions, including those under Section 37, are applied lawfully, transparently, and justifiably. The Regulator must ensure surveillance actions meet legal requirements like proportionality, necessity, and transparency, while also providing mechanisms for individuals to challenge unlawful surveillance. Transparency in data collection practices is vital, and the Regulator must advocate for citizens' awareness when data is collected or surveilled. Clear guidelines and independent oversight are essential to prevent the arbitrary or excessive use of surveillance powers, ensuring privacy rights are respected.

Parliament

The Parliament shapes the legal and regulatory framework that governs intelligence and surveillance activities, ensuring that the laws balance national security concerns with the protection of human rights. Parliament's role includes overseeing intelligence and surveillance agencies, ensuring that they operate within the law and are accountable to the public. Parliamentary committees, such as the Joint Standing Committee on Intelligence (JSCI),[25] are tasked with monitoring the activities of the SSA, SAPS, and other intelligence agencies to ensure that their operations comply with legal standards.

The judiciary and the role of the courts

In 2021, in the *AmaBhungane* case, the Constitutional Court of South Africa delivered a landmark ruling on surveillance in South Africa.[26] It confirmed the High Court's ruling declaring the interception of communications legislation, RICA, unconstitutional for failing to protect privacy rights adequately. The court identified multiple flaws in RICA, including the lack of post-surveillance notification to subjects, failure to ensure the independence of the designated judge overseeing surveillance, insufficient safeguards

25 Joint Standing Committee on Intelligence: https://www.parliament.gov.za/committee-details/244

26 *AmaBhungane Centre for Investigative Journalism NPC and Stephen Patrick Sole v. Minister of State Security and Others* (CCT 20/19) [2019] ZACC 33 https://www.saflii.org/za/cases/ZACC/2021/3.html

for *ex parte* applications, poor management of intercepted data, and inadequate protections for journalists and lawyers' communications. The Court also dismissed the legality of bulk surveillance practices under the National Strategic Intelligence Act. The Court suspended the declaration of invalidity for three years to allow Parliament time to amend the law. The process of amending the law is ongoing and a Bill is in place.

Commissions of inquiry

Significant efforts have been made to address issues of intelligence operations and oversight through various review initiatives. In 2005, the Minister for Intelligence Services, Ronnie Kasrils, established a Task Team to assess the country's intelligence-related legislation, policies, and regulatory framework. The team, led by the head of the National Intelligence Coordinating Committee (NICOC), identified gaps in accountability and transparency in intelligence agencies such as the National Intelligence Agency (NIA), South African Secret Service (SASS), and the National Communications Centre (NCC). Key findings included concerns over the intrusive nature of intelligence operations, inadequate oversight, and a culture of non-accountability within the intelligence community. The Task Team recommended reforms to improve the authorization of operations, strengthen compliance monitoring, and promote a culture of professionalism and constitutionalism within the intelligence sector.[27]

Further reviews were conducted by the Ministerial Review Commission on Intelligence (2006-2008) and the High-Level Review Panel (2018) to assess the operations of South Africa's intelligence agencies. The Matthews Commission, in particular, highlighted unlawful mass surveillance by the NCC and criticised the lack of effective oversight by institutions like the Office of the Inspector-General of Intelligence (OIGI).[28] The High-Level Review Panel, appointed by President Cyril Ramaphosa, focused on the SSA and its governance, finding that politicisation and factionalism had undermined its integ-

Significant efforts have been made to address issues of intelligence operations and oversight through various review initiatives, beginning with a government-established Task Team in 2005.

27 Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies: Final Report of the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies April 2006 47.

28 Government of South Africa 'R Kasrils: Ministerial Review Commission on Intelligence' 1 November 2006 https://www.gov.za/r-kasrils-ministerial-review-commission-intelligence

rity and capacity.[29] Both reports called for greater accountability, enhanced oversight mechanisms, and a review of the intelligence community's governance structures. They emphasised the need for a clear national security strategy and better alignment of intelligence practices with constitutional and democratic principles.

The private sector

In the private sector, the role of companies in facilitating surveillance is a growing concern. Telecommunications companies, internet service providers, and social media platforms are integral players in the surveillance ecosystem due to their control over communication infrastructures and user data. In the case of South Africa, companies such as Vodacom, MTN, and Telkom are legally required under RICA to cooperate with law enforcement agencies by providing communication data.[30] While companies are generally required to ensure that access to personal data is only granted in specific circumstances, loopholes in the law and the ease with which companies can share data with state agencies without significant scrutiny are possible. The private sector's role in enabling surveillance is also exacerbated by the proliferation of big data and data analytics tools that allow governments and businesses to collect and analyse vast amounts of personal information. The increasing dependence on third-party vendors for surveillance technology also raises accountability concerns, particularly when private companies conduct surveillance operations on behalf of the state, further blurring the lines between state and corporate surveillance.

The private sector also supplies and supports the deployment of surveillance technologies. VASTech SA Pty Ltd,[31] a South African company founded in 1999, has become a significant player in the global surveillance technology market, providing tools for large-scale communication interception and data collection.[32] It has expanded its operations to offer systems capable of intercepting satellite, mobile, and internet communications. Its products, including *PORTEVIA*, *STRATA*, and *GALAXIA*, allow for the tracking of phone calls, texts, emails, social media, and geolocation data, making it one of the leading providers of surveillance technology worldwide.[33] VASTech sells these capabilities to governments, law enforcement, and military agencies, often without adequate regulation or oversight. Concerns have been raised about the company's sale of these tools to authoritarian regimes and their potential misuse against vulnerable groups, such as activists and dissidents. The company's ability to store and analyse vast amounts of personal data, including communications, raises significant privacy con-

29 High-Level Review Panel Report on the State Security Agency report (2018) 11 https://www.gov.za/sites/default/files/gcis_document/201903/high-level-review-panel-state-security-agency.pdf (accessed 5 August 2021).

30 RICA

31 Company's profile: https://www.vastech.co.za/

32 VASTech initially gained notoriety for supplying surveillance equipment to Muammar Gaddafi's regime.

33 The Intercept: 'South African Spy Company Used By Gadaffi Touts Its Nsa-Like Capabilities" https://theintercept.com/2016/10/31/south-african-spy-company-used-by-gadaffi-touts-its-nsa-like-capabilities/

cerns, especially given the growing partnership between the private sector and state agencies in surveillance efforts. This collaboration, largely unregulated, enables the widespread use of intrusive technologies like IMSI catchers, spyware, and biometric systems, further eroding privacy rights and increasing the risk of surveillance abuse.

Private security companies in South Africa play an increasingly significant role in digital surveillance, especially in urban areas, affluent communities, and gated residential estates. These companies typically have access to sophisticated surveillance technologies like CCTV cameras, drones, and facial recognition systems. In many cases, they operate in parallel with state efforts to monitor public spaces, creating a complex landscape of both private and public surveillance. The data collected by these private companies can sometimes be shared with law enforcement agencies, which raises concerns about the potential for mass surveillance. This type of collaboration between private security firms and the state can blur the lines between private and government surveillance and create potential privacy violations. A major issue is that, unlike state agencies, private security firms are not always subject to the same level of oversight or regulation. This can lead to situations where individuals are surveilled without their knowledge or consent, which can violate privacy rights. The lack of clear regulatory frameworks and oversight for private security companies amplifies concerns about the erosion of privacy and the development of a more pervasive surveillance state. These dynamics are a part of ongoing debates in South Africa and other countries about the balance between security and privacy, as well as the regulation of private surveillance companies to protect human rights. The expanding role of the private sector in digital surveillance highlights the need for clearer regulations and oversight to balance security with privacy rights.

> Private security companies in South Africa play an increasingly significant role in digital surveillance, especially in urban areas, affluent communities, and gated residential estates.

Civil society organisations (CSOs)

CSOs in South Africa play a key role in challenging excessive surveillance through advocacy, litigation, and public campaigns. They have shaped their responses to surveillance around concerns of privacy, human rights, and the risk of government overreach. With the growing use of surveillance

technologies like data collection, facial recognition, and online monitoring, these concerns have intensified. CSO responses include legal challenges, public campaigns, and international collaborations, all aimed at ensuring surveillance practices respect privacy and human other rights.[34]

The Right2Know Campaign has been instrumental in advocating for stronger privacy protections and challenging invasive surveillance practices, emphasising the constitutional right to privacy.[35] It has been critical of the legal framework which allows government surveillance for national security and law enforcement. It has held marches, issued public statements, and collaborated with international human rights organisations like Privacy International to raise awareness and promote global privacy standards, while also calling for greater oversight and accountability of government surveillance activities.[36] Privacy International also contributed submissions on the RICA Bill.[37] ALT Advisory has also been instrumental.[38]

Though their efforts are hindered by limited resources and other constraints. CSOs have immensely contributed to surveillance reform in South Africa.

34 A case in point is the scrutiny by CSOs of the General Intelligence Laws Amendment Bill 2023 (GILAB). A public statement was issued, singed by 48 organisations, highlighting concerns: https://privacyinternational.org/sites/default/files/2023-12/231206%20-%20GILAB%20joint%20statement%20-%20final.pdf

35 The Right2Know Campaign is a democratic, activist-led initiative that empowers citizens to raise awareness, mobilise communities, and conduct research and advocacy, with a goal of promoting the free flow of information, with a focus on three key areas: access to information, communication rights, and government transparency. http://www.r2k.org.za/

36 See example here as Amici Curiae to the RICA legal challenge: https://privacyinternational.org/legal-case-files/3386/pi-and-r2k-amici-curiae-constitutional-court

37 Privacy International: 'PI's response on proposed draft RICA Bill': https://privacyinternational.org/advocacy/5153/pis-response-proposed-draft-rica-bill

38 An example is a joint submission with the Right2Know Campaign to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: The Surveillance Industry and Human Rights. The submission addressed South Africa's regulatory framework, key actors, and incidents related to the export and use of surveillance technologies that undermine fundamental rights. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/ALT_ADVISORY_and_RIGHT2KNOW.pdf

3. Key Trends and Surveillance Practices: Technological Infrastructure and Digital Surveillance Mechanisms

Surveillance technologies in South Africa have become increasingly sophisticated, enabling the state and private entities to enhance their surveillance capabilities.[39] The country has adopted various tools such as biometric technologies, spyware, interception technologies, and closed-circuit television (CCTV) to conduct both targeted and mass surveillance. These technologies are used to monitor communication, track individuals, and provide enhanced data collection, with the government both importing and locally producing these surveillance tools. Key actors involved in surveillance include law enforcement agencies, intelligence services, and private telecommunications providers. These entities utilise tools like IMSI catchers or signal grabbers to intercept communications and track locations, often without proper judicial oversight.[40] Such devices can access metadata and track mobile phone signals by masquerading as legitimate mobile towers. Spyware like Finfisher and Pegasus has been used to monitor devices remotely, intercept calls, and collect data covertly. Biometric technologies, such as fingerprint and facial recognition systems, are also deployed for identity verification in areas like government services and crime prevention. These surveillance technologies raise concerns over privacy, regulation gaps, and the potential for misuse by state and non-state actors.

3.1 INTRODUCTION OF CCTV

The rapid and unregulated expansion of CCTV surveillance in South Africa has raised significant concerns regarding privacy violations, despite its promotion as an effective tool for crime deterrence and public safety. CCTV systems are now ubiquitous in public spaces like malls, highways, and businesses, as well as in private homes. However, this widespread surveillance operates within a largely unregulated framework, sparking debates about the protection of citizens' privacy, particularly as advanced technologies such as facial recognition and data collection tools become integrated into these systems. While POPIA aims to protect personal data, including CCTV footage, challenges remain in ensuring compliance with privacy laws while balancing security needs. This research advocates for a clearer regulatory framework under POPIA to govern CCTV use, ensuring that the benefits of surveillance do not come at the cost of eroding privacy and individual freedoms. It emphasizes the need for a coordinated approach to regulate the growth of surveillance technologies in a way that respects citizens' rights.

39 G Mutung'u 'Surveillance Law in Africa: a review of six countries: South Africa country report https://opendocs.ids.ac.uk/articles/report/Surveillance_Law_in_Africa_a_Review_of_Six_Countries/26435920

40 S Swingler 'Meet the Grabber: How government and criminals can spy on you (and how to protect yourself)' 1 September 2016 Daily Maverick https://www.dailymaverick.co.za/article/2016-09-01-meet-the-grabber-how-government-and-criminals-can-spy-on-you-and-how-to-protect-yourself/

The commercialisation of CCTV surveillance, driven largely by private security and insurance companies through public-private partnerships, complicates the balance between public safety and privacy. Private companies often promote CCTV systems as crime-reduction tools that also lower insurance premiums, presenting them as a smart investment for businesses and homeowners. However, this profit-driven expansion raises ethical concerns about excessive surveillance and the potential for privacy infringements, particularly when companies prioritize financial gain over human rights. It is crucial to conduct comprehensive impact assessments to ensure that crime prevention goals are met without undermining individual privacy. Accountability is also a major concern, as private companies involved in surveillance often face limited legal consequences for human rights violations. Despite POPIA's mandate for transparency and accountability in data collection, South Africa lacks a comprehensive regulatory framework for CCTV systems, leaving significant gaps. The absence of privacy impact assessments and public involvement in decision-making processes surrounding CCTV deployment further increases the risks of unchecked surveillance, underscoring the need for robust oversight to protect citizens' fundamental rights.

3.2 USE OF DRONES

Border management security

The use of drones by the Border Management Authority (BMA) at South Africa's ports of entry, such as the Beitbridge Border Post between South Africa and Zimbabwe, represents an example of digital surveillance aimed at enhancing border security and managing migration. This technological intervention, alongside the deployment of body cameras and push tokens, is designed to prevent illegal border crossings. Drones, in particular, provide real-time surveillance, allowing for the interception of individuals attempting to cross through vulnerable areas. By pinpointing unauthorized movements, drones strengthen traditional border control mechanisms.[41] However, the implications of this surveillance practice extend beyond

41 A Munyai 'The use of drones at the Beitbridge Border Post heeds success' SABC News 5 January 2025 https://www.sabcnews.com/sabcnews/the-use-of-drones-at-the-beitbridge-border-post-heeds-success/#:~:text=BMA%20Assistant%20Commissioner%20Nkhuliseni%20Luvhengo,to%20enter%20South%20Africa%20illegally

Key Surveillance Trends in South Africa

Introduction of CCTV

Now ubiquitous in public spaces.

Use of drones

Increasingly used in border security management and in public spaces.

Introduction of 'safe' and 'smart' cities

These projects use advanced technologies to monitor public spaces.

Use of facial recognition technology

Driven by private and government efforts to address issues such as identity theft, fraud, and terrorism.

Biometric-based digital identity system

A proposed national digital identity system would be required to access government services.

Video analytics and AI-powered surveillance

Used to detect unusual behaviours or activities, such as loitering or abnormal movement patterns.

Communications surveillance

Including mandatory SIM card registration and bulk data retention.

the realm of security, raising critical concerns about privacy, human rights, and the broader social impact. While drones may improve the efficacy of border enforcement, they also contribute to an increasingly militarized border environment, where the surveillance of individuals is omnipresent. This pervasive surveillance, while aimed at enhancing security, may also infringe on personal freedoms and privacy. Also, the use of such technologies raises complex ethical questions about the balance between securing borders and protecting the rights of individuals, particularly those engaged in legal migration processes. As such, there is a pressing need for policies that address the efficacy of surveillance technologies and mitigate their potential negative effects on the rights and experiences of border-crossers.

Public spaces

The use of drones as a surveillance practice in public spaces, such as beaches, has become an increasingly prevalent tool for law enforcement, blending advanced technology with traditional policing methods.[42] In this context, drones equipped with high-definition cameras are deployed to monitor public areas and identify offenders engaging in activities such as consuming alcohol in prohibited zones. This method offers significant advantages in terms of efficiency, enabling authorities to identify violations from great distances, undetectable to the human eye, and track offenders in real-time. The integration of drones with CCTV cameras is said to enhance the management of public spaces effectively, making it easier to pinpoint individuals who attempt to circumvent regulations by hiding alcohol or engaging in other unlawful acts. However, the implications of such surveillance practices are multifaceted, especially regarding privacy and the balance between security and individual rights. Critics argue that the extensive use of high-definition, omnipresent surveillance technologies raises concerns about the potential for invasive monitoring, particularly in sensitive environments like beaches, where individuals may be in a state of undress. The ethical question emerges as to whether such surveillance is necessary or if it infringes on the public's right to privacy.[43]

While drones may contribute to crime prevention and enhance public safety, their deployment should be carefully considered within the framework of privacy protection laws, such as those outlined in South Africa's Protection of Personal Information Act. Transparency in the use of drones is equally important. The public should be adequately informed about when and how these surveillance tools are employed. While drones may offer significant benefits in law enforcement, it is essential to address the potential for overreach, ensuring that surveillance measures are justified, proportionate, and aligned with constitutional privacy rights.

42 See K Engel 'Big Brother's beach watch — drones and CCTV spark privacy concerns in Cape Town' 7 January 2025 Daily Maverick https://www.dailymaverick.co.za/article/2025-01-07-big-brothers-beach-watch-drones-and-cctv-spark-privacy-concerns-in-cape-town/

43 As above.

3.3 INTRODUCTION OF 'SAFE' AND 'SMART' CITIES

Despite 30 years of democracy, South Africa remains one of the most unequal societies globally, with extreme poverty, unemployment, and inequality, contributing to some of the highest crime rates in the world. In response to these challenges, cities like Johannesburg and Cape Town have implemented "safe city" projects that integrate advanced technologies for monitoring and managing public spaces. Johannesburg's Integrated Intelligence Operations Centre (IIOC), for example, combines municipal data on one platform to enhance surveillance, while Cape Town focuses on real-time safety and policing analytics.[44]

In Gauteng province, South Africa, nearly 7,000 surveillance cameras equipped with facial recognition technology have been deployed to combat crime, with plans for further expansion, including additional drones.[45] Premier Panyaza Lesufi introduced the initiative, covering areas such as townships, suburbs, and informal settlements, with the aim of enhancing security. While some local communities support the initiative for its potential to reduce crime, including hijackings and killings, others raise concerns about privacy violations. This initiative is part of broader national efforts to tackle crime, including the introduction of a biometric system in Gauteng aimed at reducing carjackings. The growing use of facial recognition technology in law enforcement has sparked significant privacy concerns, particularly around potential misuse, racial profiling, and its application against protesters. This ongoing debate underscores the need for clear, ethical regulations to balance security with privacy.

Other technologies such as the advanced intelligence, surveillance, and reconnaissance (ISR)-equipped aircraft, a Cessna Caravan, are also deployed in Gauteng to combat crime (such as illicit mining and vandalism of infrastructure) and are part of a broader effort to enhance public safety and rapid police response.[46] The aircraft, which flies primarily at night, is fitted with a powerful Argos-II airborne observation system featuring infrared cameras and multiple sensors to detect criminal activity, including fires and what is considered as unusual behaviour. This system is being coordinated by Bidvest Protea Coin with support from private sponsors like FNB, Nedbank, and Engen. The initiative, which is also supported by local authorities and private security firms, draws inspiration from a similar project in Cape Town, where ISR technology has been used in various crime-fighting and public safety operations since early 2024.[47]

Cape Town is grappling with one of the world's highest crime rates including murder

44 https://saiia.org.za/research/the-city-surveillance-state-inside-johannesburgs-safe-city-initiative/

45 Government of South Africa: 'Gauteng fight against crime receives a boost of 6000 CCTV cameras' 19 February 2024 https://www.gauteng.gov.za/News/NewsDetails/%7Bd9772da6-941f-42e7-9549-801048fb204a%7D

46 'Bad news for Gauteng criminals' https://mybroadband.co.za/news/security/576354-bad-news-for-gauteng-criminals.html 15 December 2024 Mybroadband

47 'Bad news for Gauteng criminals' https://mybroadband.co.za/news/security/576354-bad-news-for-gauteng-criminals.html 15 December 2024 Mybroadband

and gang violence. As a result, the use of digital surveillance technology to combat crime continues to escalate.[48] This 'eye-in-the-sky' system forms part of a broader R610 million initiative to enhance safety, with R200 million earmarked for the current financial year. The aircraft's high-definition imaging capabilities allow for the detection of heat signatures from firearms, body heat in water, and speeding vehicles, providing crucial support for smarter policing. Beyond combating crime, the technology is also being used to monitor vital infrastructure, track poaching, and assess environmental issues. Integrated with other digital solutions like bodycams, license-plate recognition cameras, and drones, this tech-driven approach is revolutionizing policing in Cape Town. The aircraft's ability to cover larger areas, stay airborne for longer, and operate in various weather conditions makes it a versatile tool in operations aimed at tackling gang violence, poaching, and rapid-response interventions. Already, it has contributed to successful law enforcement actions, such as tracking poachers in Hout Bay, highlighting the growing role of digital surveillance in modern policing.

The city plans to invest R860 million approximately US$46.84 million) over three years in surveillance technology, including bodycams, license-plate recognition, drones, and expanded CCTV coverage, as part of a broader R5.8 billion safety budget. It is envisaged that this technology will aid crime prevention by enhancing data analysis. While the crime prevention function is often fronted as a justification, there are concerns about privacy and the gaps in regulation of surveillance data.[49]

Similarly, the expansion of these surveillance systems raises significant ethical concerns. The reliance on public-private partnerships, such as Johannesburg's collaboration with IBM and private firms like Vumacam, creates transparency issues and raises doubts about the true effectiveness of these technologies in reducing crime. The use of mass surveillance technol-

Cape Town plans to invest R860 million (approximately US$46.84 million) over three years in surveillance technology, including bodycams, license-plate recognition, drones, and expanded CCTV coverage, as part of a broader R5.8 billion safety budget.

48 The city has significantly advanced its crime-fighting efforts through a multimillion-rand investment in aerial surveillance technology, including the deployment of a Cessna 337 aircraft equipped with infrared cameras. See S Mzekandaba 'Cape Town's crime fight takes to the skies' https://www.itweb.co.za/article/cape-towns-crime-fight-takes-to-the-skies/Pero37Z3GrOMQb6m

49 Thomson Reuters Foundation: K Harrisberg 'Cape Town turns to surveillance tech to stop a tide of violence' https://www.reuters.com/article/markets/commodities/feature-cape-town-turns-to-surveillance-tech-to-stop-a-tide-of-violence-idUSL8N3664PO/ 19 April 2023

ogies, especially AI-powered cameras, threatens privacy rights and could undermine other human rights. Legal frameworks like the Protection of Personal Information Act provide some safeguards but are often insufficient to address the scale of potential privacy violations.[50]

The privacy issues emanate from concerns that emerging South African smart cities face significant challenges to data security and privacy, including poor governance, skills shortages, lack of awareness, and insufficient funding. Weak oversight, non-compliance with data security laws, and ineffective public-private partnerships exacerbate these issues. Also, a shortage of cybersecurity professionals and limited awareness among citizens and employees, heightens vulnerability to cyber threats such as phishing and ransomware. Inadequate funding further hampers the implementation of robust security measures. Together, these factors leave smart cities vulnerable to data breaches and cyberattacks, highlighting the urgent need for improved governance, skill development, and investment in cybersecurity.[51]

Companies like the Chinese Huawei and ZTE, play a key role in expanding surveillance networks in South Africa by providing cheaper digital infrastructure for video surveillance and 4G networks. This is part of China's Belt and Road Initiative (BRI), which promotes "smart city" projects across Africa.[52] Thus, while these AI-powered surveillance systems that are part of smart cities are believed to enhance security and urban management, they also raise significant privacy and human rights concerns, particularly regarding mass surveillance and the potential for abuse by state security agencies.

3.4 USE OF FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology (FRT) is rapidly expanding in South Africa, driven by private and government efforts to address issues such as identity theft, fraud, and terrorism.[53] FRT is transforming traditional surveillance systems by integrating AI, machine learning, and big data analytics to enable proactive 24/7 monitoring with automated facial identification, demographic analysis, and risk mitigation. This technology, which tracks and analyses behaviour to detect criminals and improve security at events, airports, and casinos, is now more accessible to businesses like Ideco[54], which is bringing it to South Africa for functions such as fraud prevention and VIP protection.

50 https://saiia.org.za/research/the-city-surveillance-state-inside-johannesburgs-safe-city-initiative/

51 https://sajim.co.za/index.php/sajim/article/view/1847/2948

52 The Belt and Road Initiative (BRI) is a global development strategy launched by China in 2013, aimed at enhancing trade and infrastructure connectivity across Asia, Africa, and Europe. It seeks to expand China's economic influence through infrastructure investments while promoting economic interdependence and creating opportunities for technological and political leverage. See 'Understanding China's Belt and Road infrastructure projects in Africa https://www.brookings.edu/articles/understanding-chinas-belt-and-road-infrastructure-projects-in-africa/

53 Legal Resources Centre: D Turner and J Khan 'The Use of Facial Recognition Technology in South Africa' August 2024 https://lrc.org.za/wp-content/uploads/The-Use-of-Facial-Recognition-Technology-in-South-Africa_FINAL.pdf

54 https://www.ideco.co.za/

Advances in high-speed internet and biometric technologies have led to increased use of FRT in sectors like border control, government services, security, and digital banking. Banks, for instance, adopted it to combat fraud. However, the technology raises significant concerns around privacy, security, and bias, particularly with risks of mass surveillance, data breaches, and discrimination due to algorithmic biases. While South Africa has laws such as the POPIA and the Cybercrimes Act, the rapid pace of technological development has outpaced these legal frameworks, raising concerns over regulation of biometric data use. There is a need for development of localised, ethically sound biometric systems that respect constitutional rights including privacy; regular audits, context-specific algorithms, and robust cybersecurity to mitigate risks.

3.5 BIOMETRIC-BASED DIGITAL IDENTITY SYSTEM

Biometric surveillance is also ubiquitous and growing rapidly, mainly enabled by government partnerships with the private sector. Also, AI and machine learning continue to enhance biometric technologies. As part of digital transformation across various departments and broader strategy to modernise government operations, South Africa is working on developing a national digital identity system aimed at providing a unified credential for access to government services.[55] This includes the collection of fingerprints and facial scans at points of entry like airports, which are linked to national and international security databases to build risk profiles on individuals. The initiative seeks to address the challenges posed by the use of multiple identification numbers for different services, such as tax, health, and business registrations, which can create opportunities for fraud. For instance, devices like the iFace302 provide quick verification speeds and streamlining identification.

The new biometric-based digital identity system (NIS) is part of broader digital transformation efforts.[56] The proposed digital ID system, includes both a unique digital identifier and a physical card, aims to reduce identity duplication and improve efficiency. In the context of the Home Affairs Department, it is envisaged to streamline and digitize processes like birth, marriage, and death registrations. As part of a 10-year plan from the Department of Home Affairs, the NIS will integrate both biographic and biometric data, improving service delivery in civic and immigration systems. The digital transformation will also replace traditional laminated driving licenses with smart card versions, incorporating advanced technologies like blockchain.[57]

The South African government is rolling out its Automated Biometric Information System (ABIS), which uses technologies like facial recognition and fingerprint scanning, designed to enhance identity verification, border control, and national security. Bio-

55 C Burt 'South Africa begins work on national digital ID to stem fraud' 6 November 2024 https://www.biometricupdate.com/202411/south-africa-begins-work-on-national-digital-id-to-stem-fraud

56 https://www.biometricupdate.com/202412/home-affairs-central-to-south-africa-digital-government-strategy

57 These new licenses mirror international standards and are meant to improve service efficiency, with future plans to introduce electronic driving licenses.

metric systems are also integrated into migration and border control processes, with the Department of Home Affairs (DHA) utilising biometric data to enhance security. This system collects biometric data from citizens and foreign visitors, and interfaces with agencies such as the South African Police Service for crime prevention and identification purposes. The government is also exploring the use of similar biometric technologies for visa processes issuance and other related services, to reduce identity fraud, and streamline access to services, with a focus on digital transformation across various departments.

Facial biometrics are also prevalent in the banking sector. Absa Bank introduced AbsaID Facial Biometrics, an advanced security feature on its banking app that leverages facial recognition technology to enhance digital banking security.[58] By linking a user's unique facial features to their mobile device, the technology enables secure access to the banking app, allows for easy resetting of passcodes and PINs, and simplifies the account linking and transaction processes.

Using facial mapping for verification, AbsaID ensures that only the authorized user can access the account, offering a streamlined and secure banking experience. The technology has received global recognition, winning the Best Digital Innovation Initiative at the Digital Banker Middle East & Africa Innovation Awards in 2021. To set up AbsaID, users need the latest version of the Absa Banking App, a valid cell phone number, and an identification photo from the Department of Home Affairs.[59]

The growing use of biometric surveillance in South Africa to bolster security is also enabled by organisations such as the Council for Scientific and Industrial Research (CSIR)[60] which develops comprehensive biometric recognition systems for security through face, body, and number plate recognition technologies, in private and state-owned entities.[61] This system integrates various recognition technologies to monitor and track activities, particularly addressing access control challenges in

> The South African government is rolling out its Automated Biometric Information System (ABIS), which uses technologies like facial recognition and fingerprint scanning, designed to enhance identity verification, border control, and national security.

58 ABSA: https://www.absa.co.za/self-service/absa-id-facial-biometrics/#:~:text=AbsaID%20Facial%20Biometrics%20is%20a,to%20create%20even%20greater%20security.

59 https://www.absa.co.za/self-service/absa-id-facial-biometrics/

60 CSIR: https://www.csir.co.za/csir-brief

61 Id.

secure facilities. Initially deployed at the South African Army headquarters in October 2020, it tracks the movement of both vehicles and people.[62] This development reflects South Africa's increasing reliance on biometric surveillance for enhancing security, yet it raises concerns about the balance between safety and privacy, particularly as the system expands to other high-security facilities.

The adoption of biometric facial recognition technology across various sectors, including healthcare, retail, banking, law enforcement, and transportation, while enhancing security, efficiency, and user experience, also raise privacy and data protection concerns, particularly in relation to issues such as algorithmic bias and discrimination, consent, data ownership, and the potential for mass surveillance. Other concerns include discriminatory profiling, and infringements on the right to freedom of movement. Also, individuals may be unaware that their biometric data is being collected. These concerns are exacerbated by the continuous improvement of AI and machine learning, which enhance accuracy and real-time processing. However, without adequate regulatory frameworks to safeguard personal data, ensure informed consent, and prevent misuse, the risk of surveillance increases. Gaps in the legal framework, including the absence of clear regulations that govern the use of FRT and biometric data, enables widespread surveillance without adequate safeguards, potentially infringing on citizens' fundamental constitutional rights. For instance, the Department of Home Affairs' draft policy also suggests biometric data might be shared without court orders for national security purposes, heightening concerns about transparency, accountability, and the erosion of individual privacy rights.

3.6 VIDEO ANALYTICS AND AI-POWERED SURVEILLANCE IN SOUTH AFRICA

AI-driven video analytics is rapidly expanding in South Africa, powering advanced surveillance systems that analyse real-time footage to detect unusual behaviours or activities, such as loitering or abnormal movement patterns. Technologies like gait recognition, which identifies individuals by the way they walk, are enhancing identification capabilities even when facial recognition is not feasible, offering a new layer of tracking. However, despite these advancements, AI-powered surveillance systems are still imperfect and prone to errors, such as misidentifying animals or vehicles as people, or generating false alerts in suboptimal visual conditions. Even with deep learning systems, which are more accurate, misidentifications persist, highlighting the limitations of current technology and the continued need for human oversight in interpreting and responding to AI-generated alerts.[63]

62 The system incorporates camera imaging and modules for facial and body recognition, with future plans to integrate biometric identification for two-factor authentication, further strengthening access security.

63 https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf

3.7 COMMUNICATIONS SURVEILLANCE

a. Mandatory SIM card registration

SIM card registration is mandatory under RICA, requiring users to submit personal details, including full name, identity number, and proof of residence, to authenticate their identity. The registration links the SIM card to the user, enabling traceability of communications. Service providers must retain metadata for 3 to 5 years, and activating a SIM without registration is illegal.

b. Communications data retention

International human rights standards regarding bulk data retention are shaped by various international frameworks that emphasise the protection of privacy, freedom of expression, and the right to a fair trial. While there is no single, universal legal standard for bulk data retention, key principles have emerged from international human rights law, especially in relation to surveillance practices, data privacy, and state powers. The principles of necessity, proportionality, transparency, and oversight are central to the discussion on data retention. Some of the key international human rights principles that govern bulk data retention include:

Human Rights Standard	Relevant Law/Case	Key Principle/Requirement
Right to Privacy	• UDHR, Article 12 • ICCPR, Article 17	• Protection from arbitrary or unlawful interference with privacy. • Any interference with privacy must be lawful, necessary, and proportionate to the legitimate aim pursued.
Necessity and Proportionality	• ECtHR, Digital Rights Ireland (2014) • CJEU[64], Schrems II (2020)	• Data retention must be necessary for a legitimate purpose (crime prevention, national security). • Measures must be proportionate, avoiding excessive or overly broad data collection.
Data Protection and Privacy Laws	• GDPR (EU Regulation 2016/679) • Council of Europe Convention 108	• Personal data must be processed lawfully, transparently, and for a specific purpose. • Data retention practices should comply with data protection principles like necessity and minimization.

64 An analysis of the approach of the on data retention: V Mitsilegas Et Al 'Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks' (2022) European Law Journal 1-36 https://pure.port.ac.uk/ws/portalfiles/portal/61649342/Data_retention_and_the_future_of_large_scale_surveillance_PDF.pdf

European Court of Human Rights (ECtHR) Rulings	• Digital Rights Ireland Ltd. v. Minister for Communications (2014) • Roman Zakharov v. Russia (2015)	• Blanket data retention violates the right to privacy. • Data retention measures must be specific and targeted, not indiscriminate.
Right to Freedom of Expression	• ICCPR, Article 19	• Bulk data retention can violate freedom of expression by having a chilling effect (self-censorship). • Surveillance should not unnecessarily restrict the ability to freely express oneself.
Judicial Oversight and Safeguards	• UN Special Rapporteur on Privacy	• Surveillance practices should be subject to independent judicial oversight. • Legal challenges should be available to ensure compliance with human rights standards. • Oversight ensures data retention is lawful and proportionate.
Transparency and Accountability	• OECD Privacy Guidelines • Council of Europe Convention 108	• Governments should be transparent about their data retention practices (legal basis, purpose, scope). • Individuals should be informed about data collection and retention.
International Legal Challenges	• CJEU, Schrems II Case (2020)	• Bulk data retention in non-EU countries must meet EU standards for privacy protection. • Data retention should not violate international privacy standards or data protection rights across borders.

The data retention period mandated by South Africa's RICA 2002 law is 3 to 5 years. This was challenged in 2021, the Constitutional Court upheld it, while calling for stricter safeguards around law enforcement access. These include requirements for law enforcement to disclose if their targets are journalists or lawyers when seeking interception warrants, though this only applies to RICA procedures, not criminal law procedures. While RICA covers all ISPs, it currently lacks regulations specifically for ISPs, with data retention practices being defined only for mobile and fixed-line operators. Individuals have limited recourse to challenge data retention, though they can file complaints with the Information Regulator, and oversight is mostly restricted to judicial review when law enforcement accesses data. There is no current time limit for data retention after law enforcement or intelligence agencies have accessed it, though a 2021 ruling by the Constitutional Court mandated amendments to introduce such safeguards.[65]

65 See Privacy International: 'PI's Briefing on National Data Retention Laws', 19 March 2024 https://privacyinternational.org/report/5267/pis-briefing-national-data-retention-laws

In response to the Constitutional Court's judgement, Parliament issued a revised version of RICA, as of August 2023. There are concerns regarding the proposed legislation's compliance with international human rights standards, especially regarding bulk data retention. The revised law introduces Article 37A, which outlines data management procedures for data obtained through communication interception. While it applies to telecommunications providers, it fails to set a specific retention time limit, only stating the need to establish one. Individuals have limited recourse to challenge data retention, though they can file complaints with South Africa's Information Regulator. Oversight is mainly judicial, triggered when law enforcement seeks or accesses data. The law currently lacks a time limit for retained data accessed by law enforcement or intelligence agencies, but the 2021 Constitutional Court ruling required Parliament to amend the law to introduce such safeguards.[66]

66 See Privacy International: 'PI's Briefing on National Data Retention Laws', 19 March 2024 https://privacyinternational.org/report/5267/pis-briefing-national-data-retention-laws

4. Digital Surveillance and Impact on Civil Society Actors

As is the case globally, digital surveillance in South Africa is becoming an increasingly powerful tool for state security and political control, impacting a wide range of civil society actors, including HRDs, journalists, and at-risk groups, particularly those engaged in activism, protests, and human rights work. The state's use of surveillance technologies has raised significant concerns, particularly when these tools are employed to monitor, intimidate, or suppress dissenting voices. Monitoring of protests and tracking online communications makes the digital space a battleground for freedom of expression, privacy, and activism, hence the role of surveillance in stifling civic engagement becomes more pronounced. The impact of digital surveillance on civil society actors is not limited to the immediate threat to individual safety but extends to the broader consequences for democratic engagement.

The following table highlights how surveillance manifests in the digital space and the direct impact on key civil society actors in South Africa:

CSOs, Human Rights Defenders and At-Risk Groups (such as students)
Impact: • Digital surveillance on CSO communications and funding sources, especially those involved in activism or human rights work. • Increased risk of surveillance as HRDs engage in activism related to police brutality, land rights, and corruption. • Profiling of at-risk groups, especially those involved in protests or social justice movements.
Manifestation of Impact: • Monitoring of online communications, email tracking, surveillance of meetings and events. • Monitoring of social media, phone tapping, facial recognition at protests. • Collection of personal data, surveillance of protest actions, use of algorithms to target individuals.
Connection to Protests, Police Brutality, and Repression: • CSOs advocating for social justice, racial equality, or anti-corruption may be surveilled, especially during protests or public campaigns. This can lead to harassment, discrediting, or government intervention. • HRDs can be targeted by surveillance to silence their opposition to state abuse, particularly in exposing police brutality, leading to intimidation or even arrest. • Groups participating in protests face heightened surveillance, potentially leading to criminalization or suppression of their movements.

Example: Research by the Right2Know Campaign has highlighted numerous instances where political and community activists critical of the state or ruling party, particularly those involved in regular protests, have been subjected to physical surveillance, harassment, and threats by security and intelligence agencies. The research showed a connection between physical surveillance and communication interception. The cases were not effectively investigated by law enforcement, intelligence, or oversight bodies and no criminal prosecutions were initiated.[67]

Protestors

Impact: Surveillance during protests, creating a climate of fear.

Manifestation of Impact: Real-time tracking through mobile devices and police presence at protest sites.

Connection to Protests, Police Brutality, and Repression: Protestors involved in movements face digital surveillance, including phone tapping and social media monitoring, leading to arrests, harassment, or excessive police violence.

Journalists

Impact: Risk of surveillance aimed at silencing investigative journalism or exposing state corruption.

Manifestation of Impact: Tracking of movements, data breaches on sources or stories.

Connection to Protests, Police Brutality, and Repression: Journalists reporting on police violence, state capture, or corruption are at risk of being surveilled, creating a chilling effect and limiting investigative journalism.

Example: In 2018 the Right2Know Campaign released a report titled Spooked: Surveillance of Journalists in South Africa, which examines 10 case studies of surveillance targeting journalists. The report includes how surveillance occurred, who was responsible, and the broader implications for press freedom. The report aims to provide journalists with a clearer understanding of the risks they face, enabling them to better protect themselves, and to mobilise the public to support the campaign to end these abuses and the problematic policies that enable them.[68]

67 Media Policy and Democracy Project; 'The Surveillance State: Communications surveillance and privacy in South Africa' March 2016 15 https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf

68 M Hunter 'South Africa's State of Surveillance: How Journalists Are Targets for Spying' 24 July 2018 https://gijn.org/stories/south-africas-state-of-surveillance-how-journalists-are-targets-for-spying/. The report can be accessed here: https://sanef.org.za/wp-content/uploads/2024/10/R2K-Surveillance-of-Journalists-Report-2018-web.pdf

Digital Activists

Impact: Digital surveillance on online movements pushing for change, especially on issues like anti-corruption.

Manifestation of Impact: Tracking of online campaigns, social media posts, and participation in virtual protests.

Connection to Protests, Police Brutality, and Repression: Activists organizing protests against police brutality or for social justice are often tracked by state surveillance tools, contributing to a stifling of free expression and online activism.

Whistleblowers

There is currently no research on the impact of surveillance on whistleblowers in South Africa, but there is a high risk that digital surveillance targets those exposing misconduct or corruption. Whistleblowers face similar risks to journalists and human rights defenders, including the monitoring of emails and social media, which can lead to cyberbullying, online harassment, retaliation, legal threats, or public defamation. Surveillance of journalists also directly affects whistleblowers, as it creates an environment of fear and repression for those revealing sensitive information.[69]

69 Reports such as this one highlight the extensive plight of whistleblowers in South Africa. Open Democracy Advice Centre: 'Heroes Under Fire: South African Whistleblower Stories' (2015) https://opendemocracy.org.za/images/docs/publications/HeroesUnderFire.pdf

5. Impact of Digital Surveillance on Human Rights in South Africa

Digital surveillance in South Africa poses serious risks to human rights as it disproportionately targets those who challenge the status quo. While the state justifies surveillance for national security, it often leads to, for instance, self-censorship among activists and journalists, undermining core democratic values like freedom of expression and accountability. Journalists, in particular, face threats to both their safety and their ability to protect sources, while surveillance of both online activity and physical movements makes it easier for authorities to suppress dissent. This erosion of freedom of speech and press ultimately weakens democracy.

> Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimisation.[70]

The table below outlines the impact of digital surveillance on key human rights in South Africa, including the right to privacy, freedom of expression, freedom of association, freedom of assembly, and access to information.

Human Right	Impact
Right to Privacy	• Surveillance practices enable the state and non-state entities to monitor individuals' communications and personal data. This undermines the constitutional right to privacy (Section 14 of the Constitution) for activists and journalists, and protestors whose personal information is targeted and used to control or intimidate them.[71] • Professional confidentiality: Surveillance of lawyers poses serious privacy concerns, particularly regarding the confidentiality of communications between lawyers and their clients, which is essential for a fair trial and justice. When lawyers are under surveillance, their professional privilege is compromised, as seen in cases like the interception of communications involving South Africa's Legal Resources Centre by the UK's GCHQ, and the amaBhungane case. These breaches undermine the right to a fair trial, as legal professional privilege is vital for encouraging full and frank disclosure between clients and lawyers.[72]

70 United Nations Human Rights Council: F La Rue 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (2013) A/HRC/23/40 para 24 https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed 12 October 2021).

71 Privacy International, the Association for Progressive Communications & the Right2Know Campaign: 'The Right to Privacy in South Africa' https://privacyinternational.org/sites/default/files/2017-12/PI%20submission%20South%20Africa%20FINAL.pdf

72 J Duncan Stopping the Spies: Constructing and resisting the surveillance state in South Africa (2018) 115 & 199.

Freedom of Expression	• The pervasive nature of digital surveillance limits freedom of expression by discouraging individuals from speaking out against the state. • Existing research including the Right2Know Campaign reports, indicate that journalists and HRDs who engage in sensitive topics such as corruption are often targets of surveillance, creating a chilling effect that restricts the open exchange of ideas and the press' ability to hold the government accountable.
Freedom of Association and Assembly	• The Constitution provides for the right to demonstrate, petition and assemble. • Discontent among workers in the mining sector has fueled activism, with groups like the National Union of Metalworkers (NUMSA) and the Association of Mineworkers and Construction Union (AMCU) becoming targets of state surveillance. Their social justice activities, which often include protests, have led to increased monitoring of their leaders' communications, social media, and emails. This surveillance creates a chilling effect, with activists operating in fear that their plans for protests could endanger their safety and well-being.[73]
Access to Information and Whistleblowing	The impact of surveillance of journalists and other media practitioners directly impacts access to Information and whistleblowing. When journalists are monitored, the right of the public to be informed is undermined.

73 A Mare as cited in J Duncan Stopping the Spies: Constructing and resisting the surveillance state in South Africa (2018) 196.

6. Actionable Recommendations to Counter Illegitimate Surveillance

This section presents a set of actionable recommendations designed to counter the practice of illegitimate surveillance, grounded in international human rights standards. Central to these recommendations is Principle 41 of the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa,[74] which provides clear guidance on the limits of state surveillance and the protection of individual privacy. According to the Principle:

> 1. States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications.
>
> 2. States shall only engage in targeted communication surveillance that is authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.
>
> 3. States shall ensure that any law authorising targeted communication surveillance provides adequate safeguards for the right to privacy, including:
>
> - the prior authorisation of an independent and impartial judicial authority.
> - due process safeguards.
> - specific limitation on the time, manner, place and scope of the surveillance.
> - notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance.
> - proactive transparency on the nature and scope of its use; and
> - effective monitoring and regular review by an independent oversight mechanism.

The proposed actionable recommendations identify several key stakeholders, each of whom has a critical role to play in ensuring that surveillance practices are conducted in a manner that respects privacy, promote accountability, and align with human rights standards. The following recommendations outline specific actions each group should take to address the growing challenges posed by digital surveillance in South Africa, while also promoting an environment where human rights and security can coexist.

74 ACHPR: Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019) https://www.chr.up.ac.za/images/researchunits/dgdr/documents/ati/Declaration_of_Principles_on_Freedom_of_Expression_ENG_2019.pdf

6.1 POLICY ACTORS

Recommendation:

Develop and implement data protection and surveillance laws that are consistent with international human rights standards, ensuring that surveillance measures are limited, necessary, and proportionate.

Rationale:

Governments have the primary responsibility to ensure that surveillance practices are both lawful and respectful of human rights. They must enact clear legislative frameworks that protect the right to privacy and other human rights such as freedom of expression of their citizens while allowing for target-ed surveillance under strict conditions.

6.2 NATIONAL HUMAN RIGHTS INSTITUTIONS

Recommendations:

- Play a key role in monitoring and reporting on human rights violations related to surveillance, advocating for better safeguards.
- Conduct regular assessments of surveillance laws and practices, issue annual reports, and engage with governments to recommend necessary reforms.
- Encourage public participation by facilitating platforms for civil society, communities, and individuals to articulate concerns about surveillance violations.

Rationale:

NHRIs are critical in ensuring accountability for human rights violations and can be a key player in challenging unlawful surveillance practices. They can serve as an independent check on government power and advocate for reforms that align with human rights norms.

6.3 JUDICIARY AND LAW ENFORCEMENT AGENCIES

Recommendations:

- Ensure judicial oversight of surveillance activities, particularly regarding cases involving journalists, activists, and vulnerable groups.
- Courts should ensure that any surveillance activities meet constitutional and international human rights standards.
- Ensure that surveillance activities are only carried out based on specific, reasonable suspicion and that they comply with human rights protections.

Rationale:

The judiciary must act as a safeguard against state overreach by providing independent authorization for surveillance, ensuring that it is conducted only when absolutely necessary and in compliance with due process and human rights protections.

6.4 PRIVATE SECTOR

Recommendations:

- Tech companies should integrate privacy by design into their services, implement end-to-end encryption, and be transparent about how user data is collected and shared.
- Prioritise user privacy by embedding privacy protections into their services, such as ensuring end-to-end encryption, limiting data retention, and being transparent about data usage.
- Comply with local data protection laws and provide transparency about any government surveillance requests they receive, in line with international human rights standards.
- Participate in multi-stakeholder initiatives to create industry standards for privacy protection in the digital age, ensuring that technological advances do not undermine individual rights.

Rationale:

Technology companies play a central role in enabling surveillance. By adopting strong privacy standards and collaborating with governments and civil society, they can help mitigate the risks of invasive surveillance and contribute to the respect for privacy rights.

6.5 TELECOMMUNICATIONS AND INTERNET SERVICE PROVIDERS (ISPS)

Recommendations:

- Safeguard user data and comply with privacy protections by limiting the scope of data they collect and store.
- Ensure transparency by informing users of the types of data collected, the duration of storage, and when and why data might be shared with government entities.
- Establish strong encryption protocols to protect users' communications and data.
- Cooperate with law enforcement only when required by law and after independent judicial authorization has been obtained.

Rationale:

As key actors in the infrastructure of surveillance, ISPs and telecommunications providers have a significant role in protecting users' privacy. They must ensure that they only cooperate with surveillance requests that are legally sound and comply with international privacy standards.

6.6 CIVIL SOCIETY ORGANIZATIONS

Recommendations:

- Provide advocacy and digital security training to at-risk communities, raising awareness about surveillance risks.
- Engage in strategic litigation and lobbying to reform surveillance laws.
- Promote public awareness campaigns and educational programs about citizens' rights to privacy, the risks of surveillance, and the importance of complying with international human rights standards. Campaigns could target both the general public and other key stakeholders (lawmakers, law enforcement, judiciary).
- Conduct annual research and analysis of the impact of surveillance on human rights.
- Provide training for judges and law enforcement personnel on human rights standards in relation to surveillance, focusing on privacy rights and the appropriate application of surveillance measures.

Rationale:

CSOs play an important role in raising awareness about surveillance risks, providing legal support for victims of privacy violations, and holding governments accountable. Their engagement ensures that the voices of vulnerable or marginalised communities are heard in the debate about surveillance policies.

6.7 INTERNATIONAL AND REGIONAL HUMAN RIGHTS MECHANISMS

Recommendations:

- Offer technical assistance and legal expertise to ensure surveillance practices comply with international human rights law.
- Monitor and hold governments accountable for abusive practices.
- Urge member states to review and, where necessary, reform their national surveillance laws to align them with international human rights standards.

- Develop a comprehensive continental framework on surveillance and privacy for protecting citizens from undue surveillance.
- Encourage African countries to establish or strengthen independent data protection authorities tasked with overseeing the implementation of data protection laws and ensuring that surveillance practices do not violate privacy rights.

Rationale:

International and regional human rights mechanisms have a critical role in promoting the human rights framework across the African continent.

For instance, the ACHPR has an important role in promoting the human rights framework across the African continent. By providing clear guidelines and holding states accountable through its State Party reporting process, it can ensure that the right to privacy is safeguarded in the digital age, in line with Principle 41 of its 2019 Declaration.

The United Nations Human Rights Council plays an important role in setting global human rights norms. By focusing on surveillance and privacy, the Council can ensure that member states adopt policies that align with international human rights standards, such as the ICCPR. Similarly, the Human Rights Committee can play a role in promoting the rights of individuals to be free from arbitrary surveillance. By using the ICCPR in tandem with regional mechanisms, surveillance practices can be more effectively regulated.

6.8 DEVELOPMENT ACTORS

Recommendations:

- Fund initiatives focused on digital rights, privacy advocacy, and building resilience against surveillance, particularly in high-risk environments or situations.
- Fund capacity-building initiatives that help state actors understand and implement privacy laws, especially in the context of growing surveillance technologies.
- Support the development of national and regional frameworks for regulating surveillance that are aligned with international human rights standards.
- Promote the creation of multi-stakeholder dialogues involving governments, civil society, private companies, and human rights organisations to promote collaboration on surveillance-related issues.

Rationale:

International development agencies have the resources and influence to help governments adopt human rights-respecting policies, while also providing the necessary technical and financial support for sustainable governance reforms related to surveillance and privacy.

6.9 DATA PROTECTION AUTHORITY (THE INFORMATION REGULATOR)

Recommendations:

- Strengthen oversight and enforcement mechanisms by conducting regular audits of both state and private sector surveillance practices, establishing clear guidelines to ensure transparency and accountability in data collection, retention, and usage.
- Actively engage the public on data protection rights and the risks of surveillance, providing accessible complaint mechanisms for individuals to challenge unlawful practices.
- Implement clear, enforceable rules to ensure that surveillance is necessary, proportionate, and legally justified, while maintaining transparency in reviewing government requests.
- Enforce strict data minimization and retention limits, ensuring data is not held longer than necessary.
- Collaborate with international counterparts to share best practices and align regulations, ensuring that surveillance practices comply with global standards and protect privacy rights across borders.

Rationale:

Independent data protection authorities can serve as a critical check on the abuse of surveillance powers, ensuring that privacy is respected and surveillance practices are lawful and proportionate.

6.10 THINK TANKS AND RESEARCH INSTITUTIONS

Recommendations:

- Conduct independent research on the impact of surveillance on freedom of expression, privacy, and democracy, providing data and evidence to inform policy reforms.
- Develop policy briefs and toolkits that help governments, CSOs, and other stakeholders understand the risks and benefits of surveillance technologies and privacy protections.
- Promote evidence-based advocacy for strengthening laws related to targeted surveillance, including ensuring judicial oversight, due process, and proactive transparency.
- Publish comparative studies that highlight international best practices and lessons learned in balancing surveillance with human rights.

Rationale:

Think tanks and research institutions are essential in providing data-driven insights that can shape informed decision-making among policymakers. They also serve as critical sources of knowledge that guide the development of human rights-compliant surveillance laws and frameworks.

6.11 MEDIA AND JOURNALISM NETWORKS

Recommendations:

- Advocate for greater transparency in government surveillance programs, and report on the implications of surveillance practices on privacy and freedom of expression.
- Conduct investigative journalism on government overreach in surveillance, highlighting cases of privacy violations and challenging the lack of safeguards.
- Promote digital literacy programs that educate the public about their digital rights and the potential dangers of mass surveillance.

Rationale:

Media organisations are essential in raising public awareness of surveillance issues and holding governments accountable. By providing timely and accurate information, they can promote a more informed and engaged citizenry that demands the protection of their privacy and other freedoms.

6.12 THE GLOBAL PRIVACY ASSEMBLY (GPA)[75]

Recommendations:

- Provide a platform for cross-border cooperation on privacy protection and the regulation of surveillance technologies.
- Facilitate knowledge-sharing between regional privacy authorities, including the African Data Protection Authorities, to establish best practices for privacy and surveillance regulation.
- Encourage joint initiatives among global privacy organisations to address the challenges posed by surveillance technologies, particularly in ensuring that data collected for security purposes does not infringe upon the fundamental rights of individuals.

75 The Global Privacy Assembly (GPA), https://globalprivacyassembly.org/

Rationale:

The GPA plays an important role in promoting privacy protection worldwide. By promoting collaboration between regional bodies, such as the African Data Protection Authorities, and international privacy organisations, it can help ensure that surveillance practices are in line with international human rights standards

6.13 THE AFRICAN COURT ON HUMAN AND PEOPLES' RIGHTS (AFCHPR)

Recommendations:

- Use the advisory jurisdiction of the Court to interpret provisions of human rights instruments such as Principle 41 of the AfCHPR Declaration and its application in specific country contexts, particularly in relation to surveillance laws and practices.
- Encourage African governments to ratify the Court Protocol and accept the jurisdiction of the AfCHPR for cases related to surveillance, ensuring that victims of unlawful surveillance have access to justice.
- Provide guidance to national courts on the legal principles for safeguarding the right to privacy, drawing on relevant regional and international human rights standards.
- Collaborate with the European Court of Human Rights on surveillance issues. African states can benefit from Europe's legal experiences, ensuring that privacy protections are fully integrated into the African legal framework.

Rationale:

The AfCHPR has the authority to deliver binding rulings on human rights violations in Africa. By addressing surveillance-related cases, the Court can set precedents that enforce privacy protections, supporting the broader human rights framework.[76]

76 Inspiration can be drawn from the The European Court of Human Rights (ECtHR) that has been leading in the development of jurisprudence around privacy and surveillance.

7. Conclusion

Despite post-apartheid reforms intended to ensure South Africa's surveillance and intelligence services serve democratic interests and uphold human rights, several issues continue to undermine these efforts. Under former President Jacob Zuma, intelligence agencies became embroiled in the state capture scandal, where political elites, particularly those close to Zuma and the Gupta family, used the agencies for personal and political gain, including the surveillance of opponents and journalists. The Judicial Commission of Inquiry into Allegations of State Capture (the Zondo Commission) exposed significant abuses of intelligence resources, revealing weak oversight mechanisms, such as the Inspector-General of Intelligence (OIGI), which has been criticised for lacking independence and failing to hold agencies accountable. Ongoing surveillance of journalists, activists, and CSOs, often without legal justification, has raised concerns about the erosion of human rights and fundamental freedoms such as privacy and press freedom. The increasing use of digital surveillance technologies, including IMSI catchers and spyware, has intensified these concerns, as these tools enable mass data collection with limited regulatory safeguards. Public trust in the intelligence community remains low, fuelled by perceptions of corruption, political interference, and a lack of transparency, further compounded by scandals like VASTech, a company linked to authoritarian regimes and the sale of surveillance technology.

In conclusion, while there have been significant efforts to regulate and oversee surveillance practices in South Africa, the country still faces considerable challenges. The complex dynamics between state and non-state actors, the lack of transparency in surveillance activities, and the broad executive powers associated with national security have created an environment where accountability remains limited. For civil society actors, the fight for privacy and freedom from unjust surveillance continues to be an uphill battle, requiring stronger safeguards, effective legal frameworks, and enforcement mechanisms. The role of the judiciary, civil society, and other stakeholders will remain essential in ensuring that surveillance practices in South Africa respect human rights and constitutional principles.

“

For civil society actors, the fight for privacy and freedom from unjust surveillance continues to be an uphill battle, requiring stronger safeguards, effective legal frameworks, and enforcement mechanisms.

Resources

Privacy International
https://privacyinternational.org/

R2K: The Surveillance State: Communications Surveillance and Privacy in South Africa, March 2016
https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf

R2K and Media Policy & Democracy Project: New Terrains of Privacy in South Africa, December 2016
https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/r2kmpdp_new_terrains_of_privacy_in_south__africa_masterset_small.pdf

R2K: Spooked – Surveillance of Journalists in South Africa, June 2018
https://sanef.org.za/wp-content/uploads/2024/10/R2K-Surveillance-of-Journalists-Report-2018-web.pdf

R2K and Privacy International: State of Privacy: South Africa, January 2019
https://www.privacyinternational.org/state-privacy/1010/state-privacy-south-africa

R2K: Stories of South Africa's intelligence structures monitoring and harassing activist movements
https://yetu.coop/wp-content/uploads/2022/02/Big-Brother-Exposed-R2K-handbook-on-surveillance-web.pdf

Annex: Broad Recommendations on Combating Illegitimate Surveillance Practices

The recommendations below offer insights into proven approaches and strategic initiatives for building resilience to ensure that surveillance is conducted in a lawful, transparent, and accountable manner, protecting the fundamental rights of individuals, while fulfilling legitimate security obligations. The table also highlights lessons learnt from stakeholder responses to surveillance concerns to inform more effective, rights-respecting policies.

ILLEGITIMATE SURVEILLANCE	
Establish independent oversight bodies Create an independent body to oversee state surveillance practices to ensure compliance with human rights.	**Stakeholders involved**: Policy actors, judiciary, NHRIs, CSOs, International Mechanisms **Good practices**: The Investigatory Powers Tribunal in the UK is an independent body responsible for reviewing complaints about the use of surveillance powers by the UK government, including law enforcement and intelligence agencies. **Strategies for resilience & lessons learned**: Lessons from the EU's GDPR: Independent bodies like data protection authorities monitor compliance with privacy laws, ensuring public accountability.
Reform data retention laws Advocate for clear limitations on data retention and access to private communications, based on necessity and proportionality.	**Stakeholders involved**: Judiciary, policy actors, private sector, CSOs **Good practices**: Germany: significant legal challenges to data retention laws led to the Constitutional Court ruling that blanket retention of data violates privacy rights and is disproportionate. The 2016 court ruling held that data retention laws should be tailored to ensure that only data related to serious crimes and with specific judicial oversight could be retained. **Strategies for resilience & lessons learned**: South Africa's POPIA provides a framework for privacy protection, though more robust enforcement is needed.
Promote Digital Rights Awareness Launch public awareness campaigns about the risks of digital surveillance and the rights to privacy.	**Stakeholders involved**: CSOs, development actors, NHRIs, media **Good practices**: India's Digital Empowerment Foundation educates communities on privacy risks and digital rights, including cybersecurity education through workshops and local initiatives. **Strategies for resilience & lessons learned**: Global digital rights advocacy (Access Now, Electronic Frontier Foundation) have developed resources to help activists protect their digital presence.

TARGETED SURVEILLANCE

Ensure surveillance practices are targeted and proportional

Implement stronger legislative safeguards to ensure that surveillance is only used for clearly defined security threats, not to suppress dissent.

Stakeholders involved: Judiciary, policy actors, CSOs, regional and international mechanisms

Good practices: Germany's Federal Constitutional Court ruled that blanket surveillance of internet communications violates citizens' privacy rights and requires strict oversight.

Strategies for resilience & lessons learned: The UN Human Rights Council's Special Rapporteur on the Right to Privacy has outlined clear principles to ensure surveillance is lawful and proportionate, with a focus on human rights.

Require judicial authorization

Ensure surveillance operations, especially those involving sensitive data or communications, are authorised by a court, with transparency.

Stakeholders involved: Judiciary, policy actors, NHRIs

Good practices: The UK's Investigatory Powers Tribunal ensures that intelligence agencies' surveillance activities are subject to legal review, providing oversight for targeting practices.

Strategies for resilience & lessons learned: South Africa's Judicial Oversight: Court rulings, such as the 2021 ruling on the National Strategic Intelligence Bill, emphasise the need for judicial approval of surveillance.

PRIVACY PROTECTION & DIGITAL SECURITY

Encourage encryption and secure communications

Promote the use of encryption technologies for private communications and data storage, ensuring activists and journalists can protect their work.

Stakeholders involved: Private sector, CSOs, media

Good practices: Countries like Germany, Switzerland, Estonia, Norway, and Canada are notable for promoting encryption and secure communications through strong legal protections, supportive policies, and privacy advocacy. They encourage the use of encryption technologies to safeguard privacy, especially for activists and journalists, and promote a favourable environment for digital security.

Strategies for resilience & lessons learned: Encrypted Messaging Platforms like Signal and WhatsApp are used globally to protect communications and should be encouraged.

Implement whistleblower protections

Strengthen protections for whistleblowers who expose government abuses, including from surveillance retaliation.

Stakeholders involved: CSOs, international mechanisms, policy actors

Good practices: South Africa's Protected Disclosures Act offers legal safeguards to whistleblowers, but its enforcement and awareness remain areas for improvement.

Strategies for resilience & lessons learned: The EU Whistleblower Protection Directive (2019/1937) mandates that member states protect whistleblowers in both the public and private sectors, with specific emphasis on exposing corruption, misconduct, and breaches of EU law.[77]

77 Key features include: 1) Anonymous reporting which allows whistleblowers to report concerns anonymously without fear of retaliation. 2) Protection from retaliation which includes safeguards against dismissal, demotion, and harassment. 3) Multiple reporting channels in which whistleblowers can report internally within an organisation or externally to authorities. 4) Safe reporting mechanisms under the directive which encourages the use of secure communication channels to protect whistleblowers from surveillance.

ENSURING ACCOUNTABILITY AND JUSTICE

Strengthen access to legal redress

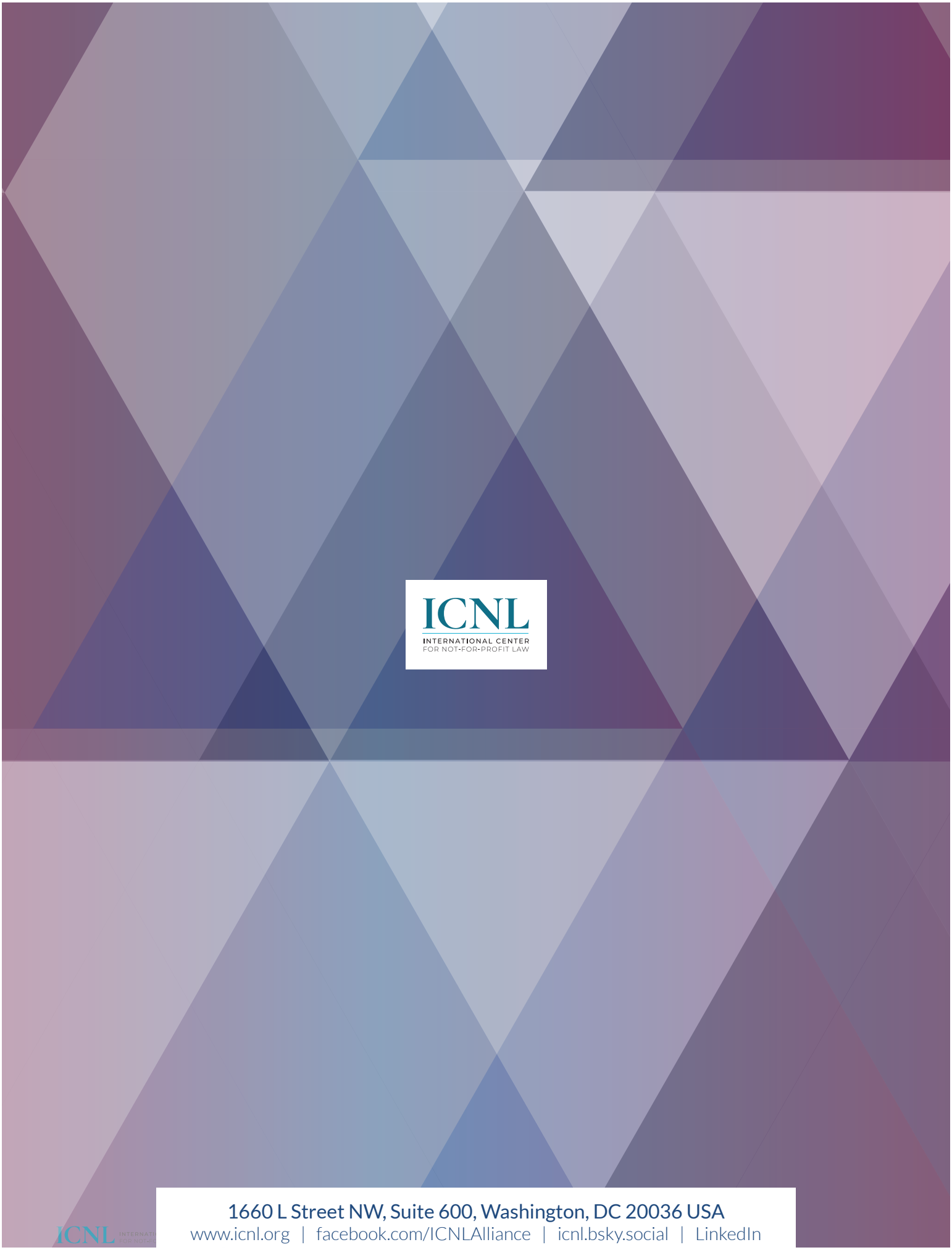
Enable CSOs and individuals to challenge illegal surveillance practices through accessible legal avenues.

Stakeholders involved: Judiciary, CSOs, international mechanisms

Good practices: Chile's National Human Rights Institute (INDH) offers legal avenues for citizens whose rights are violated through surveillance practices, promoting accountability.

Strategies for resilience & lessons learned: Lessons from South Africa's Constitutional Court: Successful challenges against unlawful government surveillance demonstrate the importance of a robust judiciary.[78]

78 Other notable examples include Germany, with its strong constitutional privacy protections and independent oversight bodies. In the US where civil society groups like the American Civil Liberties Union (ACLU) have successfully challenged surveillance programs in court. EU countries benefit from the GDPR and the European Court of Justice's rulings on privacy.



1660 L Street NW, Suite 600, Washington, DC 20036 USA
www.icnl.org | facebook.com/ICNLAlliance | icnl.bsky.social | LinkedIn