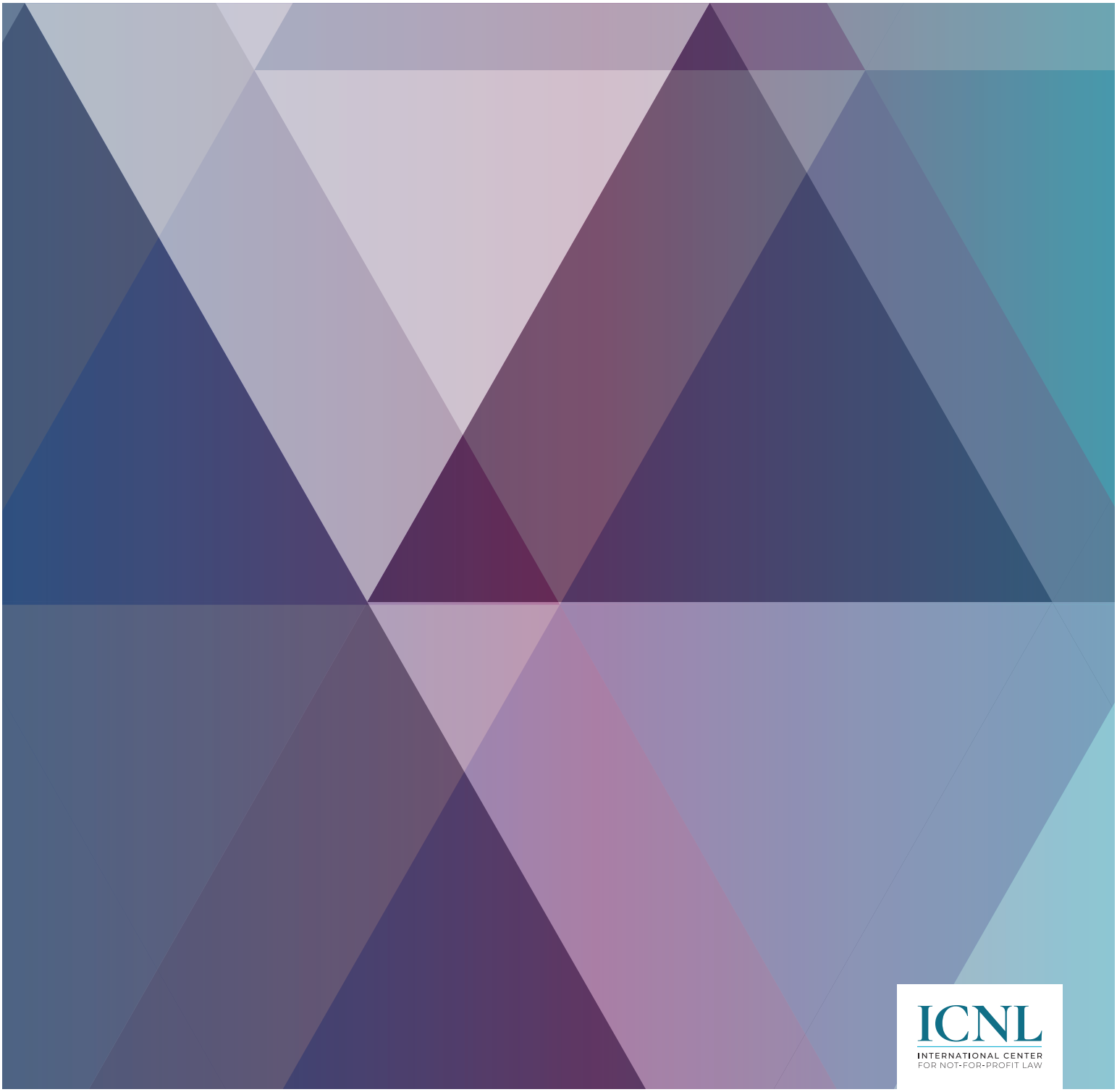
Regulation of Digital Surveillance and the Impact on Civil Society in Africa:

Experiences from Kenya

JULY 2025



ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

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

Experiences from Kenya

This report was prepared by our consultant Dr. Tomiwa Ilori 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
ACRWC	African Charter on the Rights and Welfare of the Child
ACERWC	African Committee of Experts on the Rights and Welfare of the Child
CA	Communications Authority of Kenya
CMCA	Computer Misuse and Cybercrimes Act
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DMS	Device Management System
DCI	Directorate of Criminal Investigations
DMI	Directorate of Military Intelligence
GPS	Global Positioning System
HRC	Human Rights Council
IPOA	Independent Police Oversight Authority
ISCB	Intelligence Service Complaints Board
ICCPR	International Covenant on Civil and Political Rights
IMEI	International Mobile Equipment Identity
ISPs	Internet Service Providers
JSA	Judicial Service Act
JSC	Judicial Service Commission
KICTANET	Kenya ICT Network
KICA	Kenya Information and Communication Act
KNCHR	Kenya National Commission on Human Rights
KRA	Kenya Revenue Authority
MLAA	Mutual Legal Assistance Act
NCHRD-K	National Coalition of Human Rights Defenders
NC4	National Computer and Cybercrimes Committee

List of abbreviations (continued)

NCAJ	National Council on Administration of Justice
NIIMS	National Integrated Identity Management
NIS	National Intelligence Service
NISA	National Intelligence Service Act
NPSA	National Police Service Act
NSC	National Security Council
ODPC	Office of the Data Protection Commissioner
OSA	Official Secrets Act
PTA	Prevention of Terrorism Act
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
SIGNIT	Signals Intelligence
SLA	Statute Law (Miscellaneous Amendments) Act

Executive Summary

This research report examines the prevailing trends in the regulation of digital surveillance in Kenya and their human rights impacts on civil society groups. The study provides a comprehensive analysis of the legal frameworks governing digital surveillance, identifies inconsistencies in these frameworks with international human rights law, and documents specific threats arising from implementation practices of unlawful surveillance and interception of communications.

The African Commission on Human and Peoples' Rights (ACHPR) has provided State Parties with principles on how to ensure lawful surveillance. It has also called on State Parties to ensure that victims of violations of unlawful surveillance are provided with effective remedies and that cases of unlawful surveillance are prosecuted effectively. The Kenyan Constitution, 2010 provides a Bill of Rights and the narrow scope of conditions that must be followed when restricting these rights. The courts have also described unlawful surveillance as a violation of the right to privacy in the Constitution. However, despite these legal guarantees and guidance, the use of digital surveillance by government authorities is on the rise in Kenya. Without adequate human rights safeguards, there is a risk that arbitrary surveillance poses severe human rights threats to civil society actors and their operating environment.

The main findings from the research are summarized as follows:

LEGAL FRAMEWORKS

The report reviews international, regional, and national legal frameworks related to digital surveillance. It highlights significant gaps and inconsistencies in Kenyan laws, such as the Kenya Information and Communications Act and the National Intelligence Service Act which lack adequate safeguards to protect privacy and other interdependent human rights.

Without adequate human rights safeguards, there is a risk that arbitrary surveillance in Kenya poses severe human rights threats to civil society actors and their operating environment.

SURVEILLANCE PRACTICES

The study identifies various forms of digital surveillance employed in Kenya including the use of problematic surveillance technologies that impact civil society actors. These practices are often conducted without sufficient oversight which has led to potential abuses and violations of civil liberties.

IMPACT ON CIVIL SOCIETY

The report documents the adverse effects of unlawful surveillance on civil society actors including human rights defenders, journalists, and activists. It underscores how surveillance practices undermine the rights to privacy, freedom of expression, association, and assembly which creates a chilling effect on civic engagement and democratic participation. Accordingly, awareness of these threats by mainstream CSOs is critical to foster navigation and resilience as well as ensure accountability for those implicated for conducting illegal surveillance.

HUMAN RIGHTS OF MARGINALIZED GROUPS

The research highlights the disproportionate impact of surveillance on marginalized groups, such as women and refugees. It emphasizes the need for robust legal protections to prevent discrimination and ensure that surveillance technologies do not exacerbate existing inequalities.

GOOD PRACTICES AND ACTIONABLE RECOMMENDATIONS

The report identifies good practices from other jurisdictions that could be adapted to the Kenyan context. It provides actionable recommendations for state actors, non-state actors, and the ACHPR. These recommendations include legal reforms, effective oversight mechanisms and increased advocacy to align surveillance practices with international human rights standards.

The report concludes that while lawful digital surveillance can play a role in enhancing security, it must be balanced with the protection of fundamental human rights. It calls for comprehensive legal reforms, greater transparency, and accountability in surveillance practices to safeguard the rights of civil society actors in Kenya. Civil society actors are enjoined to increase advocacy and campaigns regarding lawful surveillance practices in Kenya. State actors including those in the security and justice sectors and non-state actors including civil society actors, human rights defenders and at-risk groups will find this report useful as it provides strategic guidance and specific policy reforms on how to ensure adequate national frameworks on privacy and surveillance in Kenya.

1. Introduction and Background

Digital surveillance has been increasingly normalized due to developments in new technologies and the increasing need for security. Digital surveillance involves monitoring, intercepting, or recording communications through digital devices or platforms to collect information.[1] This can include the interception of electronically transmitted communication or the use of AI-enabled tools to collect and analyze biometric data.[2] When conducted lawfully, governments use surveillance to maintain security, enforce laws, and collect intelligence. However, extralegal digital surveillance poses great threats to human rights protection, as well as to the work and safety of civil society actors. With the advent of new and emerging technologies such as AI-enabled surveillance tools with invasive and intrusive capabilities, the expansion of digital surveillance raises significant concerns about the protection of privacy and other interdependent rights.

The purpose of digital surveillance varies, but it is often conducted by governments to investigate serious crimes such as terrorist activities or any other criminal activity with high likelihood of violence or harm to lives or property. This practice involves tracking online behavior, analyzing communications, and gathering personal data, such as through internet monitoring, social media analysis, and the interception of electronic communications.

Although the broader term "surveillance" does not necessarily involve the use of digital devices or platforms, in this research report, the terms "digital surveillance" and "surveillance" are used interchangeably.

In Kenya, surveillance and interception of communications are the dominant terms often used in laws and practice. The practices are deeply intertwined with the country's colonial past and its post-independence governance.[3] During the colonial era, the British administration employed surveillance to monitor and suppress anti-colonial activities, such as the Mau Mau rebellion. British colonial surveillance tactics included the use of informants, searches at checkpoints, and interception and monitoring of mail.[4] This legacy continued post-independence with successive governments using surveillance to maintain control and monitor political dissent.

---

1 Joseph Fitsanakis, 'The Interception of Communications in Historical Context' in Joseph Fitsanakis (ed), Redesigning Wiretapping: The Digitization of Communications Interception (Springer International Publishing 2020) <https://doi.org/10.1007/978-3-030-39919-1_4> accessed 23 November 2024.

2 International Center for Not-for-Profit Law (ICNL), 'The Impact of Artificial Intelligence Technologies on the Right to Privacy and Civic Freedoms' (2021) <https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/Submissions/CSOs/ICNL.pdf> accessed 23 November 2024; Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace 2019) <https://carnegie-production-assets.s3.amazonaws.com/static/files/files__WP-Feldstein-AISurveillance_final1.pdf> accessed 23 November 2024.

3 Victor Kapiyo, Cherie Oyier and Francis Monyango, 'Surveillance Laws and Technologies Used in Countering Terrorism and Their Potential Impact on Civic Space' (Kenya ICT Action Network (KICTANet) 2024) <https://www.kictanet.or.ke/?mdocs-file=49126> accessed 23 November 2024.

4 <https://www.amnesty.org.uk/blogs/human-rights-are-answer/predictive-policing-colonies-contemporary>; <https://www.tutorchase.com/notes/ib/history/18-10-1-british-rule-in-kenya>

The introduction of the Kenya Information and Communications Act in 1998 marked a significant development by providing a legal framework for regulating the interception of communications by authorized public entities. However, this legislation and several others enacted after it have been criticized for potentially infringing on privacy rights guaranteed under the international human rights law and the Constitution of Kenya, 2010 (Constitution).

In recent years, the use of surveillance technology has expanded, particularly with the advent of digital technologies and communications which gave rise to digital surveillance. The Kenyan government has invested in sophisticated surveillance tools including biometric systems and internet monitoring technologies for national security purposes.[5] However, these investments have raised concerns about the potential for abuse. During the 2017 elections, and the 2023 and 2024 protests, for instance, opposition figures and activists were allegedly surveilled while carrying out lawful activities.[6] Such instances highlight the need for stronger legal safeguards to protect citizens' privacy rights against unwarranted surveillance.

Therefore, this research report explores digital surveillance vis-à-vis surveillance and interception of communications in Kenya, analyzes the international and domestic legal frameworks governing them, examines various trends and practices in Kenya, and discusses the human rights impacts of unlawful surveillance on civil society actors. It provides actionable recommendations for various stakeholders to ensure that surveillance practices align with human rights standards.

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.

5 Privacy International, 'State of Privacy Kenya' (26 January 2019) <http://privacyinternational.org/state-privacy/1005/state-privacy-kenya> accessed 23 November 2024.

6 Human Rights Watch "Not Worth the Risk' Threats to Free Expression Ahead of Kenya's 2017 Elections' (30 May 2017) <https://www.hrw.org/report/2017/05/30/not-worth-risk/threats-free-expression-ahead-kenyas-2017-elections> accessed 20 January 2025; Freedom House 'Freedom on the Net' (2023) <https://freedomhouse.org/country/kenya/freedom-net/2023> accessed 20 January 2025; Kenya National Human Rights Commission 'State of Human rRghts in Kenya: July 2023 - November 2024' (20 November 2024) <https://www.knchr.org/Articles/ArtMID/2432/ArticleID/1207/STATE-OF-HUMAN-RIGHTS-IN-KENYA-JULY-2023-NOVEMBER-2024> accessed 20 January 2025.

Key Takeaways

• Digital surveillance involves systematic monitoring, interception or recording of communications through digital devices or platforms to collect information for different purposes.

• Governments use surveillance for security, law enforcement, and intelligence, but digital surveillance raises privacy and civil liberties concerns.

• This research examines Kenya's political and historical surveillance contexts, legal frameworks, and the impact of unlawful surveillance on civil society.

• It provides actionable recommendations for stakeholders to ensure surveillance practices align with human rights standards.

2. Regulation of Surveillance and Interception of Communications: International, Regional and National Legal Frameworks

National legal frameworks on surveillance or interception of communications should comply with international human rights laws, regional human rights systems, and national constitutional standards. While surveillance adversely impacts a broad range of human rights, today, these systems and legal frameworks often primarily focus on the right to privacy due to surveillance technologies' increasingly vast capabilities to access and exploit personal information, such as communication data, biometric data, location data, personal identifiers, and online activities.

2.1 REGULATION OF SURVEILLANCE AND INTERCEPTION OF COMMUNICATIONS UNDER INTERNATIONAL LAW

Regarding surveillance regulation, the UN human rights system is made up of legal frameworks including treaties and mechanisms such as treaty-based bodies and charter-based bodies.[7] The system as a whole provides for and interprets States' obligations under international human rights law.[8]

The legal frameworks are made up of the international bill of rights, including the International Covenant on Civil and Political Rights (ICCPR)[9] as the most critical treaty regarding the right to privacy and surveillance. Kenya is a State party to the ICCPR and has obligations to comply with its provisions.[10] There are ten treaty-based bodies, but the Human Rights Committee is the most proximate body that deals with surveillance and the right to privacy. Charter-based bodies comprise the Human Rights Council (HRC), the Universal Periodic Review, and Independent Investigations. Article 17 of the ICCPR provides for the right to privacy and this provision has been interpreted in relation to surveillance by both the Human Rights Committee and the HRC. According to this provision, State parties are required to regulate surveillance based on four cumulative principles namely *legality*; *proportionality*; *necessity* and *adequate safeguards*. It is important to note that while these principles are distinct, they are also interrelated and have varying similarities.

7 Privacy International, 'PI's Guide to International Law and Surveillance' (2024) <https://privacyinternational.org/sites/default/files/2024-09/2024%20GILS%20version%204.0.pdf> accessed 23 November 2024.

8 'Instruments & Mechanisms' (OHCHR) <https://www.ohchr.org/en/instruments-and-mechanisms> accessed 23 November 2024.

9 'International Covenant on Civil and Political Rights (Adopted 16 December 1966, Entered into Force 23 March 1976) 999 UNTS 171 (ICCPR)' <https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr.pdf> accessed 23 November 2024.

10 'Ratification Status for Kenya' (UN Treaty Body Database) <https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=90&Lang=en> accessed 23 November 2024.

2.1.1 Principle of legality

The principle of legality regarding surveillance is anchored on two key requirements, namely accessibility and foreseeability. The accessibility requirement obligates State parties to ensure that surveillance laws are 'publicly accessible, clear, precise, comprehensive and non-discriminatory and that such interference is not arbitrary and unlawful, bearing in mind what is reasonable for the pursuance of legitimate aim.'[11] Surveillance laws must be formulated with sufficient precision and avoid vague justifications. The foreseeability requirements call for State parties to meet a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application.[12] In the context of secret surveillance, foreseeability means that laws must be clear and detailed, giving citizens adequate indication of when and how surveillance measures may be applied to protect against arbitrary interference by authorities. Such measures must also prescribe specific offenses and targets for which surveillance or lawful interception of communication may occur and provide for transparency and accountability on how surveillance occurs, including requests to businesses, information sharing with state actors and assignment of surveillance activities to specific state authorities.[13] This is crucial due to the sophisticated nature of surveillance technology and the risks of its secret use by executive organs.

In order to comply with the principle of legality, States are required to take measures to ensure that interference with or restriction of the right to privacy is not arbitrary, is adequately regulated by law, and is subject to effective oversight and appropriate redress, including through judicial review or other means.[14] Concerning digital surveillance, State parties are also required to 'adopt adequate legal frameworks that govern the collection, analysis and sharing of social media intelligence

> Surveillance laws must be formulated with sufficient precision and avoid vague justifications.

11 UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211 (15 December 2022).

12 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40 (17 April 2013).

13 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018).

14 UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/78/210 (19 December 2023).

that clearly define permissible grounds, prerequisites, authorization procedures and adequate oversight mechanisms.'[15]

2.1.2 Principle of necessity

The principle of necessity requires State parties to show that the restriction they would impose on the right to privacy through surveillance or interception of communication is necessary to meet a particular legitimate interest.[16] Such legitimate interest could include demonstrated public health emergencies and protection of lives and properties. Therefore, mass or bulk surveillance activities, even if serving a legitimate aim and based on an accessible legal regime, may be considered arbitrary if they are not necessary and if they do not focus on specific targets.[17] Applying instances where necessity must apply to issues such as national security, the Inter-American Special Rapporteur for freedom of expression and the internet noted that when national security is used to justify monitoring personal data and correspondence, the law must clearly define the criteria for legitimate limitations and precisely outline the concept.[18]

To comply with the principle of necessity, states must prove that any limitations on privacy are strictly necessary in a democratic society to achieve their objectives. It is not enough for the measures to be merely useful or reasonable; there must be a clear and compelling need for the limitation, and no less restrictive means should be available to achieve the same legitimate aim.

2.1.3 Principle of proportionality

Proportionality requires an assessment to ensure the restriction on privacy rights is the least intrusive and targets a specific objective without unduly affecting other rights. Any intrusion must be justified, proportionate to the interest protected, and detailed with an evidence-based public interest justification for transparency.[19] There must be a rational connection between the means used and the aim sought, ensuring that the measure is the least intrusive option. The principle of proportionality requires balancing the intrusion into privacy against the public interest benefit, with any interference judged on a case-by-case basis to avoid impairing Covenant rights.[20]

15 Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022).

16 Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022).

17 Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014).

18 The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet OEA/Ser.L/V/II. CIDH/RELE/INF.11/13 (31 December 2013).

19 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015).

20 Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014).

In the context of surveillance, mass surveillance is usually deemed disproportionate. As a general principle, surveillance should be narrowly focused on specific and major threats to public safety. Such measures must be targeted, limited in duration, location and scope, with strict retention periods. Personal information accessed during surveillance such as communication data, biometric data, location data, personal identifiers, and online surveillance activities must be carefully examined for proportionality due to its intrusive nature.[21]

Inclusion of adequate safeguards

To better ensure that surveillance is proportionate and the least restrictive means of achieving the legitimate aim, State parties should put in place procedures, practices, and legislation on communication surveillance, including mass surveillance, data interception, profiling, automated decision-making, and biometric technologies to ensure they uphold the right to privacy and fully implement their international human rights obligations. The UN has specified adequate safeguards on surveillance to include:[22]

1. **Reasonable suspicion**: States must clarify that surveillance measures should only be authorized when there is reasonable suspicion that an individual is involved in criminal activity or poses a specific threat to discernible public safety.[23]

2. **Competent judicial authority**: Surveillance operations should be authorized by an independent judicial body in accordance with international human rights law, with specific limitations on time, manner, place, and scope, and must include detailed record-keeping and notification to the surveillance subjects when it does not jeopardize the surveillance purpose.[24]

3. **Access to remedy**: Effective remedies for privacy violations through digital surveillance must be accessible, involve prompt and impartial investigations, be capable of ending ongoing violations and include judicial oversight with criminal prosecution required for gross human rights violations.[25]

4. **Safeguards against unlawful access**: Create and enforce laws with effective sanctions and remedies to safeguard individuals against privacy viola-

21 Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, UN Doc A/HRC/51/17 (4 August 2022).

22 UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023); Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397 (23 September 2014).

23 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018).

24 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019).

25 Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014).

tions and abuses involving personal data, ensuring actions are based on free, explicit, and informed consent, or are otherwise lawful in line with international human rights law.[26]

5. **Effective oversight**: Oversight frameworks should integrate administrative, judicial, and parliamentary oversight with independent bodies, ensuring expertise, institutional separation, proactive monitoring, transparency, public scrutiny, appeal mechanisms, and diverse viewpoints through expert and multi-stakeholder consultations.[27]
6. **User notification and transparency**: Surveillance targets should be notified about the privacy interference and have the right to alter or delete irrelevant personal information, provided it is no longer needed for ongoing or pending investigations.[28]
7. **Safeguards for international cooperation**: States must respect international human rights obligations regarding the right to privacy in all activities involving the interception of digital communications, collection of personal data, sharing or accessing collected data, and requiring third parties to disclose personal data.[29]

2.2 REGULATION OF SURVEILLANCE AND INTERCEPTION OF COMMUNICATIONS AT THE REGIONAL LEVEL

The African human rights system is made up of three main mechanisms namely the African Commission on Human and People's Rights (African Commission), the African Court on Human and People's Rights (African Court), and the African Committee of Experts on the Rights and Welfare of the Child (ACERWC). These mechanisms are underpinned by the provisions of the African Charter on Human and People's Rights (African Charter), the Protocol to the African Charter on the establishment of the African Court, and the African Charter on the Rights and Welfare of the Child (ACRWC). Kenya has ratified all these three instruments save for the deposit under article 34(6) of the African Court protocol which allows individuals and non-governmental organizations to access the Court. However, most regional normative directions on the right to privacy and surveillance in Africa have come from the African Commission's mandate. Some of these norms are established through Guidelines, Declarations and Resolutions.

26 Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/54/21 (12 October 2023).

27 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018).

28 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018).

29 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018).

In 2017, the African Commission adopted the ***Guidelines on Freedom of Association and Assembly*** which were made pursuant to the provisions of articles 10, 11 and 45(1) of the African Charter. The Guidelines provide for the rights to freedoms of association, assembly, and the mandate of the African Commission respectively.[30] Guideline 35 specifically provides that authorities must respect the privacy of associations and avoid undue surveillance. Surveillance is only allowed with a court-issued warrant based on reasonable suspicion of legal infractions. If illegitimate surveillance occurs, affected associations or individuals are entitled to appropriate redress.

In 2019, the African Commission also adopted the ***Declaration of Principles on Freedom of Expression and Access to Information in Africa***.[31] The Declaration was made pursuant to the provisions of article 9 of the African Charter on the rights to freedom of expression and access to information. Principle 41 of the Declaration provides that states must not engage in indiscriminate and untargeted surveillance of communications.

Key Principles: Targeted Surveillance

Targeted surveillance is only permissible if authorized by law, based on reasonable suspicion of serious crime, and in line with international human rights standards. Any law permitting such surveillance must include safeguards like judicial authorization, due process, time and scope limitations, notification, transparency, and independent oversight.

At the time of the publication of this report, the African Commission is considering a draft Declaration on the Promotion of the Role of Human Rights Defenders and their Protection which addresses challenges faced by human rights defenders in Africa including unlawful surveillance.[32] Particularly, article 3.13 provides that human rights defenders have the right to privacy including the right to protection through encryption. It also adds that they should be free from arbitrary and unlawful intrusion and interference in their family, home, workplace, possessions, and correspondence, both online and offline. Article 4.10 also provides that state authorities must ensure the protection of the right provided for under article 3.13.

30 African Commission on Human and Peoples' Rights, 'The Guidelines on Freedom of Association and Assembly in Africa' <https://achpr.au.int/index.php/en/soft-law/guidelines-freedom-association-and-assembly-africa> (21 September 2017) accessed 23 November 2024.

31 African Commission on Human and Peoples' Rights, 'Declaration of Principles on Freedom of Expression and Access to Information in Africa' accessed 23 November 2024<https://achpr.au.int/en/node/902#:~:text=The%20Declaration%20establishes%20or%20affirms,to%20express%20and%20disseminate%20information> 10 November 2019 accessed 23 November 2024.

32 African Commission on Human and Peoples' Rights, 'Declaration on the Promotion of the Role of Human Rights Defenders and their Protection in Africa' <https://achpr.au.int/en/documents/2024-01-25/declaration-promotion-role-human-rights-defenders-and-their-pro> 25 January 2024 accessed 23 November 2024.

In 2022, the African Commission adopted resolution 522 on the protection of women against digital violence in Africa.[33] The resolution urged states to combat digital violence against women through legislation, research, awareness programs, education, training, cooperation between authorities and service providers, victim-friendly policies, safeguarding women journalists, and repealing vague surveillance laws.

In 2023, the African Commission adopted resolution 573 on mass and unlawful targeted communication surveillance and its impacts on human rights in Africa including its impacts on civil society in Africa.[34] The resolution called on states to ensure that any restrictions on privacy and fundamental freedoms are necessary, proportionate, and in line with international human rights law. *It provides that communication surveillance should be regulated with safeguards like judicial authorization and independent oversight, and only conducted based on reasonable suspicion of serious crime.* Additionally, states should promote privacy-enhancing technologies, avoid weakening encryption, and provide effective remedies for victims of arbitrary surveillance.

In 2024, the African Commission also adopted resolution 620 on promoting data access for advancing human rights and sustainable development in the digital age.[35] The resolution noted the misuse and abuse of data which includes the violations of rights to privacy and non-discrimination. The resolution mandated the Special Rapporteur on Freedom of Expression and Access to Information to consult broadly to examine and develop appropriate standards regarding data collection, deployment and access to data.

The African Commission's resolution 573 provides that communication surveillance should be regulated with safeguards like judicial authorization and independent oversight, and only conducted based on reasonable suspicion of serious crime.

33 African Commission on Human and Peoples' Rights, 'Resolution on the Protection of Women Against Digital Violence in Africa – ACHPR/Res. 522 (LXXII) 2022' <https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr> 11 August 2022 accessed 23 November 2024.

34 African Commission on Human and Peoples' Rights, 'Resolution on the Deployment of Mass and Unlawful Targeted Communication Surveillance and its impact on Human Rights in Africa – ACHPR/Res/573 (LXXVII) 2023' <https://achpr.au.int/en/adopted-resolutions/573-resolution-deployment-mass-and-unlawful-targeted-communication> 9 November 2023 accessed 23 November 2024.

35 African Commission on Human and Peoples' Rights, Resolution on Promoting and Harnessing Data Access as a Tool for Advancing Human Rights and Sustainable Development in the Digital Age – ACHPE/Res. 620 (LXXXI) 2024) <https://achpr.au.int/en/adopted-resolutions/620-data-access-tool-advancing-human-rights-and-sustainable-development> 17 November 2024 accessed 23 November 2024.

2.3 REGULATION OF SURVEILLANCE AND INTERCEPTION OF COMMUNICATIONS IN KENYA

Chapter one of the Kenyan Constitution provides for the supremacy of the Constitution while Chapter four provides for the bill of rights.[36] Article 2(5) and (6) provides that the general rules of international law and any treaty or convention ratified by Kenya are incorporated into Kenyan law under the Constitution. This means that the international and regional frameworks referred to above on Kenya's obligations regarding surveillance and human rights are constitutionally guaranteed. Article 24 of the Constitution also provides that the limitation of rights under the bill of rights must be provided for by law, reasonable and justifiable in an open and democratic society. Regarding the guarantee of the constitutional right to privacy, *article 31 provides that every person has the right to privacy, which protects them from unwarranted searches, seizures, unnecessary disclosure of private information, and infringement of their communications*. In addition to the Constitution, the following laws are some of the applicable domestic laws related to privacy, surveillance and interception of communications in Kenya.

Kenya Information and Communication Act, 2011

The Kenya Information and Communication Act (KICA) established the Communications Commission of Kenya (now Communications Authority of Kenya) to facilitate the development of the information and communications sector among other objectives.[37] Section 31 of the KICA criminalizes the interception of communication by a telecoms operator outside the ordinary course of their business. Section 83W(1)(b) also criminalizes the unauthorized interception of computer service. A person convicted of such interception is liable to a fine not exceeding five hundred thousand shillings or five years imprisonment. The KICA raises concerns because there are no existing adequate safeguards on the powers exercised by the Communications Authority (CA) of Kenya regarding cooperating with security agencies on interception of communications.

Mutual Legal Assistance Act, 2011

The main aim of the Mutual Legal Assistance Act (MLAA) is to provide for mutual legal assistance to be given and received by Kenya in investigations, prosecutions and judicial proceedings in relation to criminal matters.[38] Part VI (sections 27-32) provides for interception of communications, preservation of communications data and covert electronic surveillance. Under these

36 The Constitution of Kenya 2010 <http://www.parliament.go.ke/sites/default/files/2023-03/The_Constitution_of_Kenya_2010.pdf> accessed 23 November 2024.

37 The Kenya Information and Communications Act 2011 (CAP 411A) <https://infotradekenya.go.ke/media/Kenya%20Information%20Communications%20ACT.pdf> accessed 23 November 2024.

38 The Mutual Legal Assistance Act 2023 (CAP 75B) <http://kenyalaw.org:8181/exist/rest/db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/M/Mutual%20Legal%20Assistance%20Act%20-%20No.%2036%20of%202011/docs/MutualLegalAssistanceAct36of2011.pdf> accessed 23 November 2024.

sections, the MLAA allows the government to execute a request from another state to intercept communications of a subject; store such communication; preserve communications data; and surveillance or interception of communications in response to such a request. Under this law, Kenya may also carry out covert electronic surveillance including the use of tracking devices. The MLAA does not clearly identify safeguards for international cooperation especially in cases of sharing personal information of surveillance targets with other countries.

National Intelligence Service Act, 2012

The National Intelligence Service Act (NISA) was enacted to provide for the functions, organization and administration of the National Intelligence Service (NIS) pursuant to article 239(6) of the Constitution.[39] Section 36 of the NISA provides that the communications of a person suspected to have committed an offence may be investigated, monitored or otherwise interfered with, thereby limiting the right to privacy provided for under article 31 of the Constitution. It also requires the NIS to obtain a warrant under Part V of the Act prior to taking any action under section 36. Part V (sections 42-50 of the Act) provides for application for a warrant by the Director-General of the NIS to be granted by the High Court; judicial discretion for such issuance; assistance with executing the warrant; the permissible uses of a warrant; the scope and extension of such warrant and so on. Section 46 provides that the validity period of the warrant shall not be more than one month at a time, and this also applies to the extension of such warrant.

The powers to limit privacy rights of individuals under sections 36 and 42 of NISA are broadly framed in such a manner that they could be misused and abused by the Director-General. As required under international human rights law, the specific offenses for which surveillance can be carried out were not formulated with sufficient precision to allow members of the public to regulate their conduct accordingly. This gives the Director General and NIS the latitude to carry out surveillance without adequate safeguards in violation of international law.

Under the provisions of the NISA, the Director General requires prior judicial authorization from the High Court to carry out surveillance or interception of communication. However, this provision can be circumvented by accessing communications data from telecommunications networks through the Communications Authority of Kenya under its 2014 Regulations. The Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations of 2014 provides that 'a licensee shall grant the Commission's officers access to its systems, premises, facilities, files, records and other data to enable the Commission inspect them for compliance with the Act and these Regulations.' This provision, read together with the amended

39 The National Intelligence Service Act 2012 <https://www.nis.go.ke/downloads/THE%20NATIONAL%20INTELLIGENCE%20SERVICE%20ACT,%202012.pdf> accessed 23 November 2024.

provisions of section 6(2) of the Official Secrets Act, gives NIS backdoor access without a warrant to carry out surveillance or intercept communications.

Prevention of Terrorism Act, 2012

One of the main objectives of the Prevention of Terrorism Act (PTA) is the detection and prevention of terrorist activities.[40] In fulfilling this objective, the PTA provides under section 35(3)(a)(iii) that the communication of a person or entity may be investigated, intercepted or otherwise interfered with, thereby limiting their privacy rights as provided for under the Constitution. Sections 36 and 36A of the Act provide for the power to intercept communications, including by national security organs as prescribed by the Cabinet Secretary, as well as the admissibility of such intercepted communication as evidence in courts. Under section 36, a police officer of the rank of Chief Inspector of Police or above may apply *ex-parte* for an interception order from a Chief Magistrate or to the High Court to gather evidence. Such a police officer must however get a written consent from the Inspector-General of Police or the Director of Prosecutions before making such an application. The court can only authorize the interception and retention of communications if the information relates to a specific offense under the Act. Unauthorized interception by a police officer is punishable by an imprisonment term not exceeding ten years or a fine not exceeding five million shillings or to both. Under 36A (2), the Cabinet Secretary is required to promulgate implementing regulations which must be approved by the National Assembly in order to give effect to section 36A. The existing legal framework does not provide adequate safeguards, such as access to remedy for surveillance targets, effective oversight, user notification and transparency.

Under the Prevention of Terrorism Act, a court can only authorize the interception and retention of communications if the information relates to a specific offense under the Act.

40 The Prevention of Terrorism Act 2023 (CAP 59B) <https://www.frc.go.ke/wp-content/uploads/2024/03/PreventionofTerrorismAct30of2012.pdf> accessed 23 November 2024.

Computer Misuse and Cybercrimes Act, 2018

The Computer Misuse and Cybercrimes Act (CMCA) addresses offenses relating to computer systems.[41] Section 14 of the CMCA criminalizes the act of breaching security measures to gain unauthorized access to a computer system, while section 15 sets forth a separate crime when the intent of the breach is to cause harm, such as stealing or destroying information. Sections 16 and 17 also criminalize unauthorized interference with computer data and interception of data transmission, respectively. Sections 31 and 32 address the interception or misdirection of electronic mail. Part V (sections 47-65 of the Act) sets the parameters for international cooperation, especially as it relates to mutual legal assistance and transnational investigation of crimes which may include the interception of computer data or information. The law, however, fails to include adequate privacy safeguards with regards to law enforcement authorities and international cooperation, such as independent oversight and access to remedy.

Data Protection Act, 2019

The Data Protection Act (DPA), 2019 gives effect to articles 31(c) and (d) of the Constitution which provides that the right to privacy applies to information about a person's family, private affairs, and communications. It also establishes the Office of the Data Protection Commissioner (ODPC) and establishes the duties and rights for the protection of personal data.[42] While the DPA does not specifically refer to surveillance or interception of communications, but the Act exempts the processing of personal data from being subject to its provisions, if it is necessary for national security or public interest, which could lead to infringement on one's privacy where these powers are misused. In 2023, the Office of the Data Protection Commissioner (ODPC) released a Guidance Note for the Communications Sector.[43] The Note was developed to identify the duties and obligations of the Communications Authority of Kenya, service providers and the telecommunication sector regarding data subject rights. The Note highlighted five key privacy concerns in the telecommunications sector including data collection and tracking; encryption and decryption; surveillance; cybersecurity breaches and misuse of personal data. It noted that while encryption may protect sensitive information from unauthorized access, decryption and backdoor access to information may compromise the privacy of users. According to the Guidance Note, communication service providers should institute measures to protect privacy and individual rights, including subscriber information, traffic information, location information and content of telecommunications.

41 Computer Misuse and Cybercrimes Act 2018 <https://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> accessed 23 November 2024.

42 The Data Protection Act 2019 <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct_No24of2019.pdf> accessed 23 November 2024.

43 Office of the Data Protection Commissioner (ODPC), 'Guidance Note for the Communication Sector' (2023) <https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-for-the-Communication-Sector.pdf>.

The Statute Law (Miscellaneous Amendments) Act, 2020

In 2020, the Statute Law (Miscellaneous Amendments) Act (SLA) was enacted to amend provisions of the Official Secrets Act, 2012 (OSA).[44] The new law empowers the Cabinet Secretary of the Interior Ministry to petition the High Court to authorize access to data from any phone, computer, or other communication device. If the owner of the device fails to comply with an order by the High Court, they are subject to imprisonment not exceeding one year, a fine of one million shillings, or to both. The concentration of such wide, unlimited powers of surveillance with only judicial oversight as a safeguard can readily be abused, threatening privacy and other human rights.

In addition to the assessment of these laws, a general observation is that the laws applicable to privacy, surveillance, and interception of communications in Kenya do not provide for user notification, even after surveillance has been carried out. According to international human rights standards on adequate safeguards, this provision is necessary in order to ensure effective access to remedy for surveillance subjects whose privacy rights may have been violated. The absence of such provision also undermines transparency and accountability practices that could be used to protect subjects from unlawful surveillance and interception of communications. Given this analysis and applying the laws on surveillance and interception of communications in Kenya to international human rights standards, they do not provide for sufficient safeguards against unlawful surveillance in Kenya.

Key Takeaways: Kenya's Legal Framework on Surveillance

- The constitutional framework of Kenya clearly adopts international human rights standards on lawful surveillance and fundamental human rights.
- However, most of the laws that relate to surveillance and interception of communications in Kenya are not sufficient to guarantee human rights protection as they are not in line with international human rights standards.
- Aspects of these laws lack adequate safeguards, including ineffective oversight, lack of access to remedy, lack of user notification, transparency, etc.

44 The Statute Law (Miscellaneous Amendments) Bill 2020 <http://www.parliament.go.ke/sites/default/files/2020-06/Statute%20Law%20%28Miscellaneous%20Amendments%29%20Bill%2C%202020%281%29.pdf> accessed 23 November 2024.

3. Analysis of Key Trends, Practices and Actors in Unlawful Surveillance and Interception of Communications

Surveillance technology and spyware used to monitor personal communications and information have been found and used to target and suppress civil society actors such as non-governmental organizations, human rights defenders, journalists, and others in Kenya.[45] In a recent interactive map published by a community-driven initiative called Surveillance Watch, several surveillance companies, their subsidiaries, and partners were identified across the world.[46]

In Sub-Saharan Africa, ten of these companies were found to have their surveillance technologies in Kenya alone which accounts for the second highest number after South Africa and the highest in the East African region. Some of these surveillance companies include Blue Coat Systems,[47] Circles,[48] Insitu,[49] MCM Solutions,[50] NEC Corporations,[51] NSO,[52] OT-Morpho,[53] Predator,[54] Q Cybertechnologies SARL,[55] and SCL Group.[56]

45 Defenders Coalition, 'Perception Survey: Impact of Communication Surveillance on Human Rights Defenders in Kenya' (2020) <https://defenderscoalition.org/wp-content/uploads/2021/03/Coalition-Perception-Survey-English-1.pdf> accessed 23 November 2024; Privacy International, 'State of Privacy Kenya' (n 6).

46 Surveillance Watch, 'They Know Who You Are' <https://www.surveillancewatch.io> accessed 23 November 2024.

47 Morgan Marquis-Boire and others, 'Planet Blue Coat: Mapping Global Censorship and Surveillance Tools' (Citizen Lab Research Report No 13, University of Toronto 2013) <https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/> accessed 23 November 2024.

48 Bill Marczak and others, 'Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles' (Citizen Lab Research Report No 133, University of Toronto 2020) <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/> accessed 23 November 2024.

49 ScanEagle is Insitu's flagship which provides real-time intelligence and civil surveillance capabilities; Business Daily, 'Kenya Gets War Drones It Bought from US in 2015' (29 January 2017) <https://www.businessdailyafrica.com/bd/economy/kenya-gets-war-drones-it-bought-from-us-in-2015-2137930> accessed 23 November 2024.

50 MCM Solutions manufactures the highly controversial digital forensics technology Detego that enables authorities to mine information from multiple devices at once; 'Our Partners' (Detego Global) <https://detegoglobal.com/our-partners/> accessed 23 November 2024.

51 Chris Burt, 'NEC Facial Recognition Border Tech for Kenya as Airport Biometrics Rollouts Continue' (BiometricUpdate.com, 7 October 2019) <https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrics-rollouts-continue> accessed 23 November 2024.

52 Amnesty International, 'Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector' (2021) DOC 10/4491/2021 <https://www.amnesty.org/en/documents/doc10/4491/2021/en/> accessed 23 November 2024.

53 'Kenya's Opposition Coalition Alleges French OT-Morpho Tampered with Election Results; Co. Denies Allegations' (Business & Human Rights Resource Centre, 11 September 2017) <https://www.business-humanrights.org/en/latest-news/kenyas-opposition-coalition-alleges-french-ot-morpho-tampered-with-election-results-co-denies-allegations/> accessed 23 November 2024.

54 Amnesty International, 'Global: "Predator Files" Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials' (9 October 2023) <https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/> accessed 23 November 2024.

55 Amnesty International, 'The Pegasus Project: How Amnesty Tech Uncovered the Spyware Scandal – New Video' (23 March 2022) <https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/> accessed 23 November 2024.

56 Standard Communication Laboratories is best known through its subsidiary Cambridge Analytica and its role in Kenya information ecosystem. Justina Crabtree, 'Here's How Cambridge Analytica Played a Dominant Role in Kenya's Chaotic 2017 Elections' (CNBC, 23 March 2018) <https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html> accessed 23 November 2024.

In 2024, Kenya ICT Network (KICTANET) published a comprehensive research report on how surveillance laws and technologies may impact the civic space in Kenya.[57] It examined surveillance technologies developed by these companies that are deployed by Kenyan state actors such as the security and law enforcement agencies The report indicated that the relationship between the government's extensive use of surveillance technology and the companies supplying or enabling the use of such tools lacked transparency and that there were no clear legal safeguards on the tools. In some cases, such as with the use of commercial spyware, the interception of communication data by state security forces happened completely extralegally.

With regards to spyware, a 2015 Citizen Lab study linked Kenya and 32 other governments to the FinFisher spyware suite which was used for intelligence and lawful interception until the company ceased operations in 2022.[58] Evidence showed that these surveillance technologies possess invasive and intrusive capabilities for monitoring calls, SMS, and internet activities, circumventing a device's privacy settings and encryption tools, often without the device owner's knowledge. In 2018, Citizen Lab found Pegasus, NSO's spyware infections in Kenya, potentially for political targeting, using covert, sophisticated methods to install spyware on mobile devices.[59] The research report analyzed various sources including reports that linked the Kenyan government agencies such as the Kenyan Police, the NIS, the DMI, the DCI, the National Security Advisory Committee and others as direct and indirect enablers of unlawful surveillance in Kenya.

Aside from spyware, the government has reportedly deployed other commercial tools to monitor mobile communications. In 2017, the National Intelligence Service (NIS), Directorate of Military Intelligence (DMI), and Directorate of Criminal Investigations (DCI) were reported to have conducted phone inter-

57 Kapiyo, Oyier and Monyango (n 5).

58 The Citizen Lab 'Pay No attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation' (15 October 2015) <https://utoronto.scholaris.ca/server/api/core/bitstreams/db739eb7-8a0d-449a-a389-33d6f44c8ab0/content> accessed 20 January 2025.

59 Bill Marczak and others, 'HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries' (Citizen Lab Research Report No 113, University of Toronto 2018) <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> accessed 23 November 2024.

Key Surveillance Trends in Kenya

Widespread use of surveillance technologies

Kenya has the second highest number of surveillance technologies in Sub-Saharan Africa, with companies like Blue Coat Systems, NSO, and Circles providing tools used to target civil society actors.

Impact on civic space

A 2024 KICTANET report highlights the use of surveillance technologies by Kenyan state agencies without regard for international human rights obligations, including tools for phone interception and location tracking.

Legal and privacy concerns

The introduction of systems like NIIMS and Maisha Namba, as well as mandatory SIM-card registration and CCTV installations, have raised significant privacy concerns and faced legal challenges.

Abuse of Surveillance Powers

Reports indicate that Kenyan security agencies have used surveillance technologies to track and intimidate protesters, with telecom companies allegedly providing real-time access to user data, raising serious privacy and human rights issues.

ception, location triangulation, and signal jamming capabilities. They used IMSI catchers (Stingrays) to mimic cell towers and track mobile communications. Technologies like Blackbird and Verint's Engage GI2 were also used for signal geolocation and mobile phone monitoring. Citizen Lab also found Blue Coat devices used for filtering and surveillance, raising concerns about potential misuse.

The government's capability to carry out mass surveillance programs is also vast. In 2012, Kenya received a $100 million grant from China to install CCTV cameras in major cities to improve security.[60] Safaricom was contracted in 2014 to build an Integrated Public Safety Communication and Surveillance System, installing 1,800 CCTV cameras with facial recognition.61 The project faced criticism for privacy breaches and lack of oversight.

Kenya has also required SIM-card registration since 2014 to combat crime and terrorism.[62] Although mobile operators are still not in full compliance with the law, according to the Kenyan Communications Authority, civil society and privacy experts raised immediate concerns about the centralization of sensitive personal data through this registration scheme, including risks to privacy rights, the potential for the misuse of data by government authorities or for data breaches perpetrated by non-state actors. Additionally, the impact on vulnerable groups was noted as they may be unable to fulfill the registration requirements and, therefore, would not be able to acquire a SIM card. The lack of robust and transparent data protection protocols and systems and of independent oversight creates substantial risks that, critics say, are unjustified and disproportionate.[63]

Kenya has sought to expand the registration requirement in 2024 when the Communications Authority of Kenya published a public notice that at the start of 2025, it will enforce new requirements for mobile device registration to ensure tax compliance.[64] Some of the requirements include mandatory upload of IMEI numbers by local phone assemblers to a Kenya Revenue Authority (KRA) portal; importers must disclose IMEI numbers in their import documents, and retailers and wholesalers must only sell tax-compliant devices. Mobile network operators are also required to verify device compliance

60 Business Daily, 'Kenya Gets Sh8.5bn Chinese Grant for CCTV Surveillance' (23 May 2012) <https://www.businessdailyafrica.com/bd/economy/kenya-gets-sh8-5bn-chinese-grant-for-cctv-surveillance-2006672> accessed 23 November 2024.

61 Privacy International, 'Kenyans Face New Privacy Threats as State Expands Surveillance Powers' (8 January 2015) <http://privacyinternational.org/blog/1603/kenyans-face-new-privacy-threats-state-expands-surveillance-powers> accessed 23 November 2024.

62 Privacy International, 'Timeline of SIM Card Registration Laws' (11 June 2019) <http://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws> accessed 23 November 2024.

63 Sumaya Nur Hussein, 'Mandatory Sim Card Registration: Why This Is Alarming for Data Protection and the Right to Privacy of Kenyans' (Centre for Intellectual Property and Information Technology law, 20 May 2022) <https://cipit.strathmore.edu/mandatory-sim-card-registration-why-this-is-alarming-for-data-protection-and-the-right-to-privacy-of-kenyans/> accessed 23 November 2024.

64 Communications Authority of Kenya (CA) [@CA_Kenya], 'PUBLIC NOTICE Enhancing Integrity and Tax Compliance of Mobile Devices in Kenya @Mugonyid @marywambui_m @MoICTKenya @KRACorporate Https://T.Co/SLrxUcariT' <https://x.com/CA_Kenya/status/1849320644921483480> accessed 23 November 2024.

through a whitelist before connecting them. These rules apply to devices imported or assembled from 1 November 2024, while existing devices are not affected. This public notice has also been corroborated by the KRA.[65] These moves have been similarly criticized by civil society, and in December 2024, the Kenyan High Court suspended the order pending further legal review.[66]

Aside from mandatory registration, the government has instituted other policies that raise privacy concerns. In 2016, the Communications Authority of Kenya published a tender for a Device Management System (DMS) to identify active devices, isolate illegal ones, and ensure only whitelisted devices access to public networks.[67] The DMS faced privacy concerns and was initially ruled unconstitutional. Safaricom raised further privacy issues, but in April 2023, the Supreme Court allowed the CA to implement the DMS, partnering with multiple agencies to eradicate counterfeit devices by analyzing International Mobile Equipment Identity (IMEI) data.[68] Concerns about surveillance and lack of clear management rules however persist.

In 2019, the Kenyan government introduced National Integrated Identity Management (NIIMS) to create a central database of personal information for all citizens and residents, assigning unique IDs known as *Huduma Namba*.[69] Legal challenges arose due to privacy concerns, leading to a High Court ruling in 2021 that halted its rollout and required a Data Protection Impact Assessment. In 2022, the government reintroduced the system as Maisha Namba, which is ongoing and is planning to integrate it with digital birth, death certificates, and as a national ID number.

Between June and July 2024, Kenyans staged nationwide public protests against a draft tax law and government corruption tagged #RejectFinanceBill.[70] As the protests progressed, there were reports of police brutality which were swiftly followed by violent

65 Kenya Revenue Authority, 'Declaration of Mobile Devices Incorporating IMEI Numbers at Importation' (5 November 2024) <https://kra.go.ke/news-center/public-notices/2150-declaration-of-mobile-devices-incorporating-imei-numbers-at-importation> accessed 23 November 2024.

66 Abdullah Ajibade, 'High Concerns as Kenya Mandates Mobile Phone IMEI Registration as Part of Tax Compliance Measures' (TechPoint, 24 October 2024) <https://techpoint.africa/2024/10/24/kenya-mobile-phone-imei-registration/> accessed 23 November 2024; Valarie Waswa, 'Tax Compliance or Surveillance Strategy?' (KICTANet, 29 October 2024) <https://www.kictanet.or.ke/tax-compliance-or-surveillance-strategy/> accessed 23 November 2024. Also see, https://mobileidworld.com/kenya-court-extends-suspension-of-mandatory-mobile-device-imei-declaration-requirements/

67 John Walubengo, 'Device Management System by Communication Authority: The Privacy Perspective' (KICTANet, 1 May 2023) <https://www.kictanet.or.ke/device-management-system-by-communication-authority-the-privacy-perspective/> accessed 23 November 2024.

68 The National Council for Law Reporting 'Law Society of Kenya v Communications Authority of Kenta & 10 others (21 April 2023) <http://kenyalaw.org/caselaw/cases/view/256372/> accessed 23 November 2024.

69 Privacy International, 'Data Protection Impact Assessments and ID Systems: The 2021 Kenyan Ruling on Huduma Namba' (27 January 2022) <http://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma> accessed 23 November 2024.

70 ARTICLE 19, 'Kenya: Guarantee Internet Access and Stop Surveillance of Protesters' (28 June 2024) <https://www.article19.org/resources/kenya-guarantee-internet-access-and-stop-surveillance-of-protesters/> accessed 23 November 2024.

abductions and deaths of protesters by members of the Kenyan security forces.[71] There were reports that these abductions of protesters, most of whom went into hiding and in some cases found dead, were aided by the use of surveillance technologies and internet service providers.[72] In a report titled 'Exclusive: How Kenyan Police use mobile phones to track, capture suspects' by the Nation in October 2024, it was noted that Kenya's security agencies had long had unfettered access to mobile phone data, violating privacy rights while tracking criminals.[73] Call data records which enabled real-time access were reportedly provided by telecom companies such as Safaricom with the aid of a British company, Neural Technologies. Safaricom denies breaching privacy despite evidence and inconsistencies in court submissions. Instances of police using this data for sinister purposes, like abductions and killings highlight the serious conflict of interest and threats to civil rights. According to the report, Safaricom insiders revealed that telco prioritized ease of access for law enforcement over stringent safeguards which allowed security agencies real-time access to customer data. This connivance between state and private companies has also been criticized by human rights advocates as it lacks constitutional safeguards and has great potential for misuse.

Of further concern is that existing oversight mechanisms that could exercise powers to check unlawful surveillance have not been effectively utilized. This includes organs such as the intelligence Service Complaints Board (ISCB), whose functions under Section 66 of NISA include handling complaints, ensuring compliance, rights protection, giving recommendations and reporting on NIS's activities and the Independent Police Oversight Authority (IPOA), which must conduct complaints investigation, operations monitoring, investigation audits, public reporting and policy recommendations. Others include the

In an October 2024 report by the Nation newspaper, it was noted that Kenya's security agencies had long had unfettered access to mobile phone data, violating privacy rights while tracking criminals.

71 Mohammed Yusuf, 'Kenyan Security Forces Accused of Abduction, Deaths of Protesters' (Voice of America, 6 November 2024) <https://www.voanews.com/a/kenyan-security-forces-accused-of-abduction-deaths-of-protesters/7853877.html> accessed 23 November 2024.

72 'Kenya: Safaricom Denies Claims of Supporting Surveillance of Perceived Leaders of Protests against High Taxation' (Business & Human Rights Resource Centre, 25 June 2024) <https://www.business-humanrights.org/en/latest-news/kenya-safaricom-denies-claims-of-supporting-surveillance-of-perceived-leaders-protests-against-high-taxation/> accessed 23 November 2024.

73 Namir Shabibi, Claire Lauterbach, and Nation Team, 'Exclusive: How Kenyan Police Use Mobile Phones to Track, Capture Suspects' (Nation, 29 October 2024) <https://nation.africa/kenya/news/exclusive-how-kenyan-police-use-mobile-phones-to-track-capture-suspects-4804416> accessed 23 November 2024.

Kenya National Commission on Human Rights (KNCHR) which has the central mandate of human rights oversight, monitoring and investigations including in relation to surveillance and interception of communications; and the Senate Committee on Justice Legal Affairs and Human whose roles include legislative oversight, policy review and compliance monitoring and human rights protection.

In summary, the various trends and practices of surveillance and interception of communications in Kenya noted above raise at least four key issues:

1. Independent research reports have noted widespread uses of surveillance technologies by state actors in Kenya and these uses are not in line with laid down international human rights standards on lawful surveillance.
2. State actors in Kenya are invested in increasing collection of personal data which raises huge concerns regarding the safety of this data amid the widespread use of unlawful surveillance.[74]
3. Private companies are also active enablers of surveillance practices. In its dealings with these companies (e.g., internet service providers and commercial surveillance technology companies), the government does not operate transparently or require the companies to comply with human rights standards when doing business in Kenya.
4. Domestic oversight mechanisms for surveillance and human rights more broadly, such as those identified below, have not sufficiently exercised their authority to push back or raise the alarm regarding the risks and abuses stemming from unchecked surveillance in the country.

74 Privacy International, 'The Rise of the Surveillance Databases' (24 October 2024) <http://privacyinternational.org/long-read/5455/rise-surveillance-databases> accessed 23 November 2024.

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

STATE ACTORS		
Entity	**Enabling framework**	**Specific roles**
National Police Service (NPS)	Section 243 of the Constitution and Section 3 of the National Police Service Act (NPSA), 2011, Section 36 of the PTA	The NPSA, NISA, PTA and Security Laws (Amendment) Act, 2014 provides the NPS with powers to carry out surveillance and intercept communications for national security and counter terrorism purposes.
National Intelligence Service (NIS)	Sections 4-7, 14 & 18 of NISA	The NIS has the powers to carry out surveillance which includes monitoring, interception and recording of communications under the NISA for the purposes of national interests and counter terrorism.
Cabinet Secretary (Interior & National Administration)	Section 28 of the NISA & Section 36A of the PTA	The Cabinet Secretary oversees the Director General, NIS regarding the implementation of the NISA and is also part of the NSC regarding issues related to surveillance and interception of communications in Kenya.
Director-General, NIS	Section 42-47 of NISA	The Director-General makes requests, coordinates other agencies, implements policies, allocates resources, reports and accounts for surveillance and interception of communications under the NISA.
National Security Council (NSC)	Article 240 of Constitution & Section 4 of the National Security Council Act, 2012	The NSC formulates, integrates and coordinates policies, supervises, assesses and appraises, reports to the Parliament on national security issues including those on surveillance and interception of communications.
Directorate of Criminal Investigations (DCI)	Section 28 of NPSA	The DCI enables surveillance and interception of communications through criminal investigations, cybercrime and digital forensics, counter terrorism, financial crimes and collaboration with other state actors.
Directorate of Military Intelligence (DMI)	The DMI operates under the framework of the NIS as part of the Kenya Defence Forces. The Act outlines the structure of the NIS which includes various intelligence components including the DMI.	Some of the DMI's roles include Signals Intelligence (SIGNIT), supporting military operations and collaborating with other security actors.
Intelligence Service Complaints Board (ISCB)	Section 66 of NISA	Some of ISCB's roles include handling complaints, ensuring compliance, rights protection, giving recommendations and reporting on the NIS's activities regarding surveillance and interception of communications under the NISA.

Independent Police Oversight Authority (IPOA)	Section 3 of the Independent Police Oversight Authority Act	Some IPOA's roles include complaints investigation, operations monitoring, investigation audits, public reporting and policy recommendations regarding the National Police Service's activities on surveillance and interception of communications.
Communications Authority of Kenya (CA)	Section 5 of KICA	As the telecommunications, postal, courier and broadcasting regulator, the CA have the roles of ensuring legal compliance of operators regarding surveillance and interception of communications, collaboration with NPS and NIS to facilitate lawful interception of communications for national security purposes and ensuring consumer rights are protected including the right to privacy.
Office of the Data Protection Commissioner (ODPC)	Section 5 of DPA	The ODPC's roles include regulation and compliance with the DPA, handling complaints, enforcement, public awareness and advisory regarding the relationship between lawful surveillance and the DPA.
National Computer and Cybercrimes Committee (NC4)	Section 4 of CMCA	The NC4's role includes advising the NSC, coordination of cybersecurity efforts, international cooperation as it relates to surveillance and interception of communications.
Kenya National Commission on Human Rights (KNCHR)	Article 59 of the Constitution and Section 3 of the Kenya National Commission on Human Rights Act	The KNCHR has the mandate of monitoring and investigations, redress and remedies, advocacy, advisory, public awareness and education regarding the promotion and protection of human rights in relation to surveillance and interception of communications.
Senate Committee on Justice Legal Affairs and Human Rights	Article 93 & 124 of the Constitution, Standing Order 218 of the Senate Standing Orders.	Some of the Committees' roles include legislative oversight, policy review and recommendations, public inquiries and hearings, compliance monitoring and human rights protection regarding surveillance and interception of communications.
National Assembly Departmental Committee on Communication, Information and Innovation	Article 93 & 124 of the Constitution, Standing Order 216 (1) of the Standing Orders of the National Assembly.	
National Assembly Departmental Committee on Justice and Legal Affairs		

Judicial Service Commission (JSC)	Article 71 of the Constitution, Section 3 of the Judicial Service Act (JSA), 2011	The JSC performs judicial oversight, appointment of judges, and policy recommendations regarding the surveillance and interception of communications.

NON-STATE ACTORS

Sector	Key actor	Specific roles
Internet Service Providers (ISPs)	Safaricom, Faiba, Zuku, Telkom, Airtel Kenya, Poa!	These ISPs are required to cooperate with security agencies such as the NIS and NPS to facilitate lawful interception of communications.
Social media platforms	WhatsApp, Twitter (X), Facebook, TikTok, Instagram, Telegram.	Some of their specific roles include sharing user data with security agencies in specified circumstances in compliance with local laws on national security, counterterrorism or other serious crimes.
Civil society actors	Privacy International, KICTANET, Kenya Human Rights Commission, National Coalition of Human Rights Defenders (NCHRD-K), ARTICLE 19 Eastern Africa, Amnesty International Kenya.	Some of their specific roles include research and documentation, advocacy and awareness, legal support and representation for strategic litigation, capacity building, policy analysis and recommendation, monitoring and reporting.
Surveillance technologies companies	See section 3 above.	These include transparency and accountability, training and support on lawful surveillance, human rights due diligence, providing data and communications integrity as emphasized by the HRC and ACHPR in interpreting international human rights frameworks such as the ICCPR and the African Charter.

4. The Human Rights Impact of Unlawful Surveillance and Interception of Communications on Civil Society Actors

The inadequate safeguards that exist in both the laws and practices on surveillance and interception of communications by state actors pose unprecedented risks to the rights of civil society actors including non-governmental organizations, human rights defenders, journalists, at-risk groups active in the digital space in Kenya. These rights, which are interdependent and intrinsically linked are impacted in varying degrees and have become a source of concern among civil society actors in Kenya. The impact on some of these rights are discussed below.

4.1 RIGHT TO PRIVACY

The central principle of the right to privacy, especially as it relates to the digital age, is to protect human dignity and guard against unauthorized intrusion into personal information and spaces. Where such intrusion must occur as a result of lawful surveillance, it must be in accordance with international human rights standards examined under chapter 1. A state's failure to comply through law or practice increases the risks to vulnerable actors, such as civil society advocates, both online and offline. Vast, unchecked surveillance powers can lead to selective, arbitrary enforcement, with the looming threat of potential arrest, interrogation, or punishment for acts that may be completely unrelated to a specific investigation. Mass data collection, particularly the collection of biometric data, can be exploited by either government authorities or malicious non-state actors, and once such databases are breached, the harm from the disclosure of an individual's immutable characteristics may never be remedied. This can therefore undermine democratic governance and erode public trust in public institutions. Additionally, unlawful surveillance limits intellectual production and autonomy as civil society actors do not have the liberty to communicate and explore ideas without the fear of being watched and surveilled.

In Kenya's 2024 #RejectFinanceBill protests, the unauthorized monitoring and surveillance of personal communications of civil society by state actors through the aid of private actors not only violated the right to privacy of protestors and other individuals in the vicinity, it also led to the detention of hundreds of people through unlawful practices that human rights organizations have deemed to amount to enforced disappearances.[75]

4.2 RIGHT TO FREEDOM OF EXPRESSION AND OPINION

The ability to freely express oneself and disseminate opinions is one of the central tenets of the right to freedom of expression. However, the state of surveillance practices

75 <https://www.amnesty.org/en/latest/news/2024/06/kenya-abductions-of-citizens-suspected-of-involvement-in-protests-violate-human-rights/>

in Kenya threatens this right.[76] For example, when civil society actors and individuals refrain from expressing their opinions due to the fear of being monitored, it stifles dissent and encourages self-censorship. It also limits the diversity of viewpoints that are necessary for enriching public debate in an open society. Additionally, civil society actors may avoid controversial, but otherwise lawful, conversations and activities, both online and offline, in order to stave off digital or physical attacks and harassment by state actors. For example, media practitioners critical of government actors in Kenya have reported an increase in self-censorship as a result of unlawful surveillance.[77] Ultimately, these impacts erode trust in the integrity of communications in Kenya as it is becoming increasingly unsafe to communicate freely using digital devices for the fear of being monitored. Surveillance data can also be used to justify arbitrary and disproportionate orders for websites or applications to remove content or user accounts. All these impacts increase prosecution, persecution, blackmail and coercion of civil society actors, restricting their ability to operate or conduct activities.

4.3 RIGHTS TO ASSOCIATION AND ASSEMBLY

Surveillance significantly impacts the freedoms of association and assembly of civil society by creating a chilling effect where individuals avoid participating in protests and meetings due to fear of being monitored, which leads to reluctance to associate with groups under surveillance. The use of high-powered and intrusive technologies such as facial recognition and AI-enabled surveillance significantly increases the risks to the rights to association and assembly of civil society actors.[78] It also fosters intimidation and harassment by targeting activists, causing psychological distress and deterring public assembly. Recently, twelve Kenyan human rights organizations condemned Safaricom, an ISP in Kenya, for allegedly harassing of civil society actors because of a report that linked increased surveillance to

76 Freedom House, 'Kenya: Freedom on the Net 2024 Country Report' <https://freedomhouse.org/country/kenya/freedom-net/2024> accessed 23 November 2024.

77Collaboration on International ICT Policy in East and Southern Africa (CIPESA) 'Legal and Regulatory Frameworks Affecting Civil Society Organisations' Online and Offline Activities in Kenya' (2017) <https://cipesa.org/wp-content/files/briefs/report/Legal-and-Regulatory-Frameworks-Affecting-CSOs-Online-and-Offline-Activities-in-Kenya> accessed 20 January 2025.

78 ICNL Submission (n 2).

How Unlawful Surveillance Impacts the Exercise of Rights

It undermines democracy

Unlawful surveillance in Kenya severely impacts civil society actors by violating their right to privacy through unauthorized monitoring, which undermines democratic governance and erodes public trust.

It leads to self-censorship

Surveillance stifles freedom of expression, leading to self-censorship and increased harassment of media practitioners and human rights defenders.

It weakens public participation

Surveillance also deters participation in protests and meetings, fostering intimidation and disrupting group dynamics, thus weakening civil society's role in democratic engagement.

It exacerbates inequalities

Surveillance also disproportionately targets marginalized communities, exacerbating inequalities and reinforcing systemic discrimination, while creating a hostile environment that leads to chronic stress, anxiety, and reduced productivity, ultimately deterring individuals from seeking necessary help.

enforced disappearances.[79] Surveillance erodes trust within groups, disrupts group dynamics, and suppresses dissent by controlling information flow and taking preemptive actions against planned assemblies. Legal and extralegal repercussions, such as arrests and blackmail, further deter participation. Unlawful surveillance undermines democratic engagement and weakens civil society's role in holding governments accountable and advocating for social change. Additionally, the rights of civil society actors that are targets of unlawful surveillance also affect their family life as they are often forced to avoid their loved ones for the fear of putting them at risk of arrests and harassment by state actors.[80]

4.4. RIGHT TO PARTICIPATE IN PUBLIC AFFAIRS

One of the primary roles of civil society is to act as watchdogs concerning issues of public affairs in order to hold both private and public powers accountable for their actions. When unlawful surveillance is conducted by state actors, it seeks to take away that critical role performed by them. One of the key features of the right to public participation includes the right to be part of consultative processes that shape public policy including those on surveillance and state's interception of communications,[81] engaging in debate and dialogue, and doing these with mutually reinforcing rights such as the rights to privacy, expression, association and assembly and others. However, in Kenya, in instances where civil society actors know their devices have been tapped or they are under heavy monitoring by state actors, they have taken increased security measures to be safe,[82] straining the rights of individuals to take fully and freely take part in civil society and public affairs.

4.5 RIGHT TO NON-DISCRIMINATION

The impact of unlawful surveillance on the right to non-discrimination and the protection of groups are severe as it disproportionately targets marginalized communities.[83] In 2021, Front Line Defenders published a report on how the governments of Uganda and Kenya give South Sudanese National Security Service (NSS) information about whereabouts of human rights workers who fled South Sudan to seek refuge in their countries. This highlights cases of transnational digital surveillance and data sharing among African governments in ways that not only target human rights defenders,

79 Joy Kwanza '12 Organizations unite against Safaricom for harassment' (1 December 2024) <https://thekenyatimes.com/latest-kenya-times-news/12-organizations-unite-against-safaricom-for-harassment/> accessed 20 January 2025.

80 Defenders Coalition (46).

81 ALT Advisory, 'Kenyan High Court Declares Surveillance Policy Unconstitutional' (10 May 2018) <https://altadvisory.africa/2018/05/10/kenyan-high-court-declares-surveillance-policy-unconstitutional/> accessed 23 November 2024.

82 Defenders Coalition (46).

83 OHCHR, 'Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns' (16 September 2022) <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report> accessed 23 November 2024.

but do so based on their national origin.[84] In a survey carried out by Defenders Coalition, there are concerns over disproportionate state-sponsored surveillance of human rights defenders who work with marginalized or discriminated groups.[85] For example, researchers have identified how women journalists and human rights defenders face disproportionate and wide-spread technology-facilitated online gender-based violence through sharing of non-consensual intimate images, doxing, and creation and distribution of AI-generated pornographic images.[86] Moreover, the fear of constant monitoring deters vulnerable groups from participating in public life, expressing their opinions, or engaging in activism, further marginalizing them and limiting their advocacy efforts.[87]

Digital surveillance tools may also compound the current day impacts of historic discrimination. Surveillance technologies, such as facial recognition, have been shown to exhibit biases that lead to misidentifications and wrongful accusations which exacerbate existing inequalities and reinforce systemic discrimination. The biases may be a result of the prejudices of the technology developers, the prejudices embedded in the historical data the developers use to develop the tools, or both. When surveillance is seen to target people or groups due to their belonging to a specific group or identity, it severely undermines trust between these communities and public institutions which discourages them from seeking help or reporting abuse.

4.6 RIGHT TO MENTAL AND PHYSICAL HEALTH

The impacts of unlawful surveillance on the mental and physical health of civil society actors are also severe as it creates a constant sense of being monitored which could lead to heightened stress, anxiety, and paranoia. This persistent fear can cause chronic stress and could contribute to mental health issues like depression and anxiety disorders.[88] The psychological burden of surveillance can also lead to feelings of helplessness and loss of control. Physically, chronic stress from surveillance can result in conditions such as hypertension, cardiovascular diseases, and weakened immune function. Human rights defenders in Kenya have noted that the fear of being watched can deter them from seeking necessary medical or psychological help which worsens health outcomes.[89]

84 Front Line Defenders 'No Refuge: South Sudan's Targeting of Refugee HRDs Outside the Country' (March 2021) <https://www.frontlinedefenders.org/sites/default/files/no_refuge_-_final.pdf> accessed 20 January 2025.

85 Defenders Coalition (46).

86 Association of Media Women in Kenya 'An Investigation on the Prevalence of Technology Facilitated-gender Based Violence (TFGBV) Against Women with Prominent Public Lives' 26 November 2024 <https://amwik.org/wp-content/uploads/2024/11/AMWIK-TFGBV-RESEARCH-2024.pdf> <https://thekenyatimes.com/latest-kenya-times-news/12-organizations-unite-against-safaricom-for-harassment/> accessed 20 January 2025.

87 Amnesty International, 'The Right to Privacy in the Digital Age: Submission to the Office of the High Commissioner for Human Rights for the Report on the Right to Privacy in the Digital Age' (14 June 2022) <https://www.ohchr.org/sites/default/files/documents/issues/digitalage/reportprivindigage2022/submissions/2022-09-06/CFI-RTP-Amnesty-International.pdf> accessed 23 November 2024.

88 Tamar Kaldani and Zeev Prokopets, 'Pegasus Spyware and Its Impact on Human Rights' (Council of Europe 2022) <https://edoc.coe.int/en/data-protection/11112-pegasus-spyware-and-its-impact-on-human-rights.html> accessed 23 November 2024.

89 Defenders Coalition (46).

5. Good Practices on the Regulation and Oversight of Lawful Surveillance and Interception of Communications in Kenya and Other Jurisdictions

5.1 LITIGATION

Private individuals and civil society actors in Kenya have utilized the courts to pronounce on privacy and surveillance-related matters. On 31 May 2023, in the case of *Ondieki v Maeda*, the High Court of Kenya ruled on a violation of the constitutional right to privacy concerning the installation of CCTV cameras in a residential area.[90] The petitioner, Maeda, claimed that the CCTV cameras installed by his neighbor, Ondieki, infringed on his privacy by monitoring and recording activities on his property. The court determined that Ondieki, as a data controller, was required to register with the Data Commissioner and obtain Maeda's consent for data collection via the CCTV cameras. The court declared that Ondieki's actions violated Maeda's rights under Article 31 of the Constitution and the DPA. This case provides an important precedent for prospective litigants seeking to challenge unlawful surveillance in Kenyan courts.

In the case of *R v. Joe Mucheru and 2 others ex parte Katiba Institute and another,*[91] the High Court of Kenya declared the rollout of the *Huduma Namba* is illegal due to violations of the Data Protection Act, 2019, specifically the failure to conduct a required Data Protection Impact Assessment (DPIA). The court found that this omission posed a high risk to the rights and freedoms of data subjects. The case was brought by the Katiba Institute, led by Yash Pal Ghai, citing inadequate protection of personal information. The court annulled the rollout decision, mandated a Data Protection Impact Assessment before further data processing and halted the second phase of registration until compliance with the Act is ensured.

In the case of *Okoiti v Communications Authority of Kenya*,[92] the High Court of Kenya declared the Communications Authority of Kenya's plan to access mobile service subscribers' data unconstitutional. The case initiated by a legal trust's executive director argued that the system violated privacy rights and lacked sufficient public participation. The government claimed the system was needed to monitor illegal mobile devices, but the court found that it posed a privacy threat and that less restrictive measures could be used. Additionally, the court noted that the system was not provided by law, referencing international and regional privacy standards. These cases provide a fertile foundation for interested private individuals and civil society actors to institute cases

90 Ondieki v Maeda (Petition E153 of 2022) [2023] KEHC 18290 (KLR).

91 Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested Party) [2021] KEHC 122 (KLR).

92 Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others [2018] eKLR.

in court in cases where their privacy and other human rights have been violated as a result of surveillance and interception of communications.

5.2 CRITIQUE OF DESIGNATED JUDGES

In the *locus classicus* South African case, *amaBhunghane Centre for Investigative Journalism NPC and Another v Minister for Justice and Correctional Services and Others,*[93] the court identified significant shortcomings in South Africa's surveillance law, the Regulation of Interception of Communications and Provision of Communication-Related Information Act[94] (RICA) regarding the safeguards for the selection and role of the designated judge who authorizes interception directions and the absence of an adversarial process. The constitutional concerns were two-fold:

Independence of the designated judge:

The court found that the independence of the designated judge is compromised by the current selection process and the unlimited duration of their appointment. According to the RICA, the designated judge is appointed solely by the Minister of Justice, which the court deemed untenable. To address this, the court recommended that the Chief Justice should nominate the designated judge with confirmation by the Minister of Justice, for a non-renewable term of two years. This provides a useful example in ensuring adequate safeguards regarding surveillance and interception of communications and access to justice in two ways. First, it dilutes the powers of the appointing authority to include an additional arm of government which in this case is the judiciary. Second, it guards against the misuse or abuse of judicial powers by continually putting different judges in the role after each two-year period.

Absence of an adversarial process:

The court also highlighted the lack of an adversarial process which undermines the efficacy of the judicial role. The right to a fair hearing and the full application of the *audi alterem partem* principle (the right to be heard) by the subject of surveillance are not currently provided within the RICA framework. This

93 amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others [2019] ZAGPPHC 384.

94 Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 <https://www.justice.gov.za/legislation/acts/2002-070.pdf>

Good Practices: Regulation and Oversight

Litigation

Courts in Kenya have ruled on privacy violations, such as in cases involving CCTV installations and the Huduma Namba rollout which emphasizes the need for data protection and public participation.

Designated judges

The South African case highlighted the importance of independent judicial appointments and the need for an adversarial process to ensure fair hearings in surveillance matters.

Advocacy and digital security training

Civil society in Kenya actively advocates for legal reforms and provides digital security training to journalists, activists, and human rights defenders to counter surveillance risks.

Judicial training

Kenya should draw inspiration and expertise from the European Union which promotes regional judicial training to enhance the skills of judicial officers to ensure adherence to minimum standards for surveillance requests and mutual legal assistance.

absence renders the relevant provisions unconstitutional. In summary, the court held that the current model under RICA fails to ensure the independence of the designated judge and does not provide a fair hearing process for the subjects of surveillance, necessitating constitutional amendments to address these issues.

5.3 ADVOCACY AND DIGITAL SECURITY TRAINING

The prevalence of unlawful surveillance and interception of communications in Kenya has increased human rights risks for civil society actors. Some of these risks include the violation of the rights to privacy, expression, association, assembly and other associated rights. In order to counter these risks, civil society actors have been involved in various calls for legal and policy reforms to limit rights and abuse state powers.[95] These have been done through submissions during public participation calls for draft laws. Additionally, civil society actors have been the most active regarding training on digital security in Kenya. These trainings often include basic, intermediate and advanced training for journalists, activists, and human rights defenders. Civil society actors carry out training and periodic assessment of their organizational security. These are practices that could be improved on and included in proposals for legal reforms on the legal and digital protection for civil society actors.

5.4 JUDICIAL TRAINING

Capacity building of the judiciary on the regulation of digital surveillance and good practices globally is crucial in ensuring adequate protection for civil society. A good example is the Commission for the European Union which provides regional judicial training.[96] Similar initiatives can be integrated domestically or across subregions in Africa. Training is important not only to facilitate an upskill of judicial officers involved in the authorization of surveillance requests or applications but also crucial in the context of ensuring rights-respecting mutual legal assistance among member countries. The training provides judicial officers with the minimum standards to be considered in instances where security agencies make surveillance or interception of communications requests.

95 National Coalition of Human Rights Defender-Kenya (NCHRD-K) and others, 'The Right to Privacy in Kenya' (2019) <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://uprdoc.ohchr.org/uprweb/downloadfile.aspx%3Ffilename%3D7566%26file%3DEnglishTranslation&ved=2ahUKEwjwobLMh-2JAxVHgP0HHSIsNHAQFnoFCIcBEAE&usg=AOvVaw3V7HdTGvyt3JdMYPcYLYhr> accessed 23 November 2024.

96 United Nations Office on Drugs and Crime (UNDCP), Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime (United Nations 2009) <https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf> accessed 23 November 2024.

6. Conclusion and Actionable Recommendations

In conclusion, this research report highlights the pervasive and multifaceted impact of unlawful surveillance on civil society actors in Kenya. It underscores the urgent need for robust legal frameworks and effective oversight mechanisms to protect fundamental rights such as privacy, freedom of expression, and association. The study reveals how state and private actors' use of advanced surveillance technologies without adequate safeguards undermines democratic governance, erodes public trust, and disproportionately affects marginalized communities. To address these challenges, the report calls for comprehensive legal reforms, enhanced transparency, and accountability in surveillance practices and increased advocacy and training to safeguard the rights of civil society actors and ensure alignment with international human rights standards.

PARLIAMENT (NATIONAL ASSEMBLY AND SENATE)

- Ensure public participation on legal reforms that include the repeal and amendment of applicable laws highlighted above to ensure adequate legal safeguards on surveillance and interception of communications.
- Establish an independent mechanism that integrates administrative, judicial, and parliamentary oversight which ensures human rights expertise, institutional separation, proactive monitoring, transparency, public scrutiny, remedy and appeal mechanisms, and diverse viewpoints through expert and multi-stakeholder consultations to exercise oversight functions regarding surveillance practices.
- Mainstream the draft Declaration on human rights defenders when adopted by the African Commission to guarantee more human rights safeguards.
- Commit to audits of security agencies especially regarding transparency in the procurement and deployment of surveillance technologies.
- Engage in multi-stakeholder consultations for a policy framework that clearly defines the corporate accountability for surveillance companies including definition of surveillance harms and abuse, oversight and accountability mechanisms, human rights impact assessment and access to remedy.

SECURITY AGENCIES AND OTHER STATE INSTITUTIONS (NPS, NSC, NIS, CA, DCI, DMI, CABINET SECRETARY, ISCP, IPOA, ODPC, NC4)

- Ensure access to continuous legal advisory and training for those who have legal obligations and are involved in the purchase, deployment, and operation of surveillance and interception of communications.

JUDICIARY (JSC, NCAJ)

- Develop a continuously updated training manual for judicial officers on surveillance, interception of communications.
- Support peer-to-peer exchange with judicial officers from other countries and regional mechanisms on best practices and emerging trends in adjudicating surveillance and interception cases.
- Ensure stakeholder engagement for both state and non-state actors in the justice sector to provide rights-respecting guidance related to surveillance and interception of communications.

KENYAN NATIONAL COMMISSION ON HUMAN RIGHTS

- Engage more critically with both local, regional and international stakeholders on how to align Kenyan laws and practices on surveillance and interception of surveillance with international human rights obligations.

PRIVATE ACTORS (INTERNET SERVICE PROVIDERS, SOCIAL MEDIA PLATFORMS AND SURVEILLANCE TECHNOLOGY COMPANIES)

- Develop and implement robust human rights impact due diligence processes for consumer rights and government requests for surveillance and interception in line with international human rights and constitutional standards.
- Commit to the highest level of use of privacy-enhancing technologies such as encryption, anonymization, pseudonymization to protect consumer rights.

CIVIL SOCIETY ACTORS

- Increase advocacy and campaigns for lawful surveillance culture in Kenya through research, training of the media and other public actors, documentation and reporting, policy recommendations and strategic litigation.
- Utilize freedom of information requests to demand transparency from state and businesses involved in the purchase and use of surveillance technologies.
- Monitor, document and increase the visibility on trends and practices of unlawful surveillance in their reports to international and regional human rights mechanisms such as the Universal Periodic Review and Periodic Reports to the African Commission and also follow up to monitor compliance with recommendations by these mechanisms.

AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS

- Provide more guidance for States through the adoption of resolutions and other soft human rights law standards to member states on the impacts of unlawful and mass surveillance on various human rights and vulnerable groups including civil society actors in Africa.
- Ensure the implementation of the provisions of privacy and communication surveillance under the Declaration on Principles of Freedom of Expression and Access to Information in Africa.
- Carry out a comprehensive continental study on the impact of surveillance and interception of communications on human rights in Africa to inform its norm-setting standards for States.
- Adopt a model rights-based framework on surveillance, interception of communications and human rights in Africa
- Support region-wide training for judge-designates who authorize surveillance and interception request.

MEDIA PRACTITIONERS

- Ensure adequate and independent coverage of issues related to threats of unlawful surveillance and interception of communications to ensure accountability and public oversight.

DEVELOPMENT PARTNERS

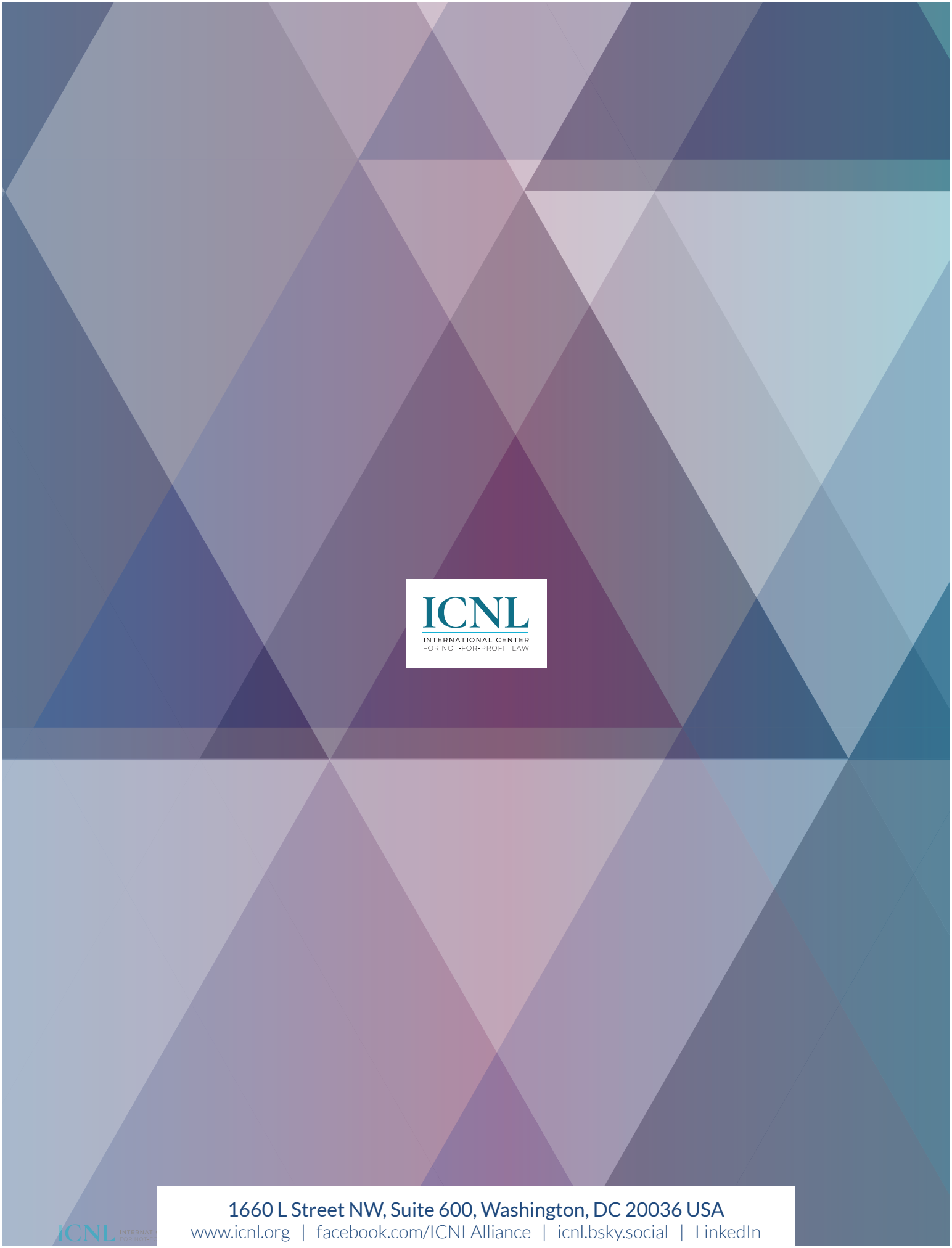
- Require that human rights impact assessments are carried out and implemented regarding the purchase and use of technologies capable of surveillance and interception of communications.

RESEARCH INSTITUTIONS AND ACADEMIA

- Increase research focus on the intersectional impacts of unlawful surveillance and interception of communications on human rights and vulnerable groups in Kenya and across the region.

REGIONAL ECONOMIC COMMUNITIES

- Consider the impacts of unlawful surveillance on the rule of law in their respective regions and urge member states to adopt rights-respecting standards on surveillance and interception of communications.



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