PERCEPTION SURVEY

Impact of Communication Surveillance on Human Rights Defenders in Kenya

OCTOBER 2020

DEFENDERS COALITION

LIST OF ABBREVIATIONS

AU	Africa 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
DPA	Data Protection Act
HRC	Human Rights Committee
HRD	Human Rights Defender
ICCP	International Covenant on Civil and Political Rights
ICRT	Information and communication Technology
OGA	Intergovernmental 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
NGO	Non-governmental organisations
NIIMS	National Integrated Identity Management System
NIS	National Intelligence Service
UDHR	Universal Declaration on Human Rights
UN	United Nations

TABLE OF CONTENTS

TABLE OF FIGURES

1 EXECUTIVE SUMMARY

This survey set out to assess Human Rights Defenders' (HRDs) level of exposure, understanding and perception of communication surveillance as well as identifying their strategies for mitigating against communication surveillance. It was guided by broad research questions around the norms and legal frameworks being used to govern right to privacy; the emerging patterns of how state use these laws and how they affect HRDs and their work; the level of HRDs' exposure, understanding and perception of communication surveillance; and the strategies HRD's use for mitigating against communication surveillance.

Key findings:

A number of findings are captured in this report:

- HRDs have high level of awareness of a number of aspects of communication surveillance, and the threats they pose to their work.
- There are various sources of information surveillance with hackers and scammers perceived as the most likely source followed by the intelligence service, and telecommunications and Internet service providers. Other sources identified include criminals, employers, friends, private companies, and families.
- HRDs perceive corporates and security forces as the ones trying to access their information, including through using friends and family members to monitor and collect information on them.
- Majority of HRDs believe that they have already been under communication surveillance because of their work. This includes through phone tapping and hacking of their social media and email accounts.
- HRDs are aware of behaviours that may put them at risk of surveillance and most have taken measures to reduce them. Face-to-face communication is perceived as the most secure in the survey; sending email and SMS without encryption are perceived as least secure.
- The most common ways that HRDs secure their communication gadgets include use of passwords which they change regularly, customising privacy settings to limit what data the cookies can access; views on social media, regular password changes, regular check of information to be collected, and use of different communication tools. Reluctance to accept phones and computer donations, securing and disguising footprints were also rated highly. HRDs are also exercising a lot of caution in what they share online.

- HRDs are concerned about the safety and privacy of their personal and work-related information. However, there are varying outcomes on the different apprehensions with gaps between concerns about online surveillance and the actual practice of information sharing.
- Majority of the HRDs though aware of the Data Protection Act are not well acquainted with its provisions and implications, including the role of the Data Commissioner.
- Majority are concerned that the data collected as part of measures to address COVID-19 pandemic is not in safe hands of the government or corporates.
- HRDs are suspicious of the biometric data collected by the National Integrated Information Management System (NIIMS) or huduma number.

Recommendations

For government:

- Fast track amendments to the Computer Misuse and Cybercrimes Act, 2018 to ensure conformity with the Constitution and international standards of protecting privacy.
- Enact policies and laws that provide an environment for defenders to conduct their work freely and in a safe and enabling environment without communication surveillance.
- Fastrack implementation of the Data Protection Act including ensuring the office of the Data Commissioner's office is operationalised, well resourced, and free from any interference.
- Investigate reported cases of unlawful surveillance on human rights defenders and ensure the culpable persons are held responsible.
- Take necessary measures to reform 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
- Disclose the surveillance capabilities of Kenyan government
- Introduce safeguards to ensure that the rights of mobile telephony subscribers in relation to their personal data are guaranteed;

For the private sector:

- Be more transparent about their business models as well as how personal data is being processed as a result of the use of their services;
- Make publicly the measures they take to respond to government request for personal data belonging their users, for example, through publication of transparency reports.
- Comply with provisions on the Data Protection Act regarding processing, storage, and sharing of data pertaining to their clients and customers.

For the Kenya 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 the government's national and international obligations to protect the privacy of its citizens and their personal data.
- Investigate all reported cases of 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 the state surveillance of online and offline activities is lawful and do not infringe on human rights defenders' right to freedom of expression and ability to defend human rights, including through use of the information communication technologies.

For national, local, and international CSOs and HRDs:

- Advocate for amendments to the Computer Misuse and Cybercrimes Act, 2018 to ensure it conforms with the Constitution and international standards of protecting privacy.
- Monitor how the Data Commissioner's office is being set up and operating to ensure it is independent and undertakes its work according to the law.
- Engage in advocacy aimed at holding ISPs accountable to the law as far as communication surveillance and privacy is concerned.
- Continue building capacity to identify threats and risks to identify relevant and effective mitigation strategies. Organisations and networks should reconsider practices that may expose HRDs to surveillance and security risks.
- Make communication surveillance and information safety as topics of constant discussion in HRDs' forums as they are at the core of their work.

For donors:

- Support HRDs and CSOs to build systems, plans, and policies that can improve implementation of safe communication policies and practices.
- Provide funding to rural based CSOs to work on issues of privacy and surveillance.
- Support efforts to protect and temporarily relocate HRDs under stressful environments due to constant surveillance and face serious security threats because of their work.
- Continue supporting HRDs to network including at international level. These include supporting some HRDs to participate in regional and international forums such as African Commission for Human rights and UN mechanisms like Special Rapporteurs.

The right to privacy is considered a fundamental right and is protected in law across the world including Kenya as is detailed in the Bill of Rights. It 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] The right to privacy encompasses information privacy, bodily privacy, privacy of communication, territorial privacy, and surveillance.[4]

Numerous Kenyan HRDs have raised concerns about their mobile phones being tapped and their communication intercepted.[5] Due to the negative implications on their security and that of their family, these experiences have had a chilling effect on the exercise of their rights and freedoms of expression, association, and assembly. 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 is of paramount importance.[6]

Due to the constitutional and statute-based protection of private communications in Kenyan law, lawful surveillance must meet minimum standards provided in law - necessary in a democratic society to achieve a legitimate aim. Individuals must be protected against arbitrary interference with their right to communicate privately. When a government wishes to conduct communications surveillance, it must only

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 Victorian Law Commission in Australia (2001) 'Privacy Law: Options for Reform', Information Paper, www.lawreform.vic.gov.au (Accessed on 16 January 2018);

5 Privacy International, (2006) Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments.

6 "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.pdf

be done in accordance with the law[7]. In CORD v Attorney General (supra) it was held 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."

This report analyses the needs, concerns, and areas of interests for HRDs in relations 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 use of communication tools ranging from face-to-face, traditional communication mediated tools like telephone and now, digital tools. All these provide varied 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 in development of intervention and advocacy strategies.

7 Privacy International, 'Communications Surveillance. Video: What Is Communications Surveillance?' https://privacyinternational.org/explainer/1309/communications-surveillance

3 METHODOLOGY

This study utilised a mixed methodology, combining qualitative and quantitative approaches. A total of 56 HRD respondents (40 women; 16 men) from 38 counties were reached in the survey, while 10 HRDs were interviewed as key informants. Respondents were chosen using purposive sampling from the database of the Defenders Coalition.

The survey data was collected using the Computer Assisted Telephone Interviewing (CATI) method. This research methodology is where an interviewer calls and administers a questionnaire to the respondent. The questionnaire was scripted into a data collection tool (Kobo Collect), which had automated skip routines and other conditional logics, which assisted in administering it effectively. After identifying the designated respondent from the preselected list, the interviewer randomly made a call to the respondent's phone number provided. For every contact provided, the interviewer made five call attempts if no one picked before making the target respondent unavailable for the interview.

Key informants responded to prepared questions, which largely comprised of issues of privacy, freedom of expression and information. The interviews were transcribed and used to enrich the analysis undertaken from the desk review.

The key informant interviews and survey were informed by review of relevant literature pertaining to communication surveillance. The desktop research captured relevant published and unpublished reports in relation to privacy, 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 on the same, human rights codes and charters, among others inform this report.

Anonymity, Security and Privacy

Given the nature of this work, anonymity of the respondents was paramount and the researchers used de-identification procedures to secure their personal data. In data collection, the researchers avoided the collection of unnecessary personal information and specific identifiers that may point to the respondents. Their data was further anonymised and stored in password-protected files only accessible by the researchers.

The researchers also obtained consent of the respondents, and built trust and rapport with them before conducting the qualitative interviews. They also took steps to ensure the physical security of the HRDs, holding the interviews in secure places where HRDs were comfortable.

Respondents' demographics

The respondents self-identified themselves as HRDs and work either individually, through networks or organisations to defend and promote human rights. From the survey, 71%, self- identified as female and 29% as men. Respondents were distributed across different ages with most of them (45%) being between 18 and 30 years old.

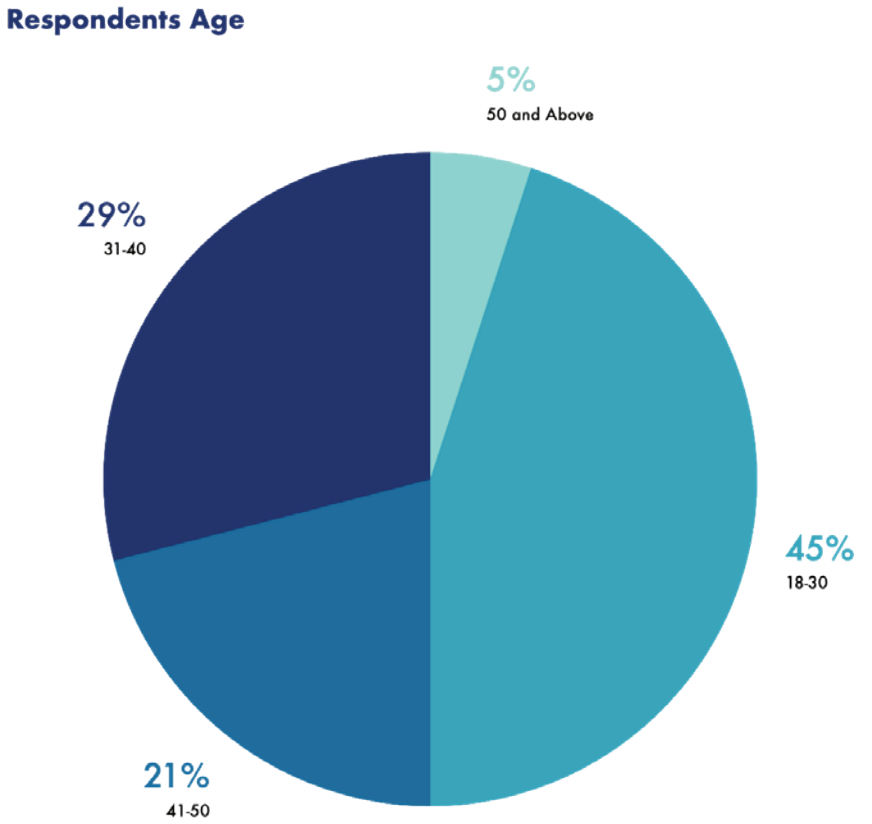


Figure 1: Respondents' age

The HRDs were affiliated or working with an organisation at the time of the interview and 54% of them had work experience ranging 1-5 years.

YEARS OF EXPERIENCE

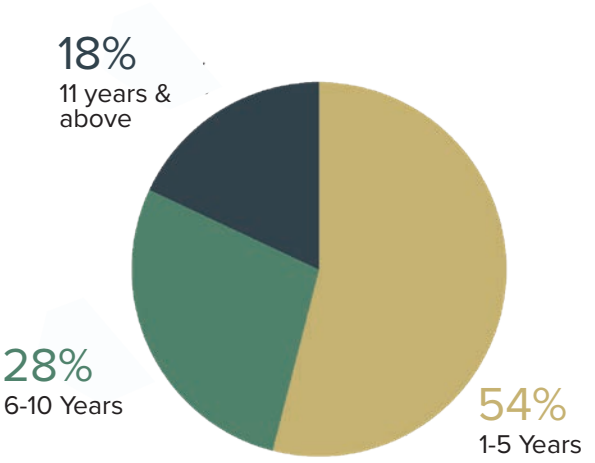


Figure 2: Years of experience in HRD work

The survey respondents had attained different education qualifications with 80% having undertaken higher or post-secondary education in various disciplines.

EDUCATION QUALIFICATION

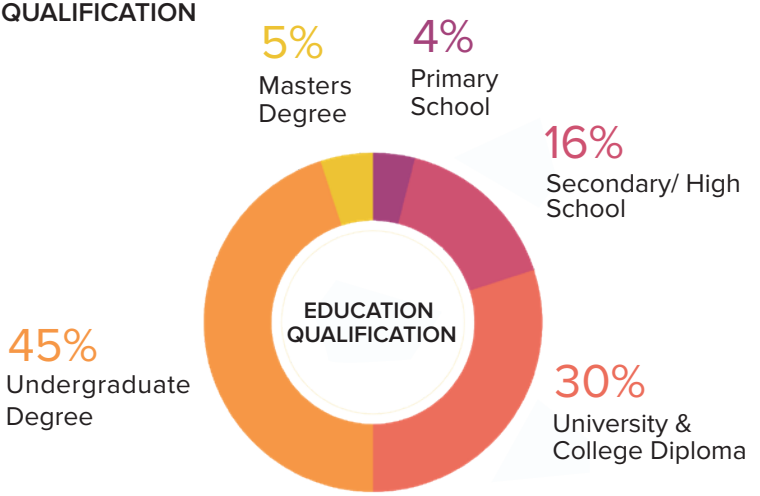


Figure 3: Highest education level attained

The respondents are involved in different types of work, fighting and advocating for various human rights issues.

What typrs of (human rights-related) issues you have been working on?

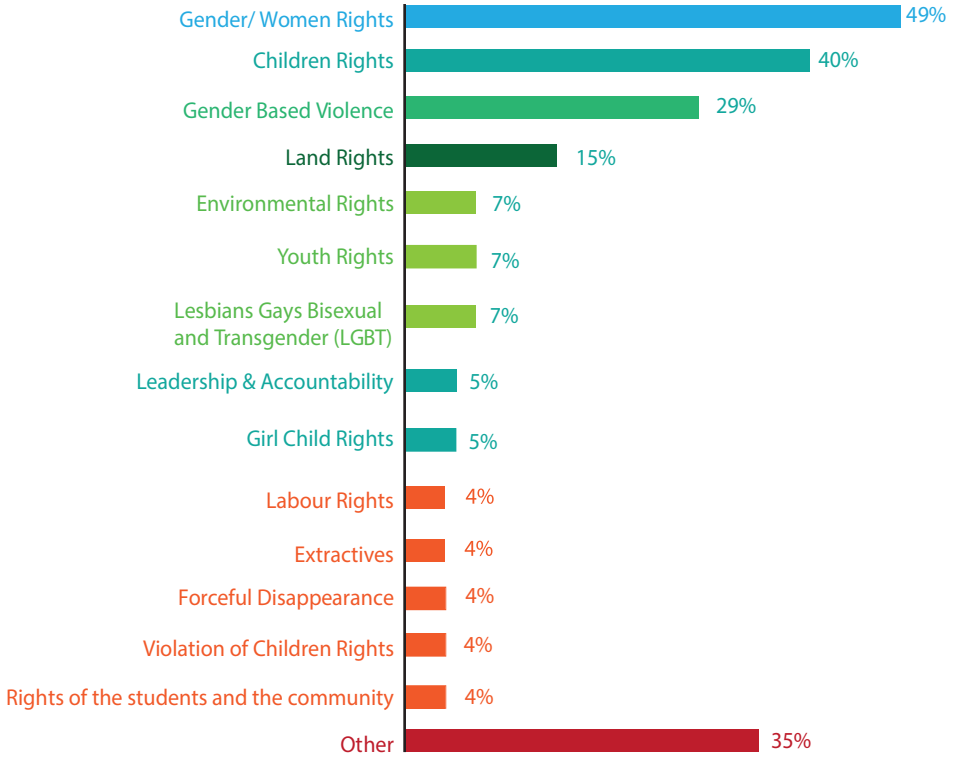


Figure 4: Type of HRD work

4 FINDING AND ANALYSIS

This section presents the survey findings, reflecting the HRDs perceptions on privacy and communication surveillance.

Legal protections of privacy, information and Communication

Article 31 of the 2010 Constitution of Kenya guarantees 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." Nevertheless, the right to Privacy is limited by law but only "to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom"[8]

The Kenya Information and Communication Act (1998) protects communication and information privacy rights in its section 31, which makes it an offence to intercept a message sent through licensed telecommunications service and to disclose its contents, the offence is punishable by three years' imprisonment or a fine of up to three thousand Kenya shillings, or both. Section 83W also prefers an offence for persons who knowingly secures unauthorised access to any computer system for the purpose of obtaining, directly or indirectly, any computer service; or who intercepts or causes to be intercepted, directly or indirectly, any function of, or any data[9] within a computer system.

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, storage, or other kinds of interception or surveillance of communications and related data. KICA also empowers the Communication Authority of Kenya (CA) to prosecute all offences under the Act (section 104).

The Computer Misuse and Cybercrimes Act, 2018 provides for offences relating to computer systems and the establishment of the National Computer and Cybercrimes Co-ordination Committee.[10] It further seeks to (a) protect the confidentiality, integrity and availability of computer systems, programs and data; (b) prevent the unlawful use of computer systems; (c) facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes; (d) protect the rights to privacy, freedom of expression and access to information as guaranteed under the

8 Article 24, Constitution of Kenya 2010

9 Section 15, Constitution of Kenya 2010

10 Not yet operationalised. The committeee is established under secton 27 of the Act, which stood suspended until 3rd February 2020

Constitution; and (e) facilitate international co-operation on matters covered under the Act.

Following the coming into force on 16th May 2018, the Bloggers Association of Kenya filed a constitutional petition on 29th May 2020 asking the High Court to declare unconstitutional 26 sections of the Act.[11] BAKE argued that sections 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 52, and 53 of the Act infringe on freedom of opinion, freedom of expression, freedom of the media and the right to privacy. These provisions deal with various issues including publication of false information, child pornography, cyber harassment, cybersquatting, and wongful distribution of obscene or intimate images. While the operation of these provisions had been ordered suspended since 2018, the court on 20th February 2020 delivered judgment dismissing the petition and finding that the impugned sections of the Act were justifiable under the Constitution and not a violation of fundamental rights and freedoms. BAKE has filed their appeal.[12]

The Data Protection Act 2019 provides for the office of the data commissioner who has a mandate to - receive and investigate any complaints under right to data protection; and carry out inspections and assessments of public and private bodies to evaluate their processing of information and personal data. It may initiate these assessments on its own motion or at the request of a private or public body.

Among other protections, the Data Protection Act No 24 of 2019 enshrines the right of a person to — (a) to be informed of the use to which their personal data is to be put; (b) to access their personal data in custody of data controller or data processor; (c) to object to the processing of all or part of their personal data; (d) to correction of false or misleading data; and (e) to deletion of false or misleading data about them

While the court in Petition 56, 58 & 59 of 2019 (Consolidated) Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR found that the Data Protection Act No 24 of 2019 has included most of the applicable data protection principles, it noted that the Act still required implementation by way of the appointment of the Data Commissioner, and registration of the data controllers and processors, as well as enactment of operational regulations. The Public Service Commission (PSC) had on 7 July 2020 commenced interviews with ten shortlisted candidates but the process had to restart after a case was filed at the Employment and Labour Relations Court which faulted the PSC for not following correct hiring procedure as outlined in the Data Protection Act.[13] On 13th October 2018, president uhuru Kenyatta nominated Immaculate Kassait as data commissioner. She was the former director of voter

11 Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020] eKLR, Petition No. 206 of 2019

12 https://www.blog.bake.co.ke/2020/05/07/we-have-appealed-the-high-court-decision-on-our-cybercrimes-case/

13 At the time of writing this report, the process was still on-going

education at the Independent Electoral and Boundaries Commission (IEBC).

While 63 percent of the HRDs interviewed were aware of the Data Protection Act, 80 percent were not aware of the Data Commissioner's office. This demonstrates a lack of familiarity and understanding of the contents of the DPA. There is need then to popularise the Act and its provisions amongst the HRDs.

The Ministry of Information & Communications Technology (MoICT) published the National Information & Communications Technology (ICT) Policy 2019. The policy places ICT at the centre of the national economic agenda and prioritises the leveraging on ICT to realise Sustainable Development Goals (SDGs) and Vision 2030,[14] Kenya's national long-term development policy, whose goals include the achievement of an information society and knowledge economy. The policy seeks to achieve this end including through providing guidance towards improved data protection, cyber security, network security, and information security.

Kenya is also party to regional and international treaties and conventions that have protections on the right to privacy. The Universal Declaration of Human Rights (UDHR), in Article 12, provides for the protection of privacy, family, home, and correspondence of individuals from arbitrary unlawful interference. 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, and 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. The general commentary on Article 17 of the ICCPR further expounds that under the article envisions that surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic, and other forms of communication, wire-tapping and recording of conversations should be prohibited.[15]

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 with the Constitution. The 2010 Constitution of Kenya thus further protects the right to privacy by enshrining relevant international laws and principles domestically.

At the African Union (AU) level, the African Charter on Human and Peoples' Rights does not have a provision for the right to privacy. In 2019, the African Commission adopted the Declaration of Principles on Freedom of Expression and Access to Information in Africa, which contains guidelines on the right to privacy and data protection in Africa. Prior to that, the AU had adopted a Convention on Cybersecurity and Personal Data Protection in 2014 but has not received the required 15 ratifications for it to come into force. Only Mauritius, Namibia, Guinea,

14 Kenya Vision 2030 document can be downloaded from http://www.vision2030.go.ke/about-vision-2030/
15 ibid

Senegal, Ghana and recently, Rwanda have ratified it. At the East Africa Community level, member States adopted the Framework for Cyber Laws in 2008.

Most African countries including Kenya are grappling with enacting specific and appropriate legislation on the regulation of data collection, control, and processing of personal data. This legal lacuna is dangerous in the context of rapidly technology advancements which themselves create new vulnerabilities for privacy and data protection.

Expansion of communication surveillance

Despite the legal and policy protections outlined above, the Kenyan government has undertaken measures that expand the powers and practices of intelligence and law enforcement agencies, in ways that could lead to unlawful interference with the right to privacy. Majority of these were implemented before the operationalisation of Kenya's data protection regime and have not since been tested for compliance with the provisions of the DPA.

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 monitor incoming and outgoing digital communication.[16] In 2013, it was alleged that there was a Blue Coat Packet shaper installation in the country. Blue Coat allows the surveillance and monitoring of users' interactions on various applications such as Facebook, Twitter, Google Mail, and Skype.[17] As with the NEWS initiative, there was uproar from the media, CSOs, and the general public citing the possible violations of the right to privacy.

In 2014, telecommunication giant Safaricom was awarded a tender to develop an Integrated Public Safety Communication and Surveillance System for the Kenya police. The goal of the project, which is in collaboration with Huawei Technologies is to, among other things, enable security agents to communicate better and boost their capacity to fight terrorism.[18] The multi-billion shilling project would result in the installation of 1,800 and 300 CCTV cameras with face and motor vehicle number plate recognition capabilities in strategic locations in Nairobi and Mombasa respectively. It also set 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

16 Communications Commission of Kenya (2012) 'Kenya and ITU sign administrative agreement for KE- CIRT/CC', 17 February, http://www.cck.go.ke/news/2012/KE- CIRT_signing.html (Accessed on 17 January 2018)

17 Citizen Lab (2013) 'Planet Blue Coat: Mapping Global Censorship and Surveillance Tools, Research Brief, Number 13, January 2013, University of Toronto, MUNK School of Global Affairs, https://citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf (Accessed on 17 January 2018)

18 Daily Nation. (2014, May 13). Why State House made a call to Safaricom chief over insecurity. Daily Nation. www.nation.co.ke/news/Why-State-House-made-a-call-to-Safaricom-chief-over-insecurity/-/1056/2313756/-/ybd3dt/-/index.html

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.[19]

The surveillance project was credited for reportedly increasing ability of law enforcement to detect and respond to crime. Huawei also took credit for 46% reduction of crime rate in Mombasa and Nairobi and 13.5% increase in international tourism in Kenya in 2016.[20] The police in 2019 claimed that the project has assisted in identifying criminals for prosecution and that a number of stolen vehicles have been recovered courtesy of the number plate recognition surveillance cameras in the two cities.[21]

However, concerns are that the Integrated Public Safety Communication and Surveillance System project infringes on citizens' rights to privacy. Human rights defenders warn of 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 unauthorised external access, and the potential for data to be deleted or modified.[22] A 2019 investigation by journalists with the Wall Street Journal found that Huawei technicians in both Uganda and Zambia had in at least two cases helped African governments spy on their political opponents, including intercepting their encrypted communications and social media, and using cell data to track their whereabouts.[23] In addition Ethiopia's national telecommunications network developed by ZTE has enhanced their government's surveillance and censorship capacities that has seen citizens suffer an array of abusive tactics – frequent internet shutdowns, targeted surveillance against journalists and opposition politicians, widespread censorship filtering, and persecutions of individuals for sharing online content.[24]

Other reports have also documented abuse of technologies by the Kenyan government, to monitor and carry out surveillance on citizens. This includes through: the alleged presence of Israeli-based NSO Group mobile phone spyware on two Kenyan Safaricom and SimbaNet ISPs (Citizen Lab 2018); alleged presence of a "middle-box" on a Safaricom cellular network, which can be used to manipulate traffic and assist in surveillance (subsequent tests returned negative results on the middle box suggesting that it was withdrawn) (CIPIT 2017); and alleged direct access to communication systems by national security agencies (PI 2017).

19 Kapiyo, V. and Githaiga, G. (2014) 'Is surveillance a panacea to Kenya's security threats?', https://giswatch.org/en/country-report/communications-surveillance/kenya
20 (Huawei)
21 (NPS 2019)
22 Privacy International and NCHRD-K 2014: 8
23 (Parkinson et al 2019)
24 (Feldstein 2020:4)

There have also been concerns over disproportionate and unlawful surveillance of journalists and HRDs by the Kenyan government,[25] especially those working on issues of impunity for post-electoral violence and extrajudicial executions; counter-terrorism; accountability, anticorruption and social auditing; sexual and reproductive rights; and land rights.[26]

In their 2017 report, Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya, Privacy International detailed the techniques, tools and culture of Kenyan police and intelligence agencies' communications surveillance practices. It focuses primarily on the use of surveillance for counterterrorism operations. The report highlighted how communications content and data is intercepted and how communications data is fed into the cycle of arrests, torture, and forced disappearances. These include through cooperation with telecommunication companies where they knowingly give privileged client information to intelligence and law enforcement agencies without following the proper channels. It also alleges that the NIS has direct access to networks, allowing them to intercept communication without the knowledge of the telecommunication companies. [27]

Section 69 of the Security laws (amendment) act amends the Prevention of Terrorism Act 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.[28] This potentially enables unchecked violation of privacy for any persons in serving government interests where such persons may be accused of committing such offence as provided in the NIS Act. The potential classification of information pertaining to the NIS for security purposes further poses surveillance and security threats to HRDs.

However, in Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya, the High 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 restrictive means of achieving the intended security purpose.[29] In addition, the court expressed its

25 https://privacyinternational.org/state-privacy/1005/state-privacy-kenya#commssurveillance

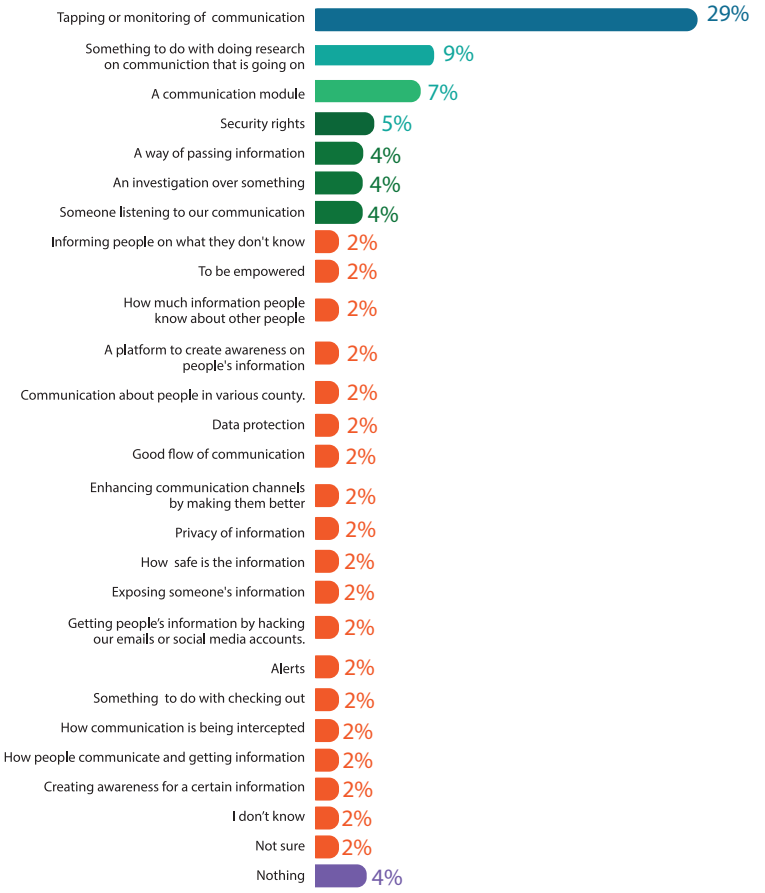
26 Peace Brigades International (2012) An assessment of the feasibility and effectiveness of protective accompaniment in Kenya https://peacebrigades.org.uk/fileadmin/user_files/international/files/special_report/PBI_Kenya_report.pdf

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

28 National Intelligence Service Act, sections 36 and42,

29 Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya &10 others [2015] eKLR. See para 52

When you hear the term COMMUNICATION SURVEILLANCE, what TERMS come to your mind (First)



confidence in the safeguards enacted to prevent the arbitrary violation of the right to privacy.[30] This sets dangerous precedent that may allow security agencies circumvent the constitutional requirement to prove that the limitation was justifiable, necessary, and proportional.

HRDs understanding of Key Concepts Related to Communication Surveillance

When asked what comes to mind when they hear the words communication surveillance, most of the HRDs said it indicates patting or monitoring of communication.

30 Coalition for Reform and Democracy (CORD) & 2 others v Republic of Kenya &10 others [2015] eKLR, para 303

Generally, there is awareness amongst the HRDs that surveillance is related to access to communication, information and data. These findings are like the 2018 report, which also indicated that the HRDs identified monitoring, intelligence, tracking, tapping, spying, police, hacking, and privacy as terms related to surveillance.

In fact, half of the respondents think their email has been hacked before or telephone tapped.

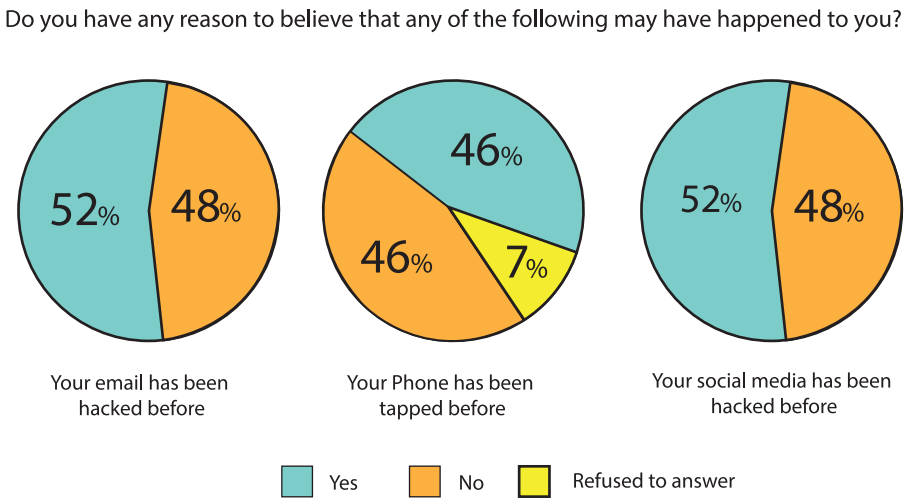


Figure 5: HRDs' experiences with communication and online surveillance

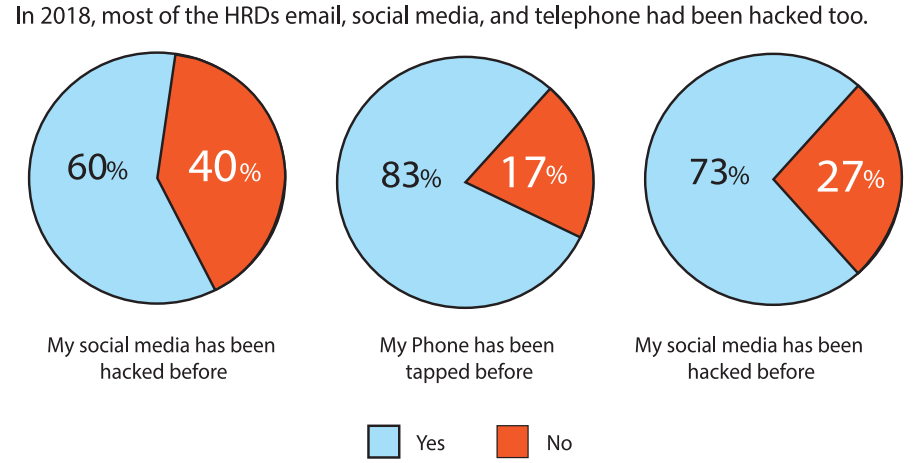


Figure 6: Online security experience (2018)

Respondents were asked to identify one concept that comes to mind when they hear about the term Communication Privacy. Most indicated terms related to secrecy of their information.

When you hear the term COMMUNICATION PRIVACY, what TERMS come to your mind (First)

Table 2: Terms associated with communication privacy

In general, how would you rate your level of awareness/ knowledge of threats and risks posed by the following in surveillance

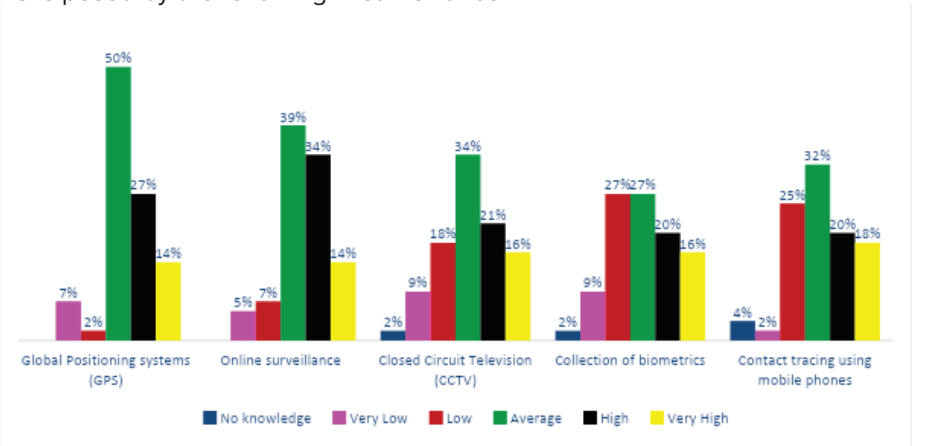


Figure 7: Awareness of data collection mechanisms and platforms

As the data shows, most of the respondents have a high knowledge on the different means of surveillance as seen from the combined percentages marked “high and “very high”. The only exception is on the Global Positioning System (GPS), which 50% said they had average knowledge on how it is used for surveillance. This is a potential area for Defenders Coalition to focus their capacity building on.

Rate your knowledge in relation to the following aspects

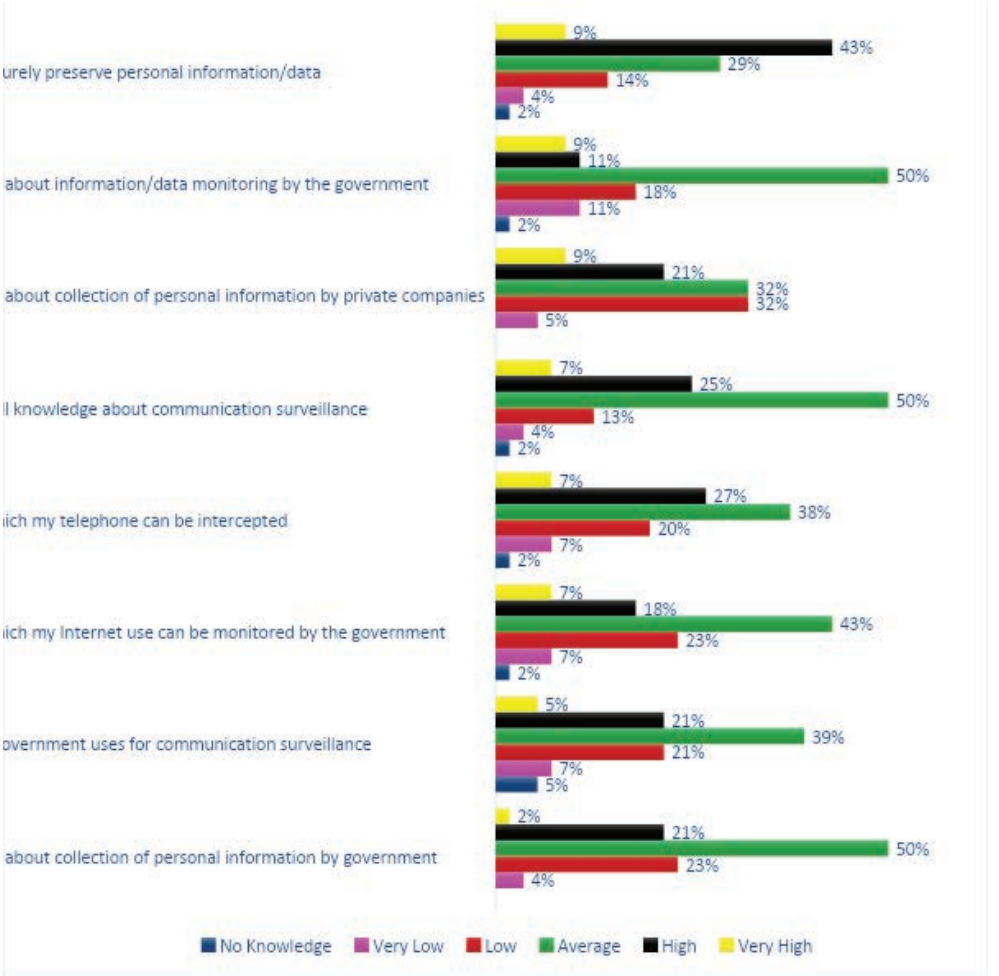


Figure 8: Awareness of communication surveillance

Most of the respondents have average knowledge about the various aspects that were tested. While most know how to securely preserve personal information, a high percentage have average understanding on how the government collects

personal information, Internet monitoring or communication surveillance. Responses from the 2018 survey indicate that 57 percent of HRDs perceived themselves as being most knowledgeable in terms of how to securely preserve information and the ways that the Internet could be monitored, with 50 percent rating their own knowledge of communication surveillance above average. While the figures are almost the same , it can be argued that there is need to continue increasing skills and knowledge of HRDs on communication surveillance and reduce threats they face.

Rate the following questions on communication surveillance

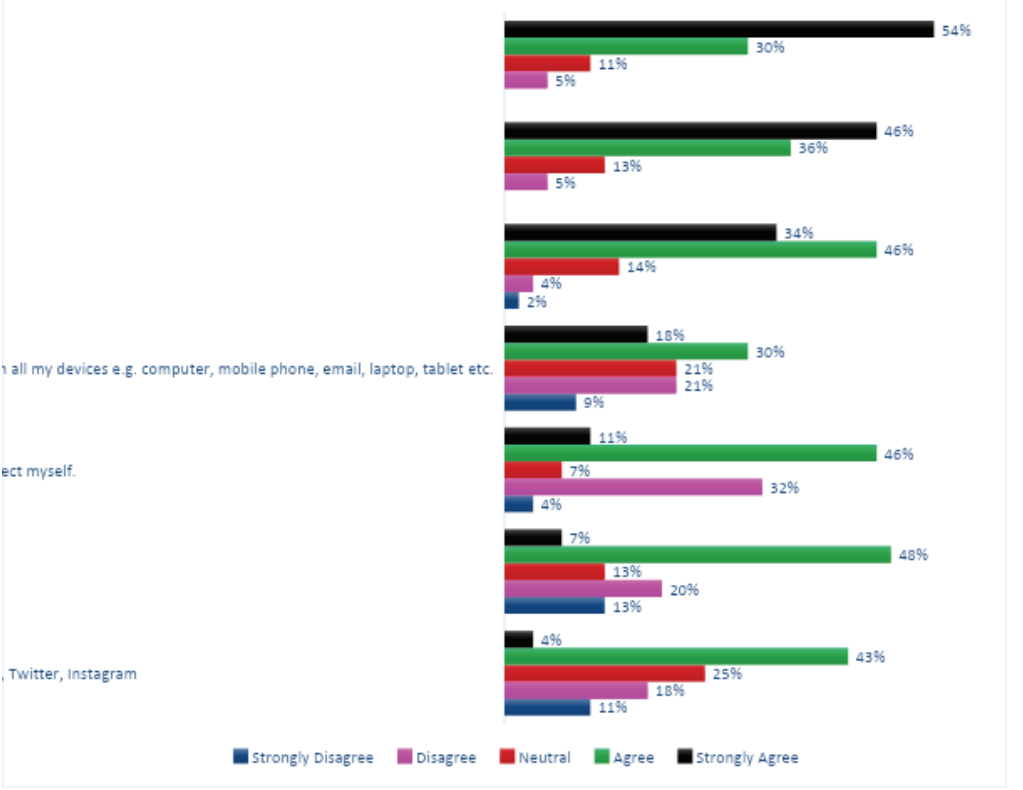


Figure 9: Perceptions of communication surveillance

However, the HRDs were concerned about online privacy and surveillance, took great care not to share private information online, and had control over their privacy as shown in the figure above.

Collection of biometric data and privacy

The Statute Law (Miscellaneous Amendment) Act, 2018 (SLMAA) amended the Registration of Persons Act to create National Integrated Identity Management System (NIIMS), popularly known as huduma number. This system allows the government to collect extensive data on Kenyans and registered foreigners in a national database including: land and house reference number, biometric data such fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA in digital form.

While the NIIMS may have been intended to enhance service delivery, it poses various threats to the right to privacy. Indeed, when asked by they did not register for Huduma Number, privacy issues were on top of the HRD concerns.

Why did you not register for Huduma Number?

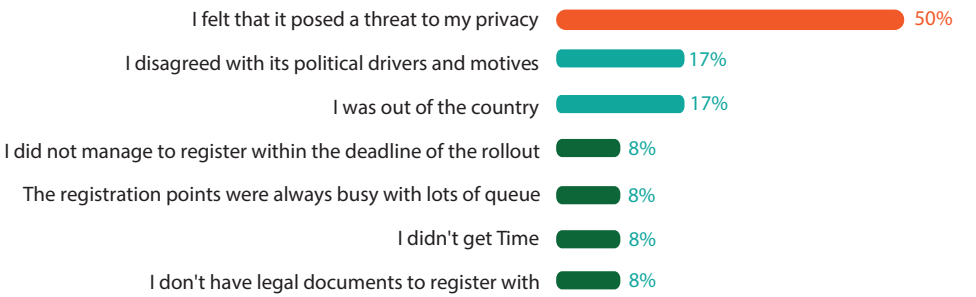


Table 3: Reasons for not registering for Huduma number

Biometric technologies use unique and permanent physical traits or characteristics to identify an individual. When the individual is enrolled in the system – for example, a national identification system – the biometric trait is captured and converted to a digital template to be stored in the system for future reference and matched to identify the individual or a person of interest.[31] As held in Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 others v Cabinet Secretary Ministry of Health & 4 others [2016] eKLR regarding the problematic aspects of government databases, "even where the goal being pursued by the State is legitimate, the manner in which data is collected can be an infringement on the right to privacy."

Collection of such data thus needs to be done in line with the law, with utmost care, and with the consent of the data subjects as is now provided under section 30(1) of the Data Protection Act 24 of 2019. This was not the case for NIIMS since the requirement to register for NIIMS was done without public consultation and made mandatory. The public or data subjects thus did not consent to the processing of their personal and sensitive data. Also arbitrary was the requirement to provide

31 Du Eliza 2013.

Global Positioning System (GPS) co-ordinates. This can potentially be used to track and conduct mass surveillance on the people in Kenya. While a number of HRDs registered for the huduma number, many pointed out that this was largely out of fear that they might be denied public services as had been threatened by the Ministry of Interior and coordination of government.[32] As part of their protection strategies, some of the HRDs registered for Huduma Number but left out some of the personal information or deliberately keyed in false information.[33]

Biometric databases like NIIMS also pose serious privacy threats. Firstly, data breaches on the centralised database would pose serious security threats to the country and its citizens and violate constitutional rights. The databases are managed by people and thus share in the flaws of individuals, they might be hacked or suffer data leak. Expert witnesses in Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR for instance testified to design and architecture flaws of NIIMS arguing that like similar systems such as Aandhar in India, it would expose Kenyans to various ills including data breaches. The collection of biometric data was also considered to potentially pose a threat to HRDs, their work, and the communities they work in/with, this especially for those who work with sexual and gender minorities.[34]

Secondly, the potential of linking an individual's unique data across different government or private databases with a single number allows for all information about an individual to be accessed across multiple databases. Ministry of Interior touted NIIMS as "a single source of truth (one-stop-shop) on persons' identity data for citizens and foreign nationals residing in Kenya."[35]

While it is commonplace and even encouraged that public bodies share data to save on costs and enhance efficiency, individual rights must be considered. Access of personal data by unauthorised officials may prejudice an individual. For instance, numerous openly accessible software and applications are now used to clone fingerprint and voice data for identity theft. Data-intensive systems thus ought only be deployed when, demonstrably, they are necessary and proportionate to achieve a legitimate aim.[36]

Considering whether NIIMS infringed on the right to privacy, the High Court in Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR held that " the collection DNA and GPS coordinates, pursuant to the impugned amendments to the Registration of Persons Act, is intrusive and unnecessary, and constitutes a

32 Interview with NC
33 Interview with SL
34 Biometrics generally pose many risks especially because we work with sexual & gender minorities.
35(NIIMS case para 329)
36 (OHCHR 2018)

violation of Article 31 of the Constitution. In September 2020, Karanja Kibicho, the permanent secretary in the Ministry of Interior revealed in a meeting before the parliamentary committee on Delegated Legislation that the government is set to begin a second phase of Huduma Namba registrations targeting groups that did not register during the 2019 exercise.

Privacy concerns related to COVID-19 pandemic

To aid in contact tracing during the Covid-19 pandemic, the Kenyan government like other states is using technology. The 'Kenya COVID-19 tracker', the government's COVID-19 tracking app, [37] enables disease surveillance teams to register contacts, report suspected COVID-19 cases to the national surveillance system, and conduct investigations for suspected cases. The app functions offline and is interoperable with KenyaEMR. The two systems jointly support workflows for case registration, contact listing, tracing, investigations, COVID-19 laboratory orders, and data exchange with the laboratory.[38]

The government also launched Jitenge, a mobile-based application as a module of the Emergency Alert and Reporting System (EARS) used by the Ministry of Health's Emergency Operations Centre (EOC) to respond to over 40 infectious diseases. Jitenge allows users to either self-register or be registered by various Ministry of Health officials at the quarantine initiation point for home quarantine, at the quarantine facilities, and at the point of entries by port health officials. Registered users then receive daily reminders and prompts to report on their health status including symptoms or any other information. The system is being used to manage and monitor - home based care management; self-quarantine for contacts; post-isolation follow-up; and monitoring of long-distance truck drivers.[39]

The Kenya government thus has been using mobile phone tools and data sources for COVID-19 surveillance activities, such as tracking infections and community spread, identifying populated areas at risk, and enforcing quarantine orders. The Ministry of Health has also been circulating SMS's on COVID-19 and 79 percent of the survey respondents have received such messages.

The use of mobile contact tracing apps for contact tracing offers several benefits: they do not rely on the memory of the case (who may be very ill at the time of interview); they allow contacts unknown to the case to be traced (e.g. fellow passengers who sat close on a train); they can potentially speed up the process; they may facilitate further follow-up of contacts by health authorities via a messaging system. A symptom-checker feature could facilitate this, although it is not essential. [40]

37 Kenya COVID-19 Tracker, https://play.google.com/store/apps/details?id=org.medicmobile.webapp.mobile.surveillance_covid19_kenya&hl=en&gl=US
38 Medic mobile 2020.
39 (mHealth Kenya 2020)
40 (ECDC 2020: 5)

However, the potential benefits that COVID-19 mobile phone–enhanced public health surveillance tools could provide are also accompanied by potential for harm. There are significant risks to citizens from the collection of sensitive data, including personal health, location, and contact data. The Kenya government has not revealed who will receive the Covid-19 data, how those recipients might use it and/or share with other entities. It is also not clear what measures will be taken to safeguard the data from theft or abuse since the Data Protection Act has not been operationalized. Most of the HRDs do not believe government or corporates will safely store their data.

How much trust do you have that your personal information collected as part of measures to address COVID-19 pandemic

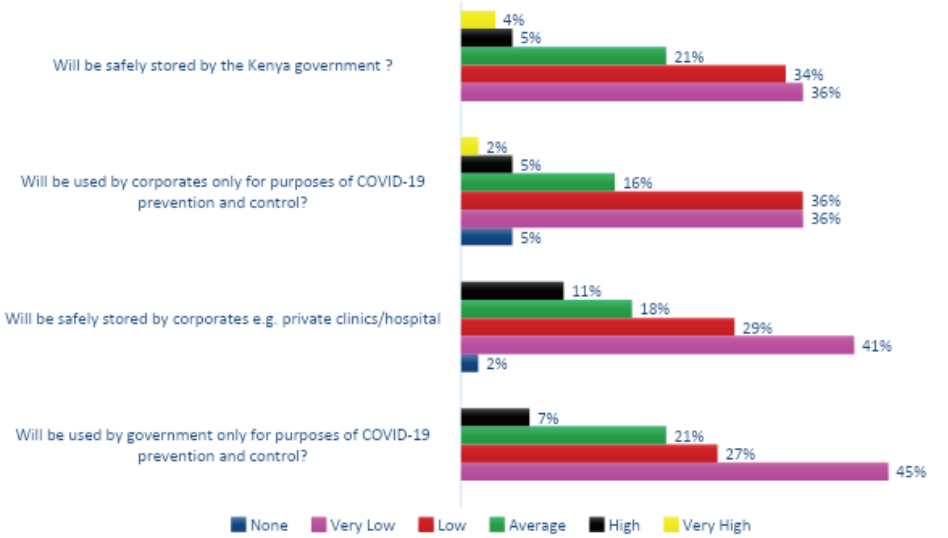


Figure 10: Perceptions of data collected to address COVID-19

If unchecked, collection of COVID-19 data could open a dangerous new front in surveillance and targeting of HRDs. For instance, several human rights organisations have expressed concerns about the misuse of contact tracing apps for the surveillance of protestors, activists, and demonstrations resulting in the infringement of rights such as the right of association, right to unionise, and the freedom of speech and expression.

Attitudes towards Personal and Work Information

To what extent do you think the following are seeking to access your personal information

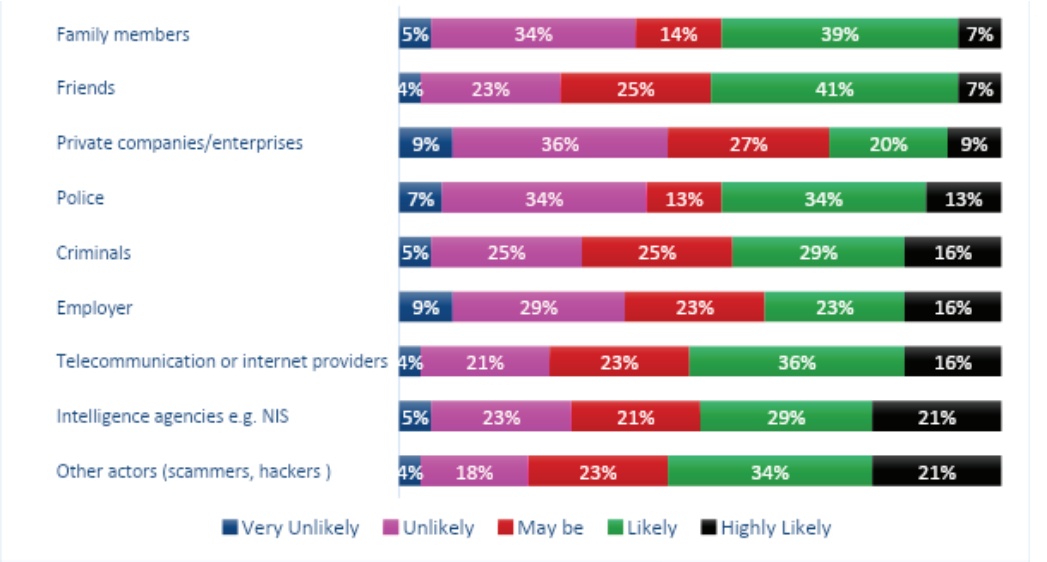


Figure 11: Sources of surveillance

Most of the HRDs think other actors like scammers and hackers are seeking their information, followed by internet/telecommunication providers and then intelligence services. Intelligence services were perceived as the most likely source of surveillance (53%) in the 2018 survey followed by police (37%) and telecommunications or Internet service providers (37%).

The HRDs nevertheless think family members and friends are the ones who are monitoring their personal information.

To what extent do you think the following are monitoring your personal information?

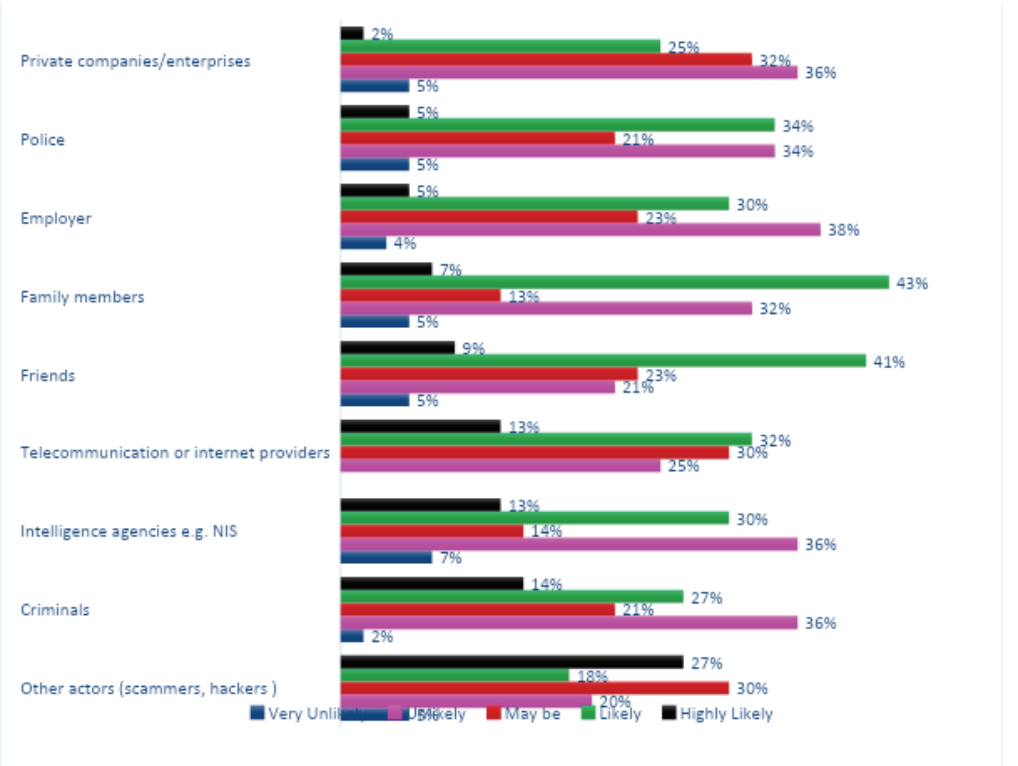


Figure 12: Active sources of surveillance

It is interesting that the HRDs while they feel corporates and security forces are trying to access their information, they believe it is the family members who are monitoring them. Possibly it has to do with the understanding that getting access requires one to have the technology or tools to do so which the family members do not have. Monitoring personal information could be seen as family members reading text messages and checking photos on the HRDs phone and computers.

In your opinion, how secure are the following forms of communication?

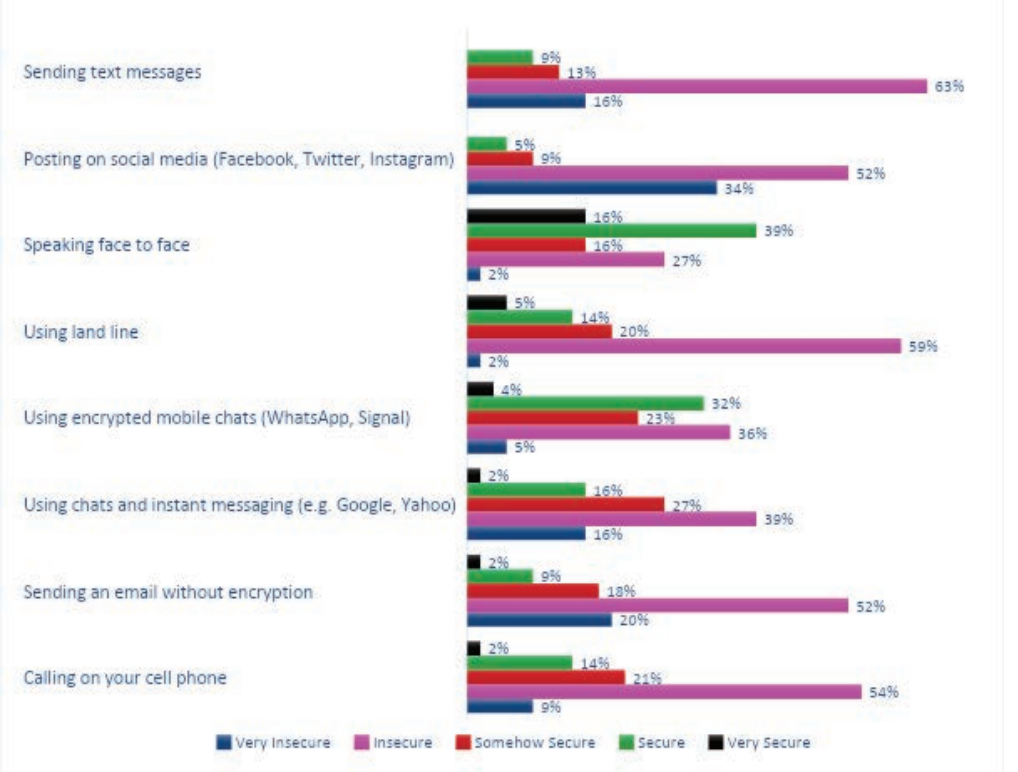


Figure 13: Perceived security of communication tools

Just like in the 2018 survey, the respondents felt face-to-face communications is the safest form of communication followed by using encrypted mobile chats. They nevertheless felt insecure sending text messages, sending unencrypted email, posting on social media, and making phone calls. This is a different view from 2018 when HRDs interviewed felt sending SMS and posting on social media were less risky forms of communication.

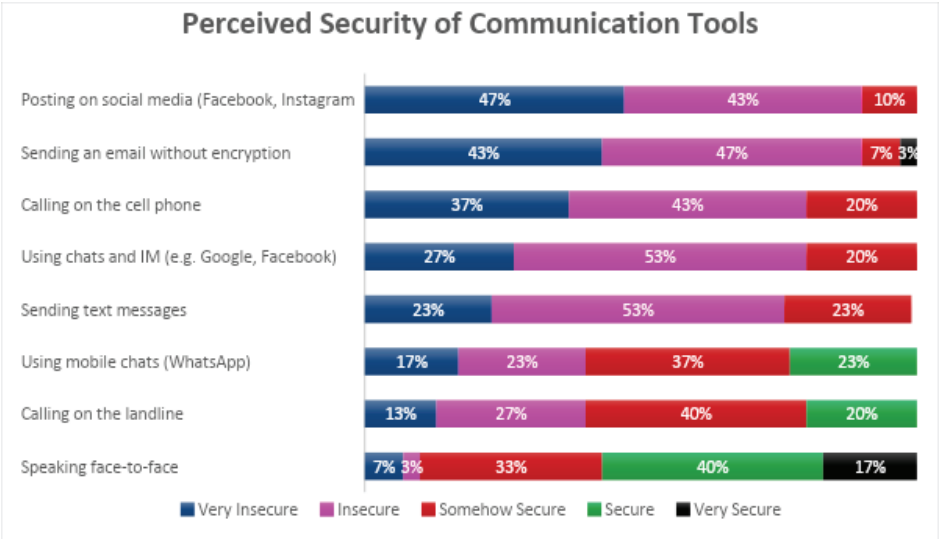


Figure 14: Perceived security of communication tools and platforms in 2018

Whilst the responses do not imply that respondents have a clear understanding of what these terms mean, the terms identified by respondents of the survey indicate that HRDs correctly associate some key terms with security and communications surveillance. Protection refers to measures adopted by individuals and/or organizations to ensure that their information is free from intrusion by any unauthorized parties. It involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data.[41] It also aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Encryption is the process of converting information or data into a code, especially to prevent unauthorized access.[42] Safety defined as the "the condition of being protected from or unlikely to cause danger, risk, or injury" is also a fitting description of the information security.

41 Bygrave, Lee A. Data protection law. Wolters Kluwer Law & Business, 2002

42 Needham, Roger M., and Michael D. Schroeder. "Using encryption for authentication in large networks of computers." Communications of the ACM 21.12 (1978): 993-999.

To what extent do you use the following practices?

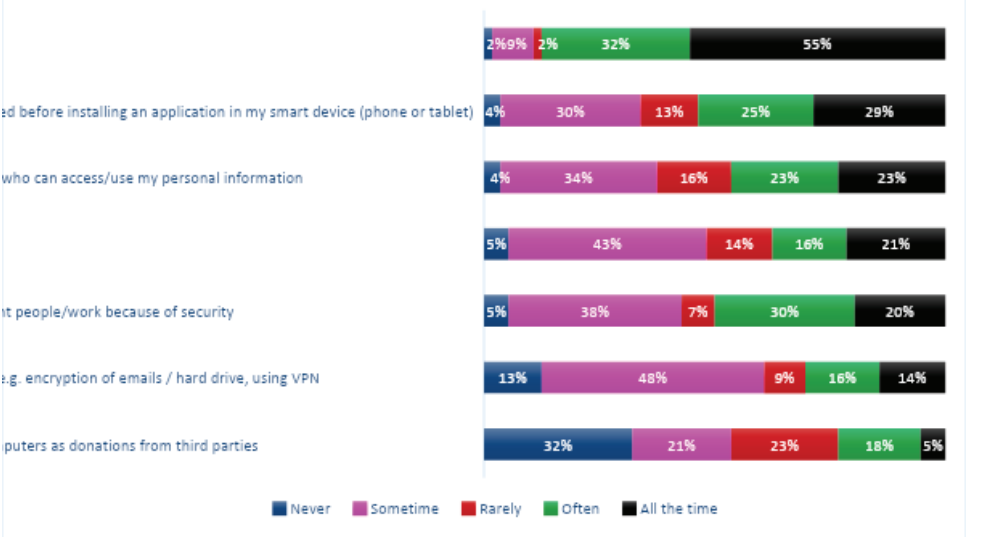


Figure 15: Online security behaviour

Basic security practices like locking mobile phones using passwords is the most popular habit that HRDs undertake to protect themselves from intrusion. Nevertheless, as many as 43percent of the respondents do not change the passwords regularly, which is likely to compromise their security. A further 48percent do not use VPN or encryption, which are highly recommended for HRDs to reduce their threat of exposure.

In 2018 survey, almost similar number (53percent) said they always use passwords to protect their personal mobile phones. Generally, the HRDs have continued with the other habits of customising privacy settings to limit access and processing of their information, regularly check of information to be collected by an application and use of different communication tools for work and for personal use.

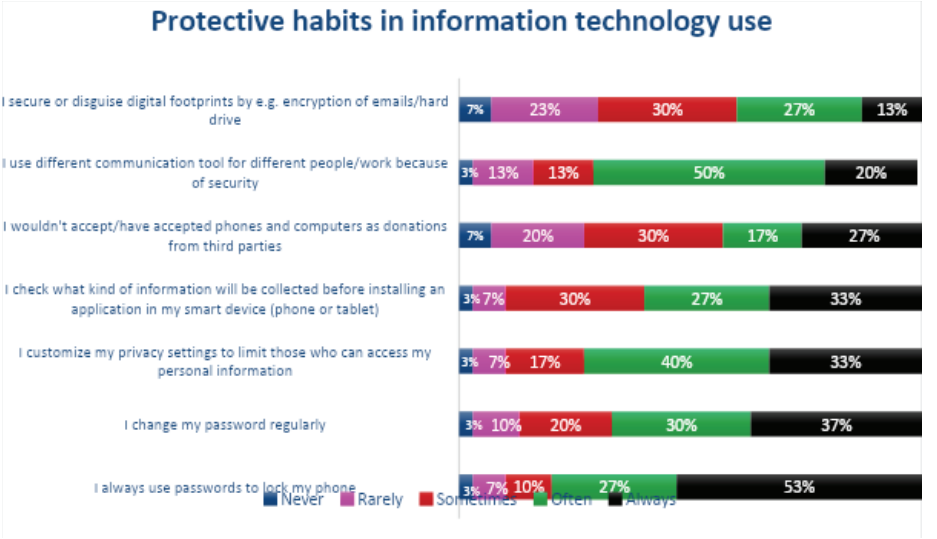


Figure 16: Protective habits survey (2018)

Nevertheless, most HRDs seem to be careful on the digital footprint they leave behind them.

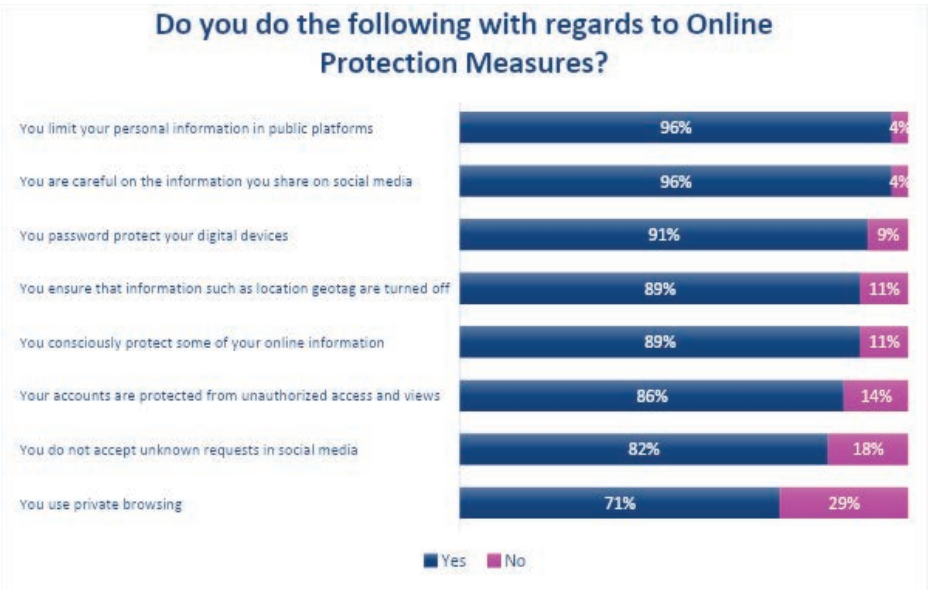


Figure 17: Online Protection measures

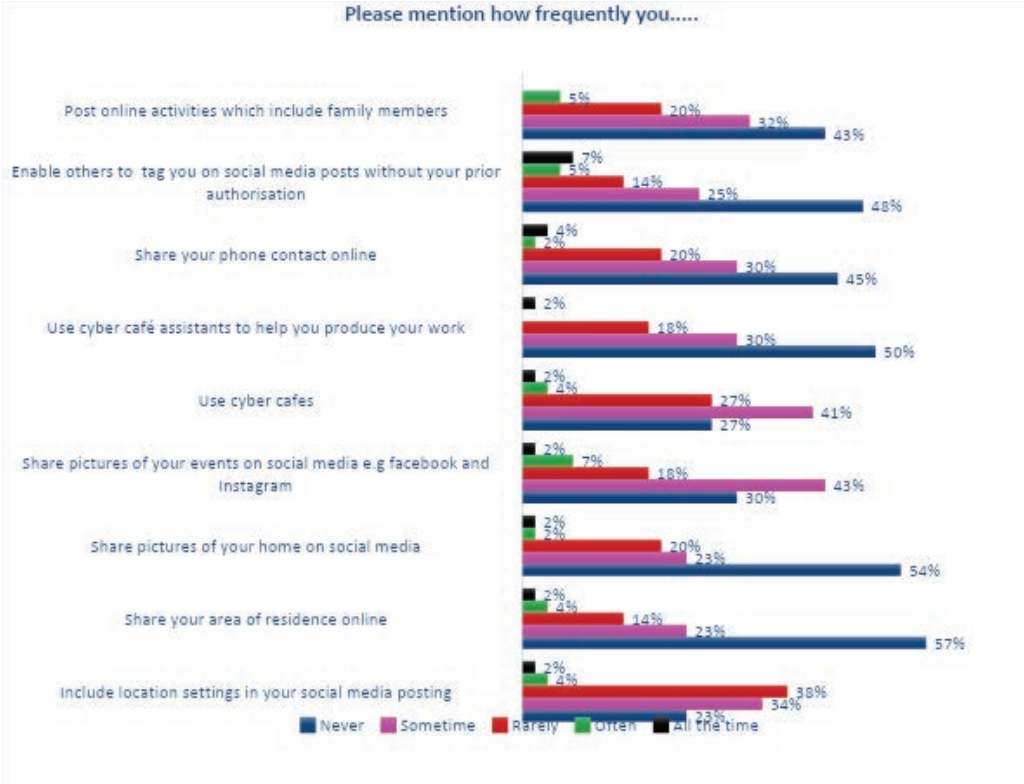


Figure 18: Online behaviour

57percent said they never shared their area of residence online and 54percent do not share pictures of their home on social media. Very few HRDs said they shared phone contacts or enable others to tag them on social media without their authorization. These practices if carried out consistently can reduce risk and threats to the HRDs.

5 CONCLUSION

Human Rights Defenders in Kenya face increased risks of privacy violations as a result of expanding surveillance capacities of security agents, weak legal framework protecting privacy rights, poor implementation of legal provisions and protections, and increased collection of personal data by state and non-state actors. HRDs are in a particularly precarious position since some of their work may involve challenging the conduct of powerful actors who are highly incentivised to protect their interests. This includes through use of surveillance tools to threaten and target HRDs and their loved ones.

This report has presented the 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. The report has also provided an increased understanding of the strategies that HRDs use to protect themselves from and mitigate against risks of communication surveillance. This was guided by broad research question on: the norms and legal frameworks being governing the right to privacy in Kenya; the emerging patterns of state and non-state actors exploit weak and/or absent regulatory frameworks to undertake unlawful surveillance, policies and practices affect HRDs and their work; as well as the level of HRDs' perceived exposure, understanding and perception of communication surveillance; and protection strategies used by HRDs.

While HRDs assessed an overall high level of awareness of communication surveillance issues including demonstrating concerns for communication conducted for personal reasons and in their professional capacity given the nature of their activities, the survey and interviews also reveal 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 pointing to scammers and hackers, intelligence services, and telecommunications and internet service providers as the primary sources. While HRDs are taking certain measures to mitigate risk, it is becoming increasingly difficult to challenge powerful state and private actors due to the power imbalance and HRDs' limited resources to counter the practices used to subject them to surveillance. However, there are still urgent and essential needs as well as opportunities to support the HRD community to better understand and institute various measures to mitigate against the risks and threats they face.

HRDs have adopted various measures to protect their communications and information. These include limiting the personal and work information made available online and on social media, password-protecting their personal devices, encrypting their online communication and customising privacy settings to limit access and sharing of their information amongst others.

Given the constantly evolving nature of Information and Communication Technologies, there is need to continually train and update HRDs on protection of their information and communication in line with emerging risks. This approach ought to be nuanced taking into account the specific context and lived realities of different HRDs. At the same time there is a need to continue challenging the policies and practices of the government as well as those of the private sector.

DEFENDERS
COALITION

SAFETY, SECURITY, WELLBEING OF HRDS

Defenders Coalition | P. O. Box 26309- 00100 Nairobi
info@defenderscoalition.org | +254 712 632 390 | www.defenderscoalition.org