National Coalition
of Human Rights Defenders - Kenya

STOP

WATCHING ME

A perception survey on communication surveillance and privacy of Human Rights Defender in Kenya

The National Coalition of Human Rights Defenders - Kenya
(NCHRD-K)
P.O. Box 26309 - 00100, Nairobi, Kenya
Cell: +254 712 632 390 **HOT LINE: 0716 200 100**
info@hrdcoalition.org |www.hrdcoalition.org

PRIVACY INTERNATIONAL
62 Britton Street,
London, EC1M 5UY UK

Designed & Printed By: Myner Logistics Ltd

62 Britton Street,
London, EC1M 5UY
UK

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF ABBREVIATIONS

AU	African Union
CDTD	Centre for Domestic Training and Development
CA	Communications Authority of Kenya
CCK	Communications Commission of Kenya
CIGI	Centre for International Governance Innovation
CSO	Civil Society Organisation
HRC	Human Rights Committee
HRD	Human Rights Defender
ICCPR	International Covenant on Civil and Political Rights
ICRT	Information and Communication Technology
IGAD	Inter-governmental Authority on Development
ITU	International Telecommunications Union
KHRC	Kenya Human Rights Commission
KNCHR	Kenya National Commission for Human Rights
KICA	Kenya Information and Communications Act
LGBTQI	Lesbians, Gay, Bisexual, Transgender, Queer/ Intersex
MUHURI	Muslim for Human Rights
NCHRD-K	National Coalition of Human Rights Defenders-Kenya
NGO	Non-governmental organisations
NIS	National Intelligence Service
PBI	Peace Brigades International
SOGIE	Sexual Orientation Gender Identity
UDHR	Universal Declaration on Human Rights
UN	United Nations

ACKNOWLEDGEMENTS

This is a report of the perception on surveillance by human rights defenders commissioned by the National Coalition of Human Rights Defenders= Kenya and Privacy International. The report was written by George Gathigi and Patrick Mutahi. We thank them for the professionalism and patience

We appreciate input provided by the staff of the National Coalition of Human Rights Defenders- Kenya and Privacy International throughout the processes. We thank the board of trustees and donor partners for all their support. Last but not least, we are grateful to human rights defenders in Kenya who took part in the survey and key informants who provided insight about communication surveillance and privacy.We believe that the study offers useful recommendations to enhance the protection of privacy

EXECUTIVE SUMMARY

This survey set out to assess Human Rights Defenders' (HRDs') level of exposure, understanding and perception of communication surveillance as well as identify their strategies for mitigating it.

It was guided by broad research questions around the norms and legal frameworks that govern right to privacy; the emerging patterns of how the State uses these laws and how they affect HRDs and their work.

Key findings:

- There are concerns about privacy of personal and work-related information being improperly and unlawfully accessed by different actors.
- Human Rights Defenders exhibited varying degrees of apprehensions on possible personal information breaches but there are gaps between concerns about online surveillance and the actual practice of information sharing.
- There are various sources of information on surveillance with intelligence services perceived as the most likely followed by police, telecommunications and internet service providers. Others include criminals, friends, private companies and families.
- The increased use of digital-based media and online interactions has enabled expansion and new forms of surveillance. The findings indicate that HRDs are exercising some caution in terms of what they share. However, this still exposes them to the risk of surveillance.
- HRDs use diverse tools to communicate and face-to-face communication is perceived as the most secure in the survey. However, interviews revealed that there are still concerns in interpersonal engagements. Calling the landline, using mobile chats and sending text messages were also perceived as relatively secure even if this is not technically accurate. Posting on social media and sending email without encryption are perceived as least secure.
- HRDs have adopted practices that improve communication security and privacy. The most common are use of passwords to lock personal gadgets, customising privacy settings to limit views on social media, regular check of information to be collected and use of different communication tools. Reluctance to accept phones and computer donations, securing and disguising online footprints were also rated highly.
- HRDs value privacy more than convenience in internet use. When they sense they are being monitored, some HRDs change their behaviour in varying degrees including by protecting private information, their perception of privacy and protecting browsing habits.

- Majority of the respondents reported that they have experienced security breaches that include unlawful access to their social media and email accounts as well as phone tapping.
- On interpersonal, relational and physical dimensions of communication surveillance, the two levels of HRDs work -national and county -have provided newer dimensions of surveillance. HRDs touching on county governments are more vulnerable to surveillance because of their proximity to those they monitor. Infiltration by individuals masquerading as HRDs was also reported.
- HRDs working in or sympathetic to minority rights areas such as LGBTQI face more risks of surveillance. Those that use media for advocacy work at the county level also face challenges.
- Many HRDs are equipped to handle issues of preparedness, individual organisational safety, responding, rescuing, and attendant policies and protocols. However, they are not adequately prepared on communication surveillance policies and data protection.
- The levels of knowledge of communication surveillance and information security vary greatly. Beyond policies and skills, there is not much investment in physical resources needed to secure information. Some organisations have adopted protective measures that include installing alarm systems, CCTV cameras and backing up data to ensure that it cannot be completely lost.

Recommendations

For government:

- Ensure an inclusive process for the development and enactment of the proposed Data Protection Bill that conform with the Constitution of Kenya, 2010 and international standards and best practices on protection of privacy.
- Ensure that the Computer Misuse and Cybercrimes Act, 2018 to conform with the Constitution and international standards of protecting freedom of expression.
- Review existing policies and laws and enact further legislation as may be necessary to provide an environment for defenders to work freely and safely without communication surveillance.
- Prevent unlawful surveillance of human rights defenders, and investigate and prosecute all perpetrators of reported cases of unlawful surveillance.
- Take necessary measures to reform surveillance policies and practices to ensure they comply with Kenya's national and international human rights obligations and ensure that any information collection process is consistent with Fair Information Practices.
- Call for accountability and transparency of law enforcement, security agencies

and private bodies undertaking surveillance activities.

- Introduce safeguards to ensure that that individuals' rights and data are protected, in particular mobile telephony subscribers.

For the private sector:

- To ensure meaningful access, opt-out, and other rights, there must be a way to provide people with notice about all of the companies collecting their information.
- Be transparent about their business models as well as how personal data obtained as a result of the use of their services is being processed.
- Make public the measures they take to respond to government requests for their clients' personal data, for example, through regular publication of detailed transparency reports.

For the Kenya National Commission on Human Rights:

- Call for an independent authority to investigate communications surveillance programmes conducted by the Kenyan government and ensure that these practices respect Kenya's national and international obligations to protect the privacy of its citizens and their personal data.
- Investigate all reported cases of unlawful surveillance of human rights defenders and ensure redress mechanisms are available should these lead to identification of violations of the right to privacy.
- Advocate adoption of safeguards to ensure that State surveillance of online and offline activities is lawful and does not infringe on HRDs' right to freedom of expression and ability to do their work, including through use of information communication technologies.

For national, local, and international CSOs and HRDs:

- Advocate enactment of the Data Protection a that conforms to the Constitution and international privacy standards.
- Advocate for the review of the Computer Misuse and Cybercrimes Act, 2018 to conform with the Constitution and international standards of protecting freedom of expression.
- Advocate policies and practices of the private sector, including telecommunications companies, that conform to international human rights and meet the standards as stipulated by the Ruggie principles.
- Build capacity of their staff and networks to assess threats and risks and to identify relevant and effective mitigation strategies.
- Assist grassroots HRDs to establish direct networks including with donors to ensure

they access necessary resources for their growth.

- HRDs establish Communities of Practice to hold each other accountable, exchange ideas and best practices to reduce threats of surveillance.
- Create and strengthen county-based networks which can support HRDs to understand and respond to information security challenges.
- Place communication surveillance and information security on top of the agenda in HRDs forums.
- Organisations and networks reconsider common practices which expose HRDs.

For donors:

- Provide necessary resources, financial and technical, to support HRDs and CSOs to build secure systems, and develop plans and policies that can improve implementation of secure communication policies and practices.
- Provide funding to rural-based CSOs to work on issues of privacy and surveillance.
- Support HRDs to network including participation in regional and international forums such as African Commission for Human rights and UN mechanisms like Special Rapporteurs.

For policymakers and law enforcers:

- Ensure open, inclusive legislative process when adopting a Data Protection Bill which must conform to the Constitution and Kenya's international human rights obligations, and in particular the right to privacy.
- Review and reform existing policies and laws and adopt new legislation that provide an environment for defenders to work freely and safely without communication surveillance.
- Investigate all reported cases of unlawful surveillance of human rights defenders.
- Demand reform of surveillance policies and practices to ensure they comply with Kenya's national and international human rights obligations.
- Call for accountability and transparency of law enforcement and security agencies undertaking surveillance activities.
- Call for accountability and transparency of the private sector policies and practices which interfere with the right to privacy of individuals and require the processing of personal data.

INTRODUCTION

The right to privacy is a fundamental right protected in law across the world including Kenya as stipulated in the Bill of Rights in the 2010 Constitution. It is essential to the protection of human dignity and serves as the foundation upon which many other rights are built. Privacy denotes "that area of individual autonomy in which human beings strive to achieve self-realization ... alone or together with others."[1]

The UN Human Rights Special Rapporteur on Freedom of Expression has presented privacy as the ability of individuals to determine who holds information about them and how that information is used.[2] As for the UN Human Rights Committee, privacy, as envisioned in the International Covenant for Civil and Political Rights, refers to "a sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with others or alone.[3]"

Numerous Kenyan HRDs have raised concerns about their mobile phones being tapped and their communication intercepted.[4] These experiences have implications for HRDs and, therefore, it is essential to ensure that HRDs are not the subject of unlawful surveillance practices and that they are able to do their work without fear of snooping by anyone.

Privacy helps individuals maintain their autonomy and individuality. People define themselves by exercising power over information about themselves and a free country does not ask people to answer for the choices they make about what information is shared and what is held close. Privacy allows our many cultures and subcultures to define for themselves how personal information moves in the economy and society. Loss of privacy leads to loss of freedom which includes the freedom of expression limiting one's ability to carry out their duties and obligations.

This report analyses the needs, concerns and areas of interest for HRDs in relation to privacy, data protection, and communications surveillance. It also establishes how surveillance impacts HRDs work and their role as actors of change in society. Human rights work demands the use of communication tools ranging from face-to-face, telephones and e-mails and short message services (SMS). All these provide varying degrees of risk, which are also specific to the work the HRDs are engaged in, as well as contexts. Examining the risk levels based on these specifics as well as finding the best-suited measures will be important for continued HRDs protection. Lastly, the report offers recommendations to various actors including HRDs to assist them to develop intervention and advocacy strategies.

1 Nowak, M. (1993) U.N. Covenant on Civil and Political Rights: CCPR Commentary, (2nd ed) Kehl am Rhein, Germany; Arlington, VA: N.P. Engel Publishers.
2 United Nations (2013) 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' A/ HRC/23/40, 17 April 2013
3 http://www.humanrights.is/en/human-rights-education-project/comparative-analysis-of-selected-case-law-achpr-iachr-echr-hrc/the-right-to-respect-for-private- and-family-life/what-is-private-life
4 "Not Worth the Risk" Threats to Free Expression Ahead of Kenya's 2017 Elections," 2017 Human Rights Watch, https://www.hrw.org/sites/default/files/report_pdf/
kenya0517_web.pd

BACKGROUND AND CONTEXT

Regional and international laws, policies and treaties Kenya is party to.

As provided in Article 2(5) of the Constitution, general rules of international law and any treaty or convention ratified by Kenya shall form part of the law of Kenya. This means that the international laws and principles directly apply in Kenya to the extent that they are not in contravention of the Constitution.

The Universal Declaration of Human Rights (UDHR), in Article 12, provides for the protection against arbitrary or unlawful interference with privacy, family, home or correspondence as well as against unlawful attacks on honor and reputation. The UDHR provisions are echoed in other international treaties that Kenya has ratified. These include the International Covenant on Civil and Political Rights (ICCPR) which protects the right to privacy in Article

17. It places an obligation on Kenya to adopt legislative and other measures to give effect to the prohibition against such interferences as well as to the protection of the right to privacy. Article 17 envisions that surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping, and recording of conversations should be not be undertaken if inconsistent with Article 17 9.

While it has not yet come into force, the African Union Convention on Cyber Security and Personal Data Protection 2014 is the first regional treaty seeking to advance data protection. In draft Article 8, it provides that "[e]ach State Party shall commit itself to establish a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data." It is important to note that there have been strong criticisms against the Convention, and its implications for human rights.10

In 2016, the Kenya government also released a Draft National Information & Communications Technology (ICT) policy. The policy is one of the steps towards achievement of Vision 20308, Kenya's national long-term development blueprint, whose goals include the achievement of an information society and knowledge economy. It seeks to achieve this through improved data protection, cyber security, network security, and information security.

Legal framework for the protection of information and Communication in Kenya

In Kenya, numerous mechanisms are in place to guarantee the protection of the right to privacy. In 2010, the right was constitutionally entrenched in Article 31 which upholds that: "Every person has the right to privacy, which includes the right not to have (a) their person, home or property searched; (b) their possessions seized; (c) information relating to

their family or private affairs unnecessarily required or revealed, or d) the privacy of their communications infringed." The Constitution also provides that any limitation of the right to privacy should be provided by law, and only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom.[5] It is thus not enough for the limitations to be provided in legislation, but they are also obligated to prove that such limitation meets this constitutional threshold.

The Kenya Information and Communication Act (1998) (KICA) protects communication and information privacy rights under Section 31. This section makes it an offense to intercept a message sent through licensed telecommunications service and to disclose its contents. It is punishable by three years' imprisonment or a fine of up to Ksh3,000, or both. Under Section 83W unauthorized access to any computer system for the purpose of obtaining, directly or indirectly, any computer service; or interception or causing to be intercepted, directly or indirectly, any function of, or any data within a computer system, is an offense.

Moreover, KICA was modified by the Kenya Information and Communication (Consumer Protection) Regulations 2010, which restricts licensed telecommunication services from monitoring, disclosing or allowing any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems. The regulations specifically bar the licensees from listening, tapping, storing, or other kinds of interception or surveillance of communications and related data.[6] KICA also empowers the Communication Authority of Kenya (CA) to prosecute all offenses under the Act (section 104).

The Computer Misuse and Cybercrime Act, 2018 in section 14 (1) imposes liability of up to three years imprisonment and/or a fine of up to Ksh 5 million for a person who intentionally accesses or enables accessing of any computer system without authorization. The Act further imposes the penalty of five years imprisonment and/or a fine of Kshs. 10 million for the acts of unauthorized access for the purposes of committing a crime (section 15); unauthorized interference of a computer system or data (section 16); and unauthorized interception of a computer system whether directly or indirectly (section 17). In addition, the bill prohibits phishing, where it makes it a punishable act to create or operate a website or send a message through a computer system with the intention to induce the user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system (Section 30).]

In July 2018, the Senate published a Data Protection Bill 2018 for public consultation. This is a renewed opportunity for Kenya to adopt a comprehensive data protection framework which will regulate the processing of personal data following a first bill proposed in 2015.

5 Article 24, Constitution of Kenya 2010
6 Section 15, Constitution of Kenya 2010

However, the new bill proposed has a number of significant shortcomings which must be addressed to ensure that the law would provide for the effective protection of privacy and would comply with international data protection standards and principles and protect the rights of individuals. Some of the areas of concerns highlighted include: poor definitions for data controller, data subject, exempt information as well as special personal information; unclear material and territorial scope of the law; some data protection principles missing, as well as rights of data subjects, broad exemptions; the lack of clarity on the powers, resources of the proposed independent supervisory authority.[7]

Judicial pronouncements on the right to privacy and lawful surveillance in Kenya

The constitution guarantees protection of private communications in Kenya. As such lawful surveillance must meet minimum standards provided in law -- necessary in a democratic society to achieve a legitimate aim. It requires that individuals are protected against arbitrary interference with their right to communicate privately. When a government wishes to conduct communications surveillance, it must only be done in accordance with the law.11 The court has made ruling on several matters affirming the right to privacy in CORD v Attorney General (supra) it was held that surveillance and intercepting of communication interferes with the right to privacy, adding that "…surveillance in terms of intercepting communication impacts upon the privacy of a person by leaving the individual open to the threat of constant exposure. This infringes on the privacy of the person by allowing others to intrude on his or her personal space and exposing his private zone."

The state has also considered that measures that may infringe on privacy require public participation and should further be allowed only when there are no less restrictive means to achieve the intended result. In two related petitions, the constitutional court considered the lawfulness of the decision of the CAK to monitor the population by installing a communication surveillance system, dubbed Device Management System (DMS) on mobile phone networks. In Kenya Human Rights Commission v CAK, the court found that the DMS did not meet the constitutional test in article 24 requiring limitations of the right to privacy to be proportional and lawful. It held that it lacked proportionality as there were less restrictive means available to achieve the intended purpose of combating use of illegal devices through the work of the police, the Kenya Revenue Authority, and the Kenya Bureau of standards, which are legally mandated to prevent the importation and use of counterfeit and illegal devices. It further found that DMS was unlawful since the mandate of combating illegal devices does not fall within the statutory mandate of CAK.12 In Okiya Omtata v CAK and 8 others,13 the court found that the introduction of DMS failed to meet the public participation requirements, holding that "the public whose data is held…and whose constitutional right to privacy is at risk in the event of breach must

7 https://privacyinternational.org/advocacy-briefing/2187/time-has-finally-come-kenya-seizing-opportunity-protect-individuals-and

as of necessity be involved in the engagements. Thus, the process must be subjected to adequate public participation wide enough to cover a reasonably high percentage of the affected population in the country."

***62 per cent** of Kenyans are concerned about their online privacy*

According to a CIGI & IPSOS 2014 survey, 62 percent of Kenyans are concerned about their online privacy14. The survey also showed that 96 percent are concerned about criminal hacking into their personal bank account; 93 percent are concerned about their online accounts being hacked and infringement of personal information; 88 percent are concerned about monitoring and commercialization of their online activities by private companies. Moreover, 73 percent of Kenyans are concerned about internet censorship by the government; 62 percent about secret monitoring of their online activities by police or other government agencies. M-Pesa15 also raised concerns owing to the use and recording of personal data.

In 2012, the Communication Commission of Kenya made public its intentions to address cybersecurity threats by setting up NEWS, an initiative of the International Telecommunication Union (ITU) that allows authorities to monitor incoming and outgoing digital communication.16 In 2013, it was alleged that Kenya had a Blue Coat Packet shaper installation. Blue Coat allows the surveillance and monitoring of users' interactions on various applications such as Facebook, Twitter, Google Mail, and Skype17. As with the NEWS initiative, there was an uproar from the media, CSOs and the general public citing the possible violations of the right to privacy.

In 2014, Safaricom was awarded a tender to develop an Integrated Public Safety communication and Surveillance system Kenya police. The project would result in the installation of 1,800 CCTV cameras with face and motor vehicle number plate recognition capabilities in strategic locations in Mombasa and Nairobi; setting up a command and control centre where footage from the CCTV cameras and handheld devices will be relayed in real time; a video conferencing system; connecting 195 police stations with high-speed internet; the development of a 4G LTE18 network for the police with 80 base stations; supplying the police with 7,600 radio communication devices with SIM cards and photo and video capability; and linking 600 police vehicles to the command and control centre.18The main goal of the project is to enable security agents to communicate better

and boost their capacity to fight terrorism.19 There was, however, a public outcry over the possibility of personal data being shared with third parties including foreign actors, the processing and collection of communications and images without the consent of individuals, the risks of insecure storage facilities and unauthorized external access and the potential for data to be deleted or modified.

There have also been concerns over unlawful surveillance of journalists and Human Rights Defenders (HRDs) by the Kenyan government, especially those working on issues of impunity in post-electoral violence and extrajudicial executions; counter-terrorism; accountability, social auditing; sexual and reproductive rights; and land rights.22 Vocal Civil Society Organisations such as the Muslim for Human Rights (MUHURI) have raised concern over surveillance of their movements and work, 23as part of an ongoing trend of intimidating and attacking HRDs.24 It has also been alleged that the government has intercepted the communications of civil society organizations like MUHURI and Haki Africa25, who were then listed as designated entities, and later deregistered by the Non-governmental Organisations Coordination Board along with 508 other NGOs, 15 of whom were accused of being a 'conduit of terrorism'.26 In what may be considered official targeting of civil society, the NGO Board was shifted from the Ministry of Devolution and Planning to the Ministry of Interior and Coordination of National Government. Moving regulation of civil society actors to the security docket is seen as intended to allow an increase surveillance of these human rights defenders since such violations of privacy can be justified by claiming necessity for security purposes.[8]

In their 2017 report, *Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya,* Privacy International in partnership with National Coalition of Human Rights Defenders-Kenya detailed the techniques, tools and culture of Kenyan police and intelligence agencies' communications surveillance practices. The report focuses primarily on the use of surveillance for counterterrorism operations. It highlighted how communications content and data is intercepted and fed into the cycle of arrests, torture and forced disappearances. These include through cooperation with telecommunication companies where they illegally give privileged client information to intelligence and law enforcement agencies. It also alleges that the NIS has direct access to networks, allowing them to intercept communication without the knowledge of the telecommunication

[8] Protection International 2017: 17

companies.[9]

However, in Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya, the court ruled that given the nature of terrorism and the manner and sophistication of modern communication, interception of communication and searches were justified and there seemed no alternative, less intrusive means of achieving the intended security purpose.

IIn addition, the court expressed its confidence in the safeguards enacted to prevent the arbitrary violation of the right to privacy.30 This position reflects current public perception with 70 percent of the 24,143 respondents in a 2016 survey done in Kenya supporting government intrusion into online communication and with 85 percent supporting this when the person is suspected of a crime.31

Section 69 of the Security laws (amendment) Act 2014 amends the Prevention of Terrorism Act 2012 to allow for interception of communication by national security bodies for the purposes of detecting, deterring, and disrupting terrorism. In accordance with Section 36 of the Prevention of Terrorism Act, such interception requires authorization from the High Court. The National Intelligence Service (NIS) Act allows for the interference with the right to privacy to the extent that the NIS is permitted to investigate, monitor, or otherwise interfere with persons who are under investigation by the service or suspected to have committed an offence subject to authority granted by the Director-General of NIS.32 This potentially enables unchecked violation of privacy for any person where such a person may be accused of committing such offense as provided in the NIS Act. Further, security agencies may escape the constitutional requirement to prove that the limitation was justifiable and necessary by explaining that this information was classified for security purposes.

Purpose and Objectives of the survey

This survey set out to:

- Assess HRDs' level of exposure, understanding and perception of communication surveillance;
- Document HRDs' current strategies for mitigating, perceived or actual communication surveillance.

The survey was guided by the following broad research questions:

1. What are the main norms and legal frameworks being used to govern the right to privacy?
2. What are the emerging patterns of how State (i.e. county or national government

[9] Privacy International (2017) 'Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya', Privacy International.

officials, police, justice system operators) use these laws and how do they affect HRDs and their work?

3. What is the level of HRDs' exposure, understanding and perception of communication surveillance?
4. What strategies do HRD's use for mitigating communication surveillance?

METHODOLOGY

This study utilised a mixed methodology, combining qualitative and quantitative approaches. A total of 49 respondents from 15 counties were reached. The quantitative component of the survey targeted 30 HRD respondents while an additional 19 were interviewed as key informants.

Respondents were chosen using purposive sampling and snowballing to identify the different players in the field given the interconnectedness of HRDs. Using this, consultants generated a list of survey respondents and key informants who comprised of HRDs and people who are closely associated with their work including human rights lawyers, judiciary officials, government officials, CSOs, CBOs and NGOs, Commissioners of the KNCHR, representatives of private sector companies and individual human rights defenders in the rural areas.

Desktop research involved reviewing relevant published and unpublished reports in relation to safety, security and protection of HRDs in Kenya by State and non-State actors. Past publications on the subject, the grounding basis on protection through international codes of HRD practices and court rulings, the Constitution of Kenya, special UN resolutions, human rights codes and charters, among others., were also explored to inform this report.

Anonymity, Security and Privacy

Given the nature of this work, anonymity of the respondents was paramount. Any specific identifiers that may point to the respondents was avoided during data collection. This also applied in during qualitative interviews. Researchers built trust with the respondents before conducting the interviews. Interviews were also conducted in places where HRDs were comfortable.

Respondents profiles

This research targeted a total of 49 respondents from 15 counties working as HRDs[10]. The respondents self-identified themselves as HRDs and work either individually, through networks or organisations to defend and promote human rights. The survey part of the research comprised of 30 respondents with diverse profiles. These included age, level of education and gender. Respondents were also asked whether they are affiliated to any organisation and the specific human rights issues they are engaged with in their work.

From the survey, most of the HRDs, 80per cent, self- identified as male, 17per cent were female and 3per cent preferred not to say their gender. Respondents were distributed across different ages. 30per cent were aged between 18-30 years, 33per cent between 31-40, and 30per cent between 41-50, while only 7per cent were aged 51 and above. In terms of work experience, 43per cent had 11 years and above while 37per cent had 6-10 years, and 20per cent had an experience of between one and five years.

[10] In this research "Human rights defender" refers to people who work to promote or protect human rights. They may be working individually, within an organisation or a collective setting. HRDs targeted in this interview address human rights concerns ranging from, governance (citizen's right to participation, decision making, transparency and accountability), extra-judicial killings, LGBTQI rights, torture, arbitrary arrest and detention, female genital mutilation, discrimination, employment issues, forced evictions, access to health care, extraction, waste management and its impact on the environment, counter-trafficking, child labour among others.

Forty per cent (40per cent) had a university degree, 33per cent a master's degree and above, 20per cent had a college certificate or diploma and 7per cent high school certificate. Of all the respondents, 77per cent were affiliated with an organisation while 33per cent were independent.

Type of HRD Work

HRDs are involved in different types of work advocating various human rights issues. In the course of their work as seen later in the survey, they are exposed to communication surveillance in various degrees and through various means.

From the survey data, 90per cent of the respondents were engaged in general human rights work especially that touching on holding government and leadership to account. This includes monitoring how bodies such as the police, the army and intelligence services use their power. Human rights defenders are involved in questioning extra-judicial killings, torture and security.

It also involves how government systems discharge their mandate and authority specifically the Executive, Legislature and Judiciary and touches on both national and county levels of governance. Governance issues include protection of public resources, rights of people in terms of access to resources, protection of individual rights such as ownership of property and due processes in governance.

Gender and women rights followed with 40per cent. These HRDS handle matters related to equality and equity, access to resources by women, rights and proportional representation as established in the Constitution, right to property ownership, advocating against gendered violence and exploitation, gendered labour/work related issues, health dimensions, and advocating beyond heteronormativity for the LGBTQI community.

Third, was countering violent extremism with 37per cent. HRDs work on issues of grave human rights violations related to extra judicial killings, forced disappearances and prosecution.

From the survey findings, 20per cent of the respondents are engaged in extractive and labour rights sectors. The question of extractives has become central especially with the discovery of uranium in Kwale, salt in Malindi, oil in Turkana and coal in Kitui. Access and extraction of these minerals has raised concerns about ownership (between the local population, county and national government and investors), access to opportunities related to extraction, environmental effects of extractions and distribution of resources. HRDs are also involved in labour rights issues that spread across various grievances from fair compensation, working conditions, exploitation and child labour.

Ten per cent reported working in counter-trafficking, while refugees/migration were identified by seven per cent. Kenya is a major conduit and market for human trafficking for labour and exploitation. Those exploited include children who are smuggled in from neighbouring countries to work here and for export markets, especially the Middle East. Kenya is also home to refugees in various camps mainly from Somalia, South Sudan, Ethiopia, Eritrea and DR Congo.

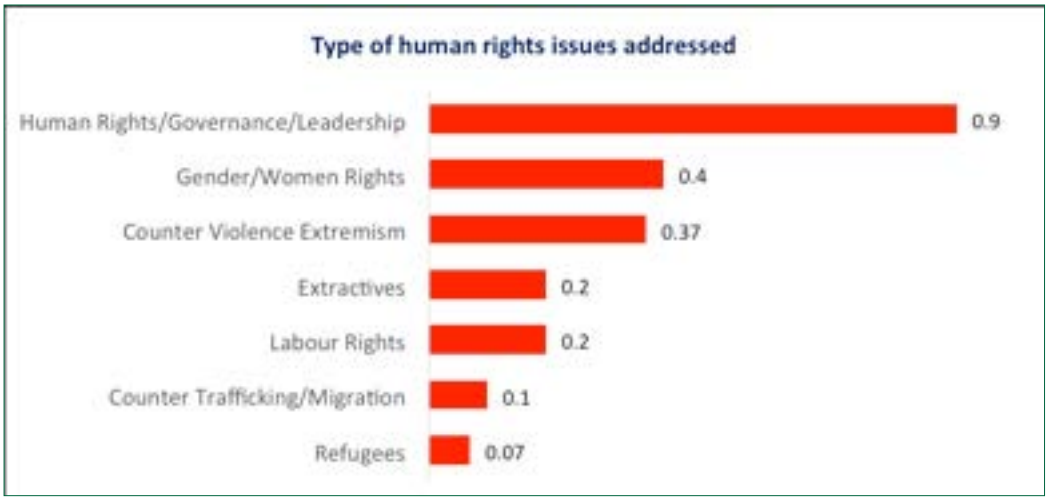


Figure 1: Type of human rights issues addressed

The type of work that HRDs do exposes them to risks and threats of communication surveillance at different levels. As noted by a key informant working to protect HRDs in danger, experience shows there is no perceived blanket surveillance of HRDs, but there are reports of individuals being targeted depending on the nature of their work. However, HRDs have different capacities to handle threats both at individual and organisational levels. For example, HRDs who have worked in a specific area for a long time know their adversaries. Some will be warned or even threatened verbally.

From interviews with HRDs, perceived sources of threats come in different ways. One is directly through instruments of force such as police or hiring other people to attack HRDs or direct threats from powerful people. Secondly, it can be done through coercion and intimidation by influential individuals. Third, is through proxies where HRDs are targeted through their own network, for example, using a fellow HRD to convince another to drop a court case or such messages passed through family members or close friends.

FINDINGS AND ANALYSIS

This section presents the findings of this survey from the range of issues that were covered. We present HRDs knowledge on communication surveillance related issues then examine their attitudes towards it and the actual practice and behaviour. This multi-level approach is important because it helps to isolate individuals and issues as well as examine HRDs daily work engagement with communication surveillance.

Understanding of Key Concepts Related to Communication Surveillance

This section explores HRDs understanding of key concepts on communication surveillance and privacy from both qualitative and quantitative angles. This understanding is important especially for organisations working with HRDs to build their expertise and knowledge of communication surveillance policies and practice. This is to raise awareness of the potential threats they may be facing and experiencing. Knowledge of these key concepts determines the HRDs awareness level of the possible risks that their communication may involve. Knowledge may lead the HRDs to act in a certain way because they are aware of the relationships between their actions and outcomes.

Communication Surveillance

Respondents were asked to identify one concept that comes to mind when they hear about the term Communication Surveillance. The most common terms identified were monitoring, intelligence, tracking, tapping, spying, police, hacking, and privacy. Other terms such as snooping, observing, extraction (of information) were also identified. This is represented in the infographic below:

Figure 2: communication surveillance

These terminologies point to a good degree of awareness of communication surveillance

by the HRDs.[11]/[12]

A number of HRDs said they believed their phone calls were being monitored. "I know my phone is tapped. I feel another call coming in when am talking but there is no missed call. Other times I feel the sound of 'tap, tap' when am talking," said a HRD based in the Coast region. Another one in the same region noted, "I know my phone is tapped when I hear an echo or delay in the receiving or response of calls from the other end. It means someone is listening in." Whilst these are legitimate concerns and perceptions, they do not constitute evidence of communication surveillance. Communication surveillance more often than not goes undetected.

Communication Privacy

Respondents were asked to identify one concept that comes to mind when they hear about the term Communication Privacy. The most common term identified was confidential. Others included secure, freedom, secrecy, private, clandestine, passwords, protection, intrusion, free, transmission, codes, trustworthy and intrusion-free. These are shown in the infographic below:

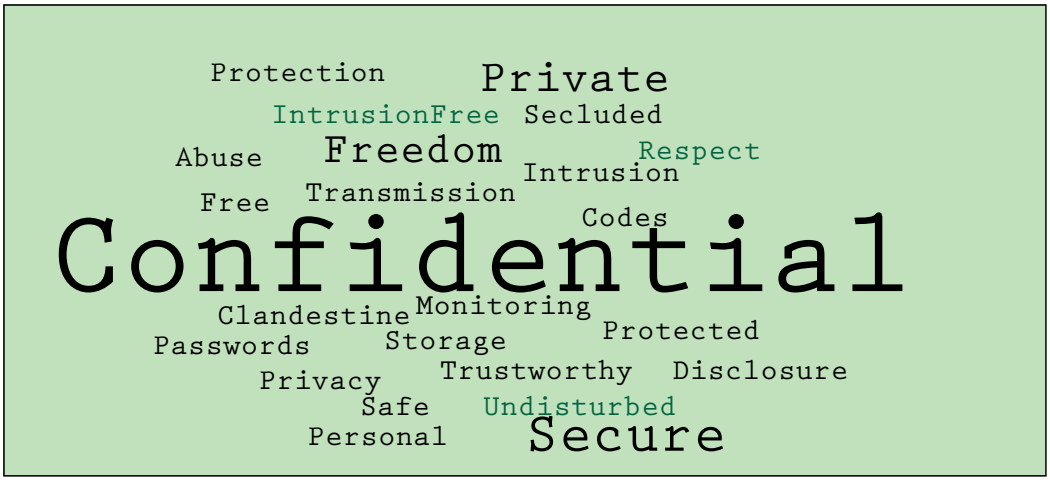


Figure 3: Communication privacy

Communication and information privacy relates to protection of information held by individuals and considered private for example e-mails and phone calls.[13] Terms such as freedom and respect allude to the fact that HRDs have the right to work without other parties intruding in their information. Other terminologies – codes, passwords, safe — point to attributes of information privacy.

[11] Communications surveillance," https://www.privacyinternational.org/explainer/1309/communications-surveillance

[12] UN General Assembly, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," 17 April 2013 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[13] Katz v United States 386 U.S. 954 (1967).

Communication Security

When respondents were asked to identify one concept that comes to mind when they hear about the term Communication Security, a number of terminologies were mentioned. The most common included protection, encryption, privacy, secure and safety. Others were coding, communication, safekeeping, digital security, communication integrity, confidence and deterrent. These are shown in the infographic in Figure 5.

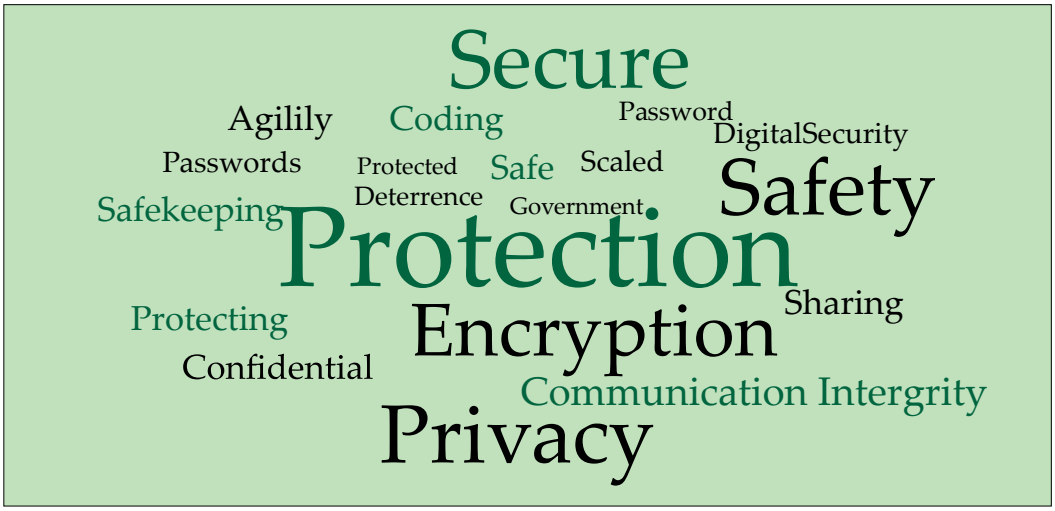


Figure 4: Communication security

Whilst the responses do not imply that respondents have a clear understanding of what these terms mean, they indicate that HRDs correctly associate some key terms with security and communications surveillance.

Awareness of Communication Surveillance

This section examines awareness of communication surveillance. Respondents were asked a series of questions to assess measures they perceive individuals can take to protect themselves from surveillance and ensure privacy of their communication and data. We also sought to gauge awareness on sources of communication surveillance. It can be argued that having an increased understanding of HRDs' level of awareness of communication surveillance can help understand how they go about their work, their self-assessed degree of risk exposure to communication related risks and the level of security. In a scale ranging from very low to very high, the findings are summarised below:

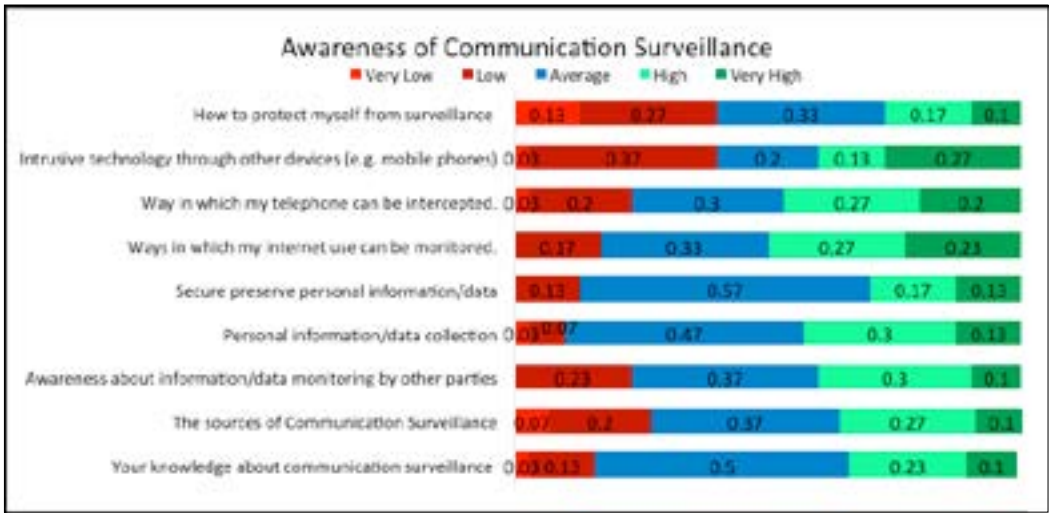


Figure 5: Awareness of communication surveillance

Responses indicate that HRDs perceived themselves as being most knowledgeable in terms of how to secure information (over 57 percent) and the ways that the Internet could be monitored, with 50 percent rating their own knowledge of communication surveillance above average. During qualitative interviews, HRDs reported that they had undergone some form of digital security training both within their organisations and those organised by other players such as National Coalition for Human Rights Defenders (NCHRD), Protection International, Amnesty International and Kenya National Commission on Human Rights (KNCHR). Others, through years of experience and interaction with various players, noted that they had become (more) aware of communication surveillance. However, the information provided by respondents seemed to indicate that they felt they were least knowledgeable on how intrusive devices can be used in surveillance.

Attitudes towards Personal and Work Information

HRDs attitudes towards sharing and protecting personal information was examined through a number of factors. These include concerns over online surveillance, nature of different information sharing, privacy concerns, and sense of control over privacy as shown in Figure 7. Respondents were provided with a list of concerns and were asked to indicate whether those were or not of concern across a five-point scale: from strongly disagree to strongly agree.

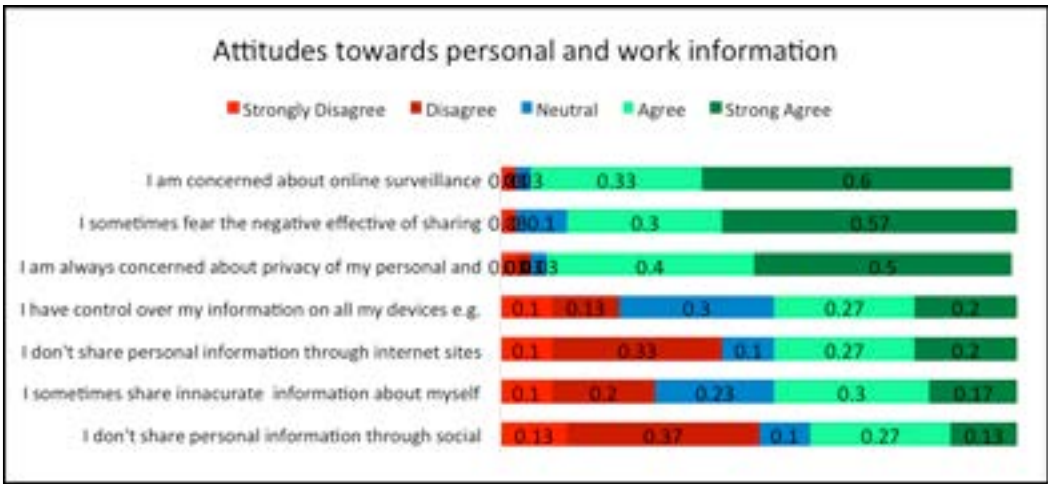


Figure 6: Attitudes towards personal and work information

The responses indicated that the majority of respondents were concerned about online surveillance and its negative effects in relation to personal and work information. Ninety-three (93) per cent, are very concerned about online surveillance while 87 percent fear the negative effects of sharing information online and the privacy of their personal information. Ninety (90) per cent are concerned about privacy of their information while about half of the respondents (47per cent) indicated they feel they have control of the information on their devices.

The gap between concerns about online surveillance and the actual practice of sharing information shows a difference between attitudes and actual practice. HRDs argue that due to various roles that they have to play—as professionals, community members and family members — it can be hard to implement practices that will help them protect their information. "These are people who know us by name and even where we live. They know our friends, families and even where our children go to school."

Sources of Surveillance

Respondents were asked about their perceived surveillance from different sources including intelligence agencies, police, internet service providers, employers, as well as family and friends. This ranged from very unlikely to highly likely. The responses indicate that HRDs perceive that the source of surveillance comes from different actors.

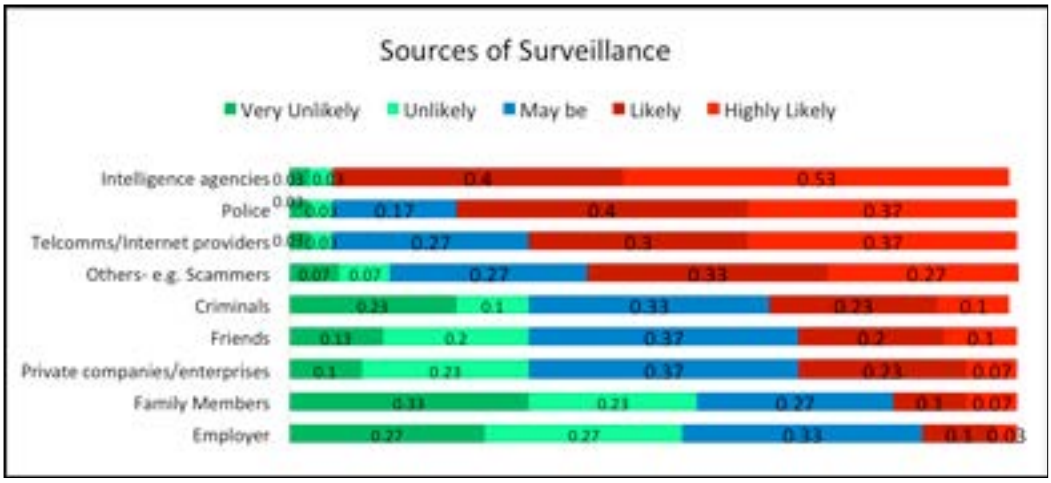


Figure 7: Sources of surveillance

Intelligence services were perceived as the most likely source of surveillance followed by police and telecommunications or internet service providers. These responses indicate that HRDs perceive State institutions as the biggest source of surveillance compared to the private sector. There are several factors why this could be but an exploration of this falls beyond the scope of this survey.

A HRD explains the role of police and security organs in surveillance and complex relationship with other players.

> The main actors involved are the police, intelligence, paramilitary formations and the army. They work with the Executive (civil servants) and politicians. These are the people who direct the police. The police just implement orders. There could also be some parastatals, some quasi-governmental such as Communication Authority of Kenya (CA). The devolved governments can also share information on HRDs with the national agencies because they have a relationship. For example, in the last election, I spoke to a governor who told me that "that the NIS had some intelligence that they had shared which showed he [the governor] would win the party primaries and this came to pass. It means he has access to the NIS and can thus can share information.

There are a number of reasons why intelligence and police are perceived as the main sources of surveillance. According to key informants, many HRDs' work touch on the State and, therefore, susceptible to its instruments. Secondly, many HRDs have a history with these agencies because they are the biggest culprits in curtailing civic space.

Thirdly, are claims that intelligence and police have been used by diverse players to intimidate and harass HRDs. One HRD reported that they felt that police track and tap their phones more so when they have public activities.

Other adversaries such as scammers, criminals, friends, private companies and family members were also identifiedSome HRDs fear they are being monitored by criminal gangs such as al-Shabaab. They suspect those working in Countering Violence Extremism are exposed to al-Shabaab recruiters. During the interviews, some of the HRDs said they had been called by al-Shabaab youths who had returned from Somalia. "Most of the times you have no idea how they got your number. This is a security threat to us that needs to be handled by the police. The government can easily pick you when this happens and you have to explain your relations with the returnees or al-Shabaab."

The role of telecommunication and internet service providers is also important because they are perceived as actors with access to a lot of information. There are reports that ISPs collaborate directly or indirectly with both intelligence and law enforcement agencies.

With increased utilisation of digital media and online interactions, leaving digital footprints has become common source of surveillance. A digital footprint is a trail of data that one creates while using the Internet. This may include the websites visited, emails sent and information submitted online.

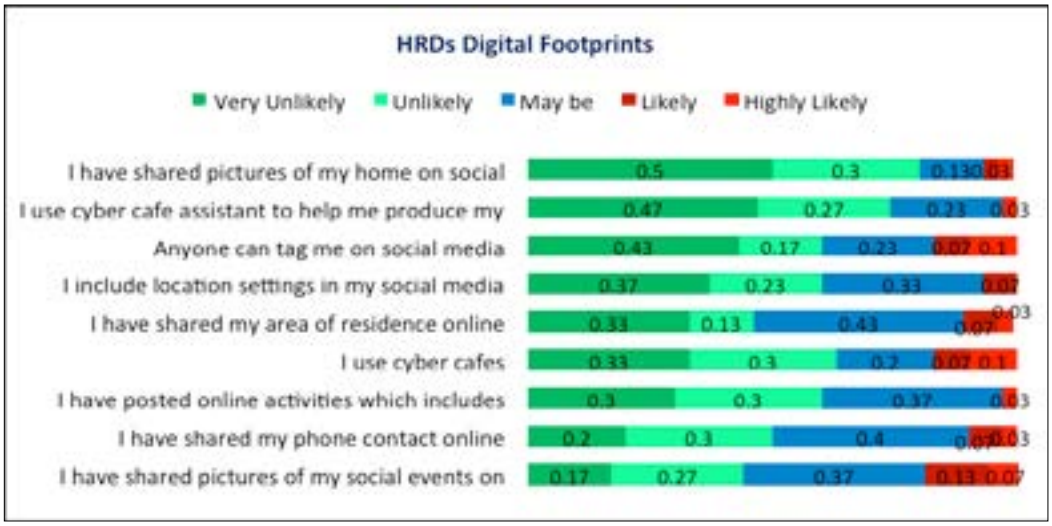


Figure 8: HRDs digital footprints

80 per cent of HRDs said they are unlikely to share pictures of their home on social media while 74 per cent are unlikely to use cyber café assistants. Many also do not share phone contacts online.

While these scores indicate that those who responded do not share certain types of information online, significant risks remain. Leaving digital footprints that exposes HRDs is not so much as a result of lack of information.

Other HRDs have related what they perceive to be safer sharing practices. For example, if one visits a location that they find exciting and want to share, they only post after they have left. It is perceived that such practices help reduce risk of being identified and located in real-time. HRDs must consider these risks when deciding when and what to share online.

Perceived Security of Communication Tools

There are many communication tools that are available for HRDs. Each tool comes with its own security concerns. The tools range from use of telephone (both mobile and landline), emails, social media including mobile based applications and even face-to-face communication. Respondents were asked to rate the communication tools based on perceived security and responded as shown in Figure 10 below.

Figure 9: Perceived security of communication tools

The respondents believe that face-to-face communication entails less risk followed by calling on landline. Sending text messages, using online messaging applications, calling on cell phone and posting on social media are perceived to carry lower risk and communications is less likely to be interfered with. While this is the way respondents perceive each means of communication, this does not necessarily reflect the actual security and safety of each mode of communication.

Face-to-face communication is perceived as less risky and more secure. This is largely because HRDs feel they have control on various communicative realities including the space and the person they are engaging. One is also aware of reactions and can use the various cues to make decisions of communication aspects. However, interviews with HRDs revealed high level of concern in interpersonal engagements especially when engaging in a network because not everyone can be trusted. There are cases where network members have been compromised. As noted by a HRD, "I do not think it is hard to get my number or even that of other HRDs. It only depends on how well connected the person is. You can easily get from any HRD network member."

Messaging apps have some additional security features such as end-to-end encryption, but HRDs are still concerned about how their information can be used. This relates more with the behaviour of other users they interact with on those platforms. For example, one HRD said he feared that anything that is on WhatsApp is likely to find its way to multiple destinations regardless of the author's intention, especially when someone takes screenshots and shares. Instances of leaked WhatsApp conversations are common. Also, WhatsApp groups were identified as raising risks because they involve different people whose motives are hard to establish and behaviour impossible to control. One respondent stated:

> On a Whatsapp platform, there was a guy who wanted information on CDF (Constituency Development Fund). Some strangers later went to his home and abducted him. They held him overnight in a cemetery. The abductors wanted to know who had supplied the information. So if you seek or share information on a media platform, don't front yourself as an individual to spread the risk.

These concerns are not limited to Whatsapp, they also apply to SMS and other forms of communication.

Another way of surveillance is monitoring of emails; who is the sender and what is the

subject as well as content. It is easy to draw the connections as pointed out by a HRD, "if I receive an unencrypted email from X I know I will be in the radar since that organisation is heavily monitored." Even if the message is encrypted, some information can be gathered including the name of the sender and the recipient, and their email addresses, the time the message was sent. This information is known as metadata.[14]

In one specific case, HRDs who were pushing for transparency in a communication project implemented in their county were targeted in various ways as one of them explained:

> …The question was who spent money. Within that week, my email was "hacked" [unlawfully accessed] twice from a Nairobi location. Before that I had been called by a close friend working with the company that had partnered with person X in the project. He said I was talking too much about the matter.

Whilst the language used widely refers to 'hacking' (as above), instances reported do not necessarily mean that the system was interfered using technical means targeting software and hardware. It could mean that the email was unlawfully accessed possibly due to poor password management of the individual.

Engagement on social media comes with its own risks due to the virtual nature of the platforms interactions. Online surveillance has become easier due to the nature of social media platforms, and yet the risk associated with their use is widely misunderstood as a result of the opaque nature of business practices of these platforms.

Companies regularly monitor content, such as messages or images posted, and other data, which is generated when someone uses a social networking site. This information involves person-to-person, person-to-group, group-to-group, and includes interactions that are private and public.[15] Moreover, HRDs face not only dangers associated with their posts but also risks of being exposed by friends and followers on Facebook, Twitter etc.

The survey indicates that HRDs have some level of awareness of a number of aspects of communication surveillance that may be used to undermine their work. The responses also indicate some awareness of behaviours that may put them at risk. Based on this initial part of the survey, information technology habits were also explored.

Measures taken by HRDs to protect their information

This section looked at some measures taken by HRDs which they perceive reduce the risks they face. A number of practices commonly used by individuals were reviewed with responses indicating whether HRDs used these measures from very rarely to always as shown in Figure 11.

Survey findings show that HRDs perceive that they take certain measures to protect their informational usage habits. 53 per cent responded that they always use passwords to lock personal phones. Other habits include customising privacy settings to limit access and

[14] https://privacyinternational.org/video/1621/video-what-metadata
[15] https://privacyinternational.org/explainer/55/social-media-intelligence

processing of their information, regular checks of information to be collected by use of different communication tools for work and for personal use.

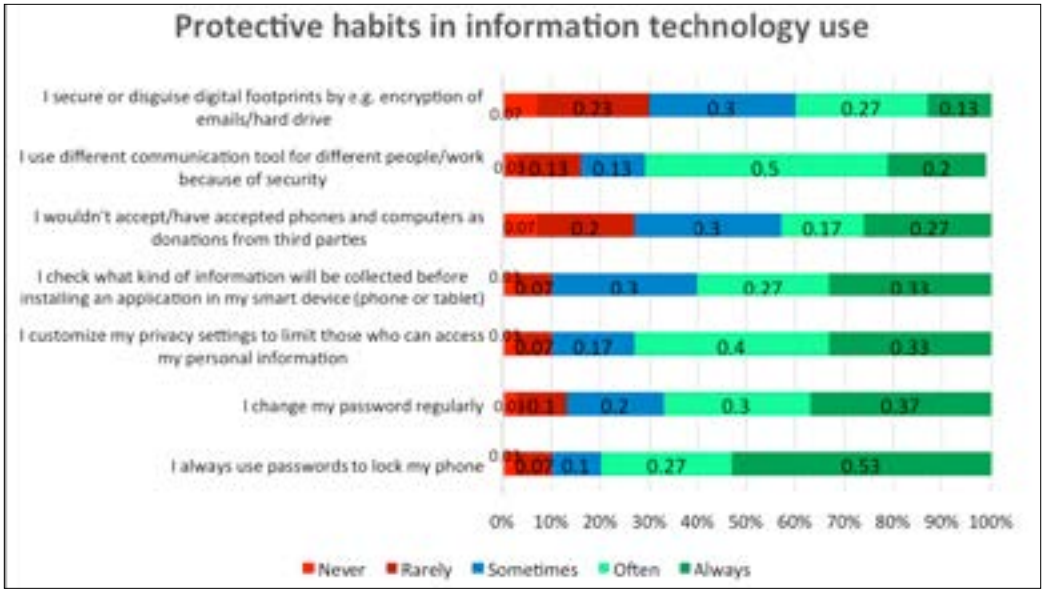


Figure 10: Protective habits in information technology use

> *"My phone is encrypted and has multiple passwords. Depending on whom I am talking to, I take precautions. This is because there are people who have been tracked using their phones and we were working with them," noted a HRD. Some also said their employers support them to have separate phones for personal and official communication hence no mixing the two levels of interaction.*

Online Security Behaviour

Related to protective habits above, respondents were asked on some practices including protecting private information, their perception of privacy, protecting browsing habits and changing behaviour when they sensed they are being monitored. Answers ranged from strongly disagreeing to strongly agreeing as shown in Figure 12.

These responses are consistent with general understanding by HRDs that their work attracts attention from various sources hence the need for them to adopt certain practices to minimise the risks. As articulated by a HRD, "We don't easily accept friends on Facebook or trust people. We don't expose a lot on social media and we don't compromise our security while travelling. We arrive home early—we are careful in our socializing."

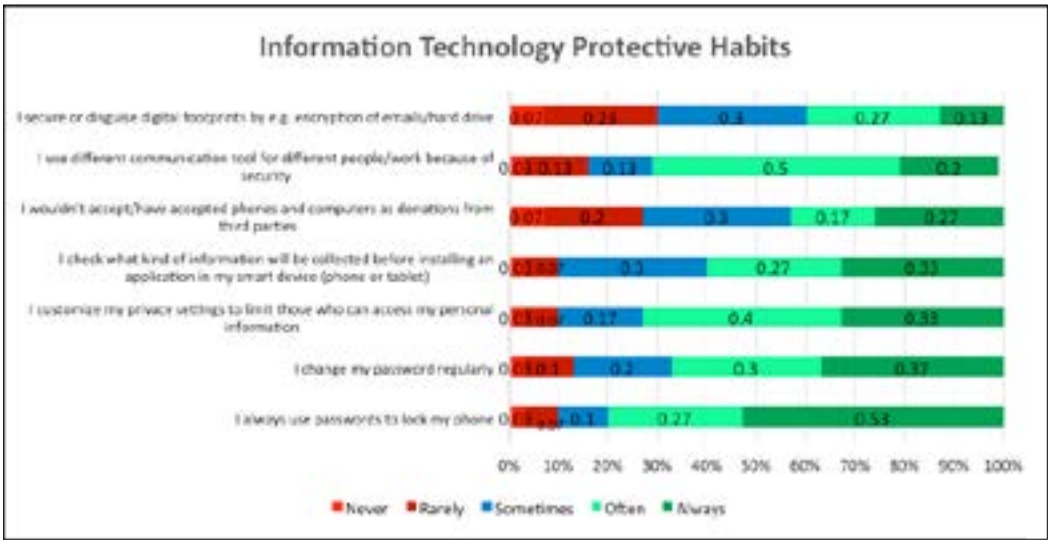


Figure 11: Online Technology protective habits

Specific online challenges were noted especially by LGBTQI HRDs or those that are sympathetic to LGBTQI causes. These include various practices in online groups that have collective HRDs as well as posting on social media.

> *We have different groups such as XXX [name of group withheld] where negative information about LGBTs is posted. They talk of gay and lesbians snatching their girlfriends and boyfriends. Names of people are outed.*

Working within a network rather than individually appears to be one of the strategies that some HRDs use. Another strategy is to use influential individuals.

> *For my own case, I am not out and people identify me as an LGBTQI activist. I also work with other artists as an artist. I use that kind of a platform. If I meet three artist friends, I make sure during their event, we bring them into our [acting] cast. If I am posting something on LGBTQI issue, I tag influential heterosexuals having shared with them my intention beforehand.*

For LGBTQ HRDs, creating a sense of togetherness with influential persons helps to deflect possible backlash and targeting.

Online Protection Measures

Respondents were asked on various measures they take which they perceive to minimise the risks they face in the course of their work and the extent to which they practice them. The degree of care in sharing on social media, protection of digital devices, limiting information on public platform, geotagging, among others. These are shown in Figure 13.

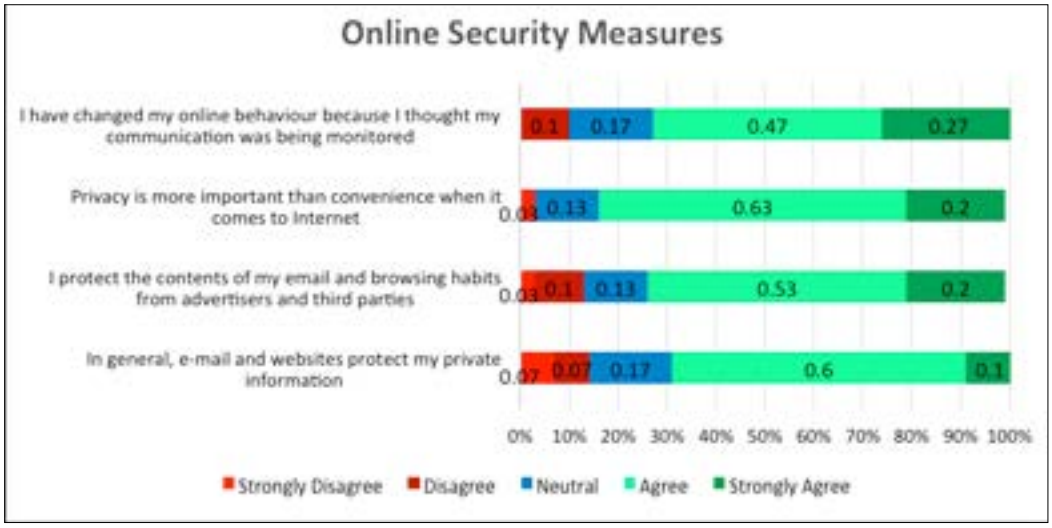


Figure 12: Online protection measures

Scores of perceived online protection behaviour are high. Twenty-seven per cent of HRDs strongly agreed to changing their online behaviour when they thought they were being monitored while 47per cent agreed. Only 10per cent strongly disagreed while 17per cent were neutral. The data shows that HRDs largely value privacy more than convenience in internet use. Seventy per cent of the HRDs agree that it is better to be inconvenienced rather than lose their privacy online. A significant number (73per cent) reported they have taken measures they perceive protect their email and browsing habits from advertisers and third parties with 60per cent agreeing and 10per cent strongly agreeing.

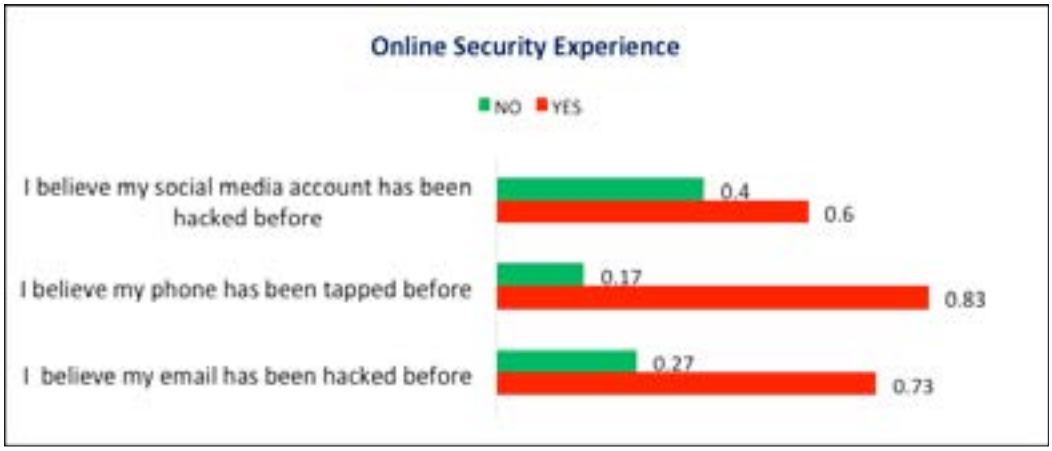
The findings indicate that there is some degree of awareness of the risks of surveillance HRDs may experience. During qualitative interviews, many reported that they have undergone some form of digital security training. These trainings are conducted by organisations like NCHRD-K, Protection International, Amnesty International, Kenya Human Rights Commission, and Frontline Defenders. Some of the trainings have centred on risks and threats of communication surveillance. However, majority of the trainings have been on general safety and security of HRDs. Risks and threats of communication surveillance is usually a small part of the training.

For LGBTQ activists, certain measures are useful to avoid backlash online. One is to communicate on behalf of a group rather than in their individual capacity. That way, it is harder to have attacks directed to a specific individual but rather the group becomes the target which is easier to deal with.

Online Experiences

Respondents were asked about their experience with breach of security through unlawful access to their social media accounts and emails as well as phone tapping. As earlier noted, whilst the language used widely refers to 'hacking,' it does not necessarily mean that the system was interfered using technical means.

Figure 13: Online security experience



Sixty per cent per cent believe that their social media account has been unlawfully accessed before, 83per cent believe that their phone has been tapped before and 73per cent believe that their email accounts had been unlawfully accessed before. In qualitative interviews, the same sentiments were reported with a huge majority believing that their conversations are always being listened to. One respondent said, "I feel another call coming in when am talking but there is no missed call. Other times I feel the sound of 'tap, tap' when am talking." Another said, "I know my phone is tapped when I hear an echo or delay in the receiving or response of calls from the other end. It means someone is listening in." Others reported that they knew their email accounts had been unlawfully accessed when security officers get information about their activities (for the NGO) even before they are formally released.

Interpersonal and Relational Dimensions of Communication Surveillance

Beyond the mediated aspects of communication surveillance, this survey also examined the interpersonal and physical dimensions of surveillance. Through the in-depth interviews, a number of issues critical to human rights defence work emerged.

First, HRDs work at two levels—the national and the county, largely as a result of devolution. For many HRDs, counties have created opportunities to concentrate on local issues (especially in matters of governance and security). However, with many HRDs working in a smaller space of engagement this has also meant that their activities are more likely to be visible, and so they face a higher risk of exposure and hence become targets of surveillance.

This proximity to the people they check has provided a new dynamic of increased use of traditional surveillance mechanisms. HRDs are experiencing infiltration where individuals call themselves HRDs but when offered certain opportunities, i.e. decision-making roles, they change their loyalty and forget they were HRDs. They are essentially spies who release the information they have gathered to other parties.

HRDs also share multiple platforms on social media, such as WhatsApp and Facebook

groups. To some, especially LGBTIQ community, these groups are used to collect information and also to repress them. Some LGBTIQ HRDs interviewed expressed difficulties working within the human rights circles because even fellow HRDs do not easily accept them. In the forums, some have made oppressive comments while others have shared information — such as one's sexuality even when the targets haven't publicly declared their status.

HRDs also see a close nexus between their work and media. Because HRDs use media for advocacy work, they have over time developed close working relationship with journalists. But some journalists have joined county governments as communication officers. Through their past engagements, they are able to access the HRDs and use previous connections to their advantage. Thus, the surveillance risks are not limited just to mediated communication. Rather, they are multidimensional and in the process, creating multiple challenges.

Organisational Dimensions of Communication Surveillance

While a huge chunk of this survey examined the individual HRDs, many of them work in organisational or network contexts. The work of HRDs is interrelated as they tend to draw strength in numbers.

This study shows that organisations are largely equipped on issues of preparedness, individual HRD safety, responding and rescuing and attendance policies and protocols. However, they are inadequate when it comes to risks and threats of digital surveillance, communication surveillance or online monitoring. They lack policies to guide them on how to understand the risks they face and how to mitigate those risks and protect their information.

Organisations have sent their members for trainings, but implementation of the knowledge acquired is poor because most of those trained do not feel they are at a level to mitigate the risks they face. Some said the language used during training is technical and this hinders their ability to understand and internalise safety concepts. In addition, they said most trainings focus on too many topics. They recommended that trainers should choose one or two things to focus on e.g. only, mobile phone security or email encryption so that the HRDs can build up their knowledge slowly but in an in-depth manner.

A few organisations reported that they had received in house training on tackling communication surveillance and online monitoring risks as well as how to protect their information. This approach is seen as extremely helpful because it brings a large number of people together and also allows for building capacity that is tailored to the specific organisations. This means participants and their organisations may be more responsive to implement what they learn in the training. Beyond policies and soft skills, there is not enough investment in terms of physical resources needed to secure information. A few organisations reported that they had made some investments in resources that can help to protect themselves from unlawful physical intrusion.

Some have installed alarm systems, CCTV cameras and back up data regularly to ensure that if there are any incidences of theft it is not all lost. At least three members of a network in Western Kenya and one organisation in Mombasa have been attacked in the recent

past. As narrated by an HRD, "The offices of one community organisation have been broken into many times, computers and hard disks stolen but I do not think they had cloud back up."[16]

[16] If using "cloud" backup services, it is imperative that there is encryption at all points – at rest in the office, on the wire to the "cloud" - at rest on the "cloud" (preferably encrypted before uploading)

CONCLUSION

This report has presented findings on the HRDs working in different parts of Kenya on their perceived level of exposure, understanding and perception of communication surveillance and online monitoring. It has provided an increased understanding of the strategies that HRDs perceive mitigate risks of communication surveillance and social media monitoring.

This was guided by a number of broad research questions on the norms and legal frameworks being used to govern the right to privacy; the emerging patterns of how weak and/or absent regulatory frameworks are used by the government to undertake surveillance, and how these policies and practices affect HRDs and their work. Others were the level of HRDs' perceived exposure, understanding and perception of communication surveillance; and the strategies used by HRDs to mitigate risks and threats of the surveillance.

While HRDs assessed showed an overall high level of awareness of communication surveillance issues at personal and organisational levels, the survey also reveals gaps between knowledge and practice. As such, even if some HRDs reported having a high knowledge on communication issues this does not necessarily translate to adoption of good practices.

HRDs are aware of the various sources of surveillance especially from the intelligence services, police and telecommunications and internet service providers.

While HRDs report taking certain measures to mitigate risk, these are not always technically correct and also the power wielded by some of these bodies as supported by the State apparatus or monopolistic companies is hard to challenge. Whilst it is becoming increasingly difficult to challenge such actors, there is need to urgently support the HRD community to better understand the risks and threats they face in order to put in place sound mitigation measures.

HRDs have started to adopt various measures they perceive mitigate some of the risks to their privacy and security of communications and information. These include use of passwords to lock personal devices and customising privacy settings to limit access and sharing of their information. Those who have been exposed to training on information protection appear to be more empowered. Given the sensitivity of information and changing realities of information technologies, continued capacity building for individual HRDs can be helpful but at the same time there is need to challenge the policies and practices of the government as well as those of the private sector.

At interpersonal, relational and physical dimensions of communication surveillance, the work at both national and county level suggest that specific efforts that take into account realities and nuances of these contexts must be considered in looking at protection.

HRDs are increasingly working within networks that bring a number of advantages in their work. But such collectives also present various risks including leaking of sensitive information by infiltrators who expose HRDs, especially those working with minorities. This demands

examination of communication surveillance and online monitoring risks from a different dimension, the individual but also the collective.

Finally, the fact that many HRDs work in institutional or network settings makes their communication and information issues intertwined, which raises new challenges and risks which must be addressed. Organisations have gaps on the issue of internal policies and sustained practices to mitigate risks and threats of surveillance. Knowledge levels need to be improved across the community and within each organisation. Organisations also need to invest in resources that improve information security.

RECOMMENDATIONS

A number of recommendations are made from this research, which can help to improve and ensure sufficient safeguards whenever there is collection and processing personal information for whatever legitimate reasons and ultimately, the work of HRDs in advocating a just society.

For Government:

- Fast track and ensure an open, inclusive process for the development and enactment of the proposed Data Protection Bill that conforms with the Constitution of Kenya, 2010 and international standards and best practices on protection of privacy.
- Ensure that the Computer Misuse and Cybercrimes Act, 2018 is reviewed to conform with with the Constitution and international standards of protecting freedom of expression, privacy and fair administrative actions
- Review existing policies and laws and enact further legislation as may be necessary to provide an environment for defenders to conduct their work freely and safely in a safe and enabling environment without communication surveillance.
- Prevent unlawful surveillance of human rights defenders, and investigate and prosecute all hold to account perpetrators of reported cases of unlawful surveillance.
- Take necessary measures to reform surveillance policies and practices to ensure they comply with Kenya's national and international human rights obligations and ensure that any information collection and processing adheres to Fair Information Practices.
- Call for accountability and transparency of law enforcement, and security agencies and private bodies undertaking surveillance, collect and process personal information.
- Introduce safeguards to ensure that everyone's rights and data are protected, in particular mobile telephony subscribers.

For The Private Sector:

- To ensure meaningful access, opt-out, and other rights, there must be a way to provide people with notice about all of the companies collecting their information;
- Be transparent about their business models as well as what and how personal data obtained is processed as a result of the use of their services;
- Make public the measures they take to respond to government requests for personal data belonging their clients, for example, through regular publication of detailed transparency reports.

For the Kenya National Commission on National Human Rights:

- Call for appointment of an independent authority to investigate communications monitoring and surveillance programmes conducted by the Kenyan government and ensure that these practices respect Kenya the government's national and international obligations to protect the privacy of its citizens and their personal data.
- Investigate all reported cases of unlawful surveillance of human rights defenders and ensure redress mechanisms are available should these lead to identification of violations of the right to privacy.
- Advocate for the adoption of safeguards to ensure that State surveillance of online and offline activities is lawful and does not infringe on HRDs' right to freedom of expression and ability to do their work, defend human rights, including through use of the information communication technologies.

For National, Local, and International CSOs and HRDs:

- Advocate for enactment of the Data Protection bill that conforms to with the Constitution and international privacy standards of protecting privacy.
- Advocate for the review of the Computer Misuse and Cybercrimes Act, 2018 to conform with the Constitution and international standards of protecting freedom of expression and fair administrative actions.
- Advocate to ensure that the policies and practices of the private sector, including telecommunications companies conform to international human rights and meet the standards as stipulated by the Ruggie principles.
- Build the capacity of their staff and networks to identify and assess threats and risks, and to identify and implement relevant and effective mitigation strategies.
- Assist grassroots HRDs to establish direct networks including with donors to ensure they access necessary resources, i.e. funding and other opportunities to secure their digital rights and work.
- HRDs establish Communities of Practice to hold each other accountable, exchange ideas and best practices to reduce threats of surveillance.
- Create and strengthen county-based networks which can support HRDs to understand and respond to information security challenges.
- Make communication surveillance and information security on top of the agenda as topics for constant discussion in HRDs' fora as they are at the core of their work.
- Organisations and networks reconsider common practices which serve to expose HRDs.
- Trainers should choose one or two things to focus on e.g. only, mobile phone security or email encryption so that the HRDs can build up their knowledge slowly but in an in-depth manner.

For Donors:

- To provide necessary resources, financial and technical, to support HRDs and CSOs to build secure systems, and develop plans that can improve implementation of secure communication policies and practices.
- Provide funding to rural- based CSOs to work on issues of privacy and surveillance.
- Support HRDs to network including at international level. This include supporting some HRDs to participation in regional and international forums such as sessions of African Commission for Human rights and UN Human Rights Council and other mechanisms like Special Rapporteurs.

For Policy Makers and Law Enforcers:

- Ensure open, inclusive legislative process when in view of adopting a Data Protection Bill must conform to with the Kenyan Constitution and Kenya's international human rights obligations, and in particular the right to privacy.
- Review and reform existing policies and laws and adopt new legislation that provide an environment for defenders to conduct their work freely and in a safely without communication surveillance.
- Investigate all reported cases of unlawful surveillance of human rights defenders.
- Demand reform of surveillance policies and practices to ensure they comply with Kenya's national and international human rights obligations.
- Call for accountability and transparency of law enforcement and security agencies undertaking surveillance activities.
- Call for accountability and transparency of the private sector policies and practices which interfere with the right to privacy of individuals and require the processing of personal data.

APPENDIXES

HUMAN RIGHTS DEFENDERS (HRDS) COMMUNICATION SURVEILLANCE SURVEY TOOL

Human Rights Defenders (HRDs) Commmunication Surveillance Survey

SECTION I: PERSONAL INFORMATION

	Respondent Identifier (e.g. 001, 0024 etc.)	
1.	Age Bracket	18-30 31-40 41-50 50 and above
2.	Gender	Female Male Non-binary/third gender Prefer not to say
3.	Highest Education Level	Secondary/High School College Certificate/Diploma First Degree Master's Degree and Above
4.	Years of Experience in HRD Work	1-5 6-10 11 and above
5.	Are you affiliated with an organization?	Yes No
6.	What types of [human rights-related] issues have you been working on? (Choose one)	Human Rights/Governance/Leadership Gender/Women Rights Counter Trafficking/Migration Extractives Private Enterprises related Labour Rights Refugees

KEY CONCEPTS	
7.	If you hear the term COMMUNICATION SURVEILLANCE, what TERMS come to your mind (Write two, single words only)
8.	If you hear the term COMMUNICATION PRIVACY, what TERMS come to your mind (Write two, single words only)
9.	If you hear the term COMMUNICATION SECURITY, what TERMS come to your mind (Write two, single words only)

AWARENESS OF COMMUNICATION SURVEILLANCE

10.	Rate your knowledge in relation to the following aspects	Very Low	Low	Average	High	Very High
	Your knowledge about communication surveillance	1	2	3	4	5
	The sources of communication surveillance	1	2	3	4	5
	Awareness about information/data monitoring by other parties	1	2	3	4	5
	Personal information/data collection	1	2	3	4	5
	How to securely preserve personal information/ data	1	2	3	4	5
	Ways in which my Internet use can be monitored	1	2	3	4	5
	Ways in which my telephone can be intercepted	1	2	3	4	5
	Intrusive technology through other devices (e.g. mobile phone)	1	2	3	4	5
	How to protect myself from surveillance	1	2	3	4	5

ATTITUDES TOWARDS PERSONAL AND WORK INFORMATION

11.	Rate the following questions on Communication Surveillance	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	I am concerned about online surveillance	1	2	3	4	5
	I have control over my information on all my devices e.g. computer, telephone, email, laptop, Ipad etc.	1	2	3	4	5
	I sometimes share inaccurate information about myself online to protect myself.	1	2	3	4	5
	I don't share personal information through internet sites	1	2	3	4	5
	I don't share personal information through social networking sites e.g. Facebook, Twitter, Instagram	1	2	3	4	5
	I am always concerned about privacy of my personal and work information	1	2	3	4	5
	I sometimes fear the negative effects of sharing information online	1	2	3	4	5

SOURCES OF SURVEILLANCE

12.	To what extent do you think the following are observing your information	Very Unlikely	Unlikely	May be	Likely	Highly Likely
	Police	1	2	3	4	5
	Intelligence agencies e.g. NIS	1	2	3	4	5
	Private companies/enterprises	1	2	3	4	5
	Telecommunication or internet providers	1	2	3	4	5
	Employer	1	2	3	4	5
	Criminals	1	2	3	4	5
	Family members	1	2	3	4	5
	Friends	1	2	3	4	5
	Other actors (scammers, hackers)	1	2	3	4	5

HRDS DIGITAL FOOTPRINTS

13.	Digital Footprints	Never	Some-time	Rarely	Often	All the time
	I include location settings in my social media posting	1	2	3	4	4
	I have shared my phone contact online	1	2	3	4	5
	I have shared my area of residence online	1	2	3	4	5
	I have posted online activities which include family members	1	2	3	4	5
	I have shared pictures of my home on social media	1	2	3	4	5
	I have shared pictures of my social events on social media	1	2	3	4	5
	Anyone can tag me on social media	1	2	3	4	5
	I use cyber cafes	1	2	3	4	5
	I use cyber café assistants to help me produce my work	1	2	3	4	5

PERCEIVED SECURITY OF COMMUNICATION TOOLS

14	Rate your perception of security level of the following communication tool	Very Insecure	Insecure	Somehow Secure	Secure	Very Secure
	Speaking face to face	1	2	3	4	5
	Using land line	1	2	3	4	5
	Calling on your cell phone	1	2	3	4	5
	Sending text messages	1	2	3	4	5
	Sending an email without encryption	1	2	3	4	5
	Using mobile chats (WhatsApp, Telegram)	1	2	3	4	5
	Using chats and IM (e.g. Google, Yahoo)	1	2	3	4	5
	Posting on social media (Facebook, Twitter, Instagram)	1	2	3	4	5

HABITS

15	Protective Habits in Information Technologies Use	Never	Sometime	Rarely	Often	All the time
	I use a different communication tool for different people/work because of security	1	2	3	4	5
	I customize my privacy settings to limit those who can access my personal information	1	2	3	4	5
	I check what kind of information will be collected before installing an application in my smart device (phone or tablet)	1	2	3	4	5
	I wouldn't accept/have accepted phones and computers as donations from third parties	1	2	3	4	5
	I secure or disguise digital footprints by e.g. encryption of emails / hard drive, using VPN	1	2	3	4	5
	I always use passwords to lock my phone	1	2	3	4	5
	I change my password regularly.	1	2	3	4	5

ONLINE SECURITY BEHAVIOUR

16.	Online behavior	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	I protect the contents of my email and browsing habits from advertisers and third parties	1	2	3	4	5
	In general, I am worried about my current levels of privacy protection by ISP, e-mail and websites.	1	2	3	4	5
	Privacy is more important than convenience when it comes to internet	1	2	3	4	5
	I have changed my online behavior because I thought my communication was being monitored	1	2	3	4	5

ONLINE PROTECTION

17.	Online Protection Measures	Yes	No
	I consciously protect some of my online information	1	2
	My accounts are protected from unauthorized access and views	1	2
	I password protect my digital devices	1	2
	I am careful on the information I share on social media	1	2
	I do not accept unknown requests in social media	1	2
	I limit my personal information in public platforms	1	2
	I ensure that information such as location geotag are turned off	1	2
	I use private browsing	1	2

ONLINE EXPERIENCE

18.	Online Experience	Yes	No
	I believe my email has been hacked before	1	2
	I believe my phone has been tapped before	1	2
	I believe my social media account has been hacked before	1	2

QUALITATIVE INTERVIEW QUESTIONS

1. Briefly tell us about yourself and your work as a Human Rights Defender.
2. In your understanding, what does communication surveillance entail?
3. Why is communication surveillance important in the work of HRDs?
4. As a HRD, what are your concerns about communication surveillance?
5. What do you see as sources of surveillance in your work as HRD?
6. How do you protect your communication privacy and security as an HRD?
7. What communication tools do you use in your everyday work and how would you rate their level of security?
8. In what ways can a HRD secure and protect their communication?
9. What protective measures have you adopted to ensure your communication security and privacy?
10. What kind of surveillance have you ever been under because of your work?
11. What kind of online threats have you faced and how did you address them?
12. At organisational level – What level of control do you have over your information?

The National Coalition of Human Rights Defenders - Kenya
(NCHRD-K)
P.O. Box 26309 - 00100, Nairobi, Kenya
Cell: +254 712 632 390 **HOT LINE: 0716 200 100**
info@hrdcoalition.org | www.hrdcoalition.org

@nchrdkenya Nchrd Kenya nchrd_k