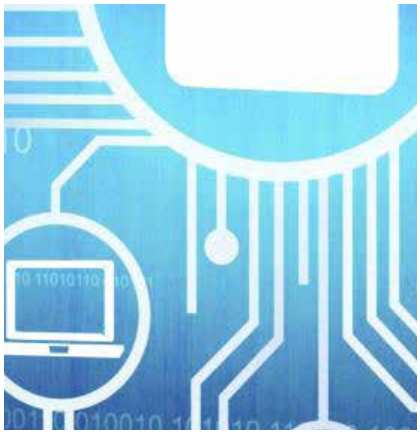
Unwanted Witness

Amplifying voices Changing lives

State of Security for
Human Rights Defenders in a Digital Era








Ugandan Case: Perception and Practices.

State of Security for
Human Rights Defenders in a Digital Era

Ugandan Case: Perception and Practices.

Published by:
Unwanted Witness

CITATION:
The Report can be cited as: "State of Security for Human Rights Defenders in a Digital Era. Ugandan Case: Perception and Practices."

Design and layout by:
Esam Concepts (U) Ltd, Tel: 0774438107

TABLE OF CONTENTS

ACRONYMS

CCTV	Closed-Circuit Television
HRDS	Human Rights Defenders
ICT	Information and Communication Technologies
LAN	Local Area Network
PI	Privacy International
UNOHCHR	United Nations High Commission for Human Rights
UK	United Kingdom
UW	Unwanted Witness
VPN	Virtual Private Network

ACKNOWLEDGEMENTS

The Unwanted Witness wishes to thank the research team led by Mr. Paul Kimumwe, for their efforts in putting this research report together. The team included; Brian Ssenabulya, Deo Walusimbi, Benkerry Mawejje, Julius Esegu, Najib Mulema and the entire UW team.

Notably UW is grateful to her staff, Dorothy Mukasa for the overall leadership and supervision of the research project, and Wokulira Ssebaggala, for providing technical support and Paul Kimumwe for editing of the report.

Unwanted Witness is equally grateful to National Coalition of Human Rights Defenders Uganda (NCHRD-U) for linking the research team to the different respondents in the country. All the respondents are highly commended for their time, patience and responses accorded to the research team throughout the research process.

The Unwanted Witness also wishes to acknowledge the generous support received from the Office of the United Nations Office of the High Commissioner for Human Rights in Uganda (UN OHCHR) and the Irish Aid for the research and publication of this report.

However, neither the UN OHCHR, nor Irish Aid are responsible for the content of the report.

EXECUTIVE SUMMARY

This report presents findings of a study that sought to establish the perceptions, practices and knowledge level of the digital threats and online surveillance among Human Rights Defenders in Uganda.

The study used a combination of qualitative and quantitative data collection tools that included conducting a review of relevant literature to the subject as well as in-depth interviews with purposively selected 153 (101 M and 52F) respondents from across the nation.

Of these, 49% described their primary occupation as journalists/journalism; 46% as human rights defenders, while 5% were human rights lawyers.

Findings

Digital threats to HRDs

From the findings, majority of the respondents (97%) think that HRDs face significant digital threats and are subjected to online surveillance.

In terms of age distribution, all the respondents aged 41 and above believe that HRDs face digital threats and are subjected to online surveillance, while 6% and 2% of those aged between 20-30 and 31-40 respectively think that HRDs do not face any digital threats.

"Besides, sending me threatening messages directly on email and other social media channels, I have experienced scenarios where I have been tracked up to my residence. Some email addresses have been hacked into, and instead used by thugs to email my workmates in search for more information pertaining our activities,"

Experience with digital threats

During the study, respondents were also asked if they have experienced any digital threats and online surveillance in the course of their work. Almost half of the respondents (49%) said that they have been victims of the digital threats, with 51% responding in the negative

"Besides, sending me threatening messages directly on email and other social media channels, I have experienced scenarios where I have been tracked up to my residence. Some email addresses have been hacked into, and instead used by thugs to email my workmates in search for more information pertaining our activities," explains a male human rights activist from Mubende.

In terms of age, the majority of those aged 31 and above said that they have ever been victims of digital threats and online surveillance, with all respondents aged 51 and above answering yes, followed by those aged 41-50 at 69% and those aged 31-40 standing at 52% answering in the affirmative.

Impact of the digital threats to HRDs work and life

Majority of the respondents, 54% said that the threats have had an impact on their work and lives as human rights defenders.

In terms of regional distribution, the majority of respondents in the Northern (64%) and Western (73%) regions reported that the digital threats had affected their work and life as HRDs as opposed to (54%) in Central, (58%) Eastern and (58%) Karamoja who felt that the threats haven't affected their work.

"As a person working on matters of governance and accountability, sometimes I feel threatened to pursue particular issues and so are some of my partners," explains a male human rights activist from Karamoja

Preparedness to deal with digital threats

From the study, the majority of the respondents (79%) felt that the human rights defenders are lacking in the knowledge, skills and tools to circumvent the threats.

The lack of technical competency was reflected across of the regions, and among all the three categories of human rights defenders, human rights lawyers and journalists interviewed.

In terms of regional distribution of self-reported skills and tools to secure their online communication, a slight majority of respondents in the Eastern (54%), Karamoja at 53%, and Western at 57% reported having the skills while in the Northern region, 51% of the respondents said that they do not have the skills and tools needed to secure their online communications.

Lack of institutional-based digital safety and security plan/policy

During the study, respondents were also asked if their institutions had a digital and security plan/policy in place in case they or their colleagues were faced with any danger. A majority of the respondents (84%) responded negatively.

Conclusions

From the findings, it is clear that majority of the HRDs are ill equipped to deal with the rampant digital threats and online surveillance cases that both the state and non-state actors subject them to regularly. Majority of the respondents noted that the threats are related to their work as human rights defenders.

Across all the regions, there was consensus that HRDs face all sorts of digital threats including online surveillance. And probably because of the nature of their work, the majority of the human rights defenders and lawyers reported having experienced digital threats than their counterparts, the journalists.

Also, because of the threats, 83% of the respondents reported to have changed the way they approach their work and life as human rights defenders.

The lack of an institutional digital safety plan/policy in most of the organizations for which the respondents worked means that human rights defenders are more vulnerable and exposed to risks and threats by the perpetrators with the knowledge that they will be dealing with an individual without any kind of support from their (HRD's) institutions.

Recommendations

The government should amend retrogressive laws and policies, such as the Regulations of Interception of Communications Act 2010, and the Anti-Terrorism Act 2002, that give broad powers for the interception of communication and surveillance, because these are open to abuse.

The government should also expedite the passage of the Privacy and Data Protection Bill, 2015 to guarantee the right to peoples' privacy while communicating online.

Human Rights Defenders should always seek to empower themselves with the requisite skills, knowledge and tools that will enable them reduce their vulnerabilities to digital threats by adopting smart and multi-layered security systems

1.0 INTRODUCTION

It is now 15 years since the 2002 Anti-Terrorism Act[1] was passed, to among other things, "… suppress acts of terrorism, to provide for the punishment of persons who plan, instigate, support, finance or execute acts of terrorism…." Since then, there has been an increased concern about surveillance of political dissidents, human rights defenders, and journalists in Uganda[2], particularly in response to the government's increased efforts to allegedly address the threats of terrorism.[3]

Part VII of the Act provides for the interception of communication surveillance. Section 19 (1) states that; "Subject to this Act, an authorized officer shall have the right to intercept the communications of a person and otherwise conduct surveillance of a person under this Act."

The Act also includes provisions that threaten the freedom of expression. With section 9(2) stating that; any person who, without establishing or runs an institution for the purpose, trains any person for carrying out terrorism, publishes or disseminates news and materials that promote terrorism, commits an offence and shall be liable on conviction, to suffer death[4].

Eight years later, the government finally enacted the Regulation of Interception of Communications Act (RICA) 2010, to further reinforce the government's efforts to intercept and monitor peoples' communications in the course of their transmission through a telecommunication, postal or any other related service or system[5].

1 http://www.vertic.org/media/National%20Legislation/Uganda/UG_Anti-Terrorism_Act_2002.pdf
2 https://www.defenddefenders.org/wp-content/uploads/2016/03/The-Right-to-Privacy-in-Uganda-Uganda.pdf
3 https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Uganda. pdf
4 Section 9(2)
5 http://www.ulii.org/ug/legislation/act/2010/18/Regulations%20of%20Interception%20of%20Communications%20Act%2C%202010.pdf

The Act has broad provisions for the interception of communications with limited oversight or safeguards. Under Section 3, it gives the ICT Minister the power "to set up a monitoring Centre, equip, operate and maintain the Centre, acquire, install and maintain connections between telecommunication systems and the Monitoring Centre; and administer the Monitoring Centre at the expense of the state."
Under section 8 of this Act, communication service providers are required to provide assistance in intercepting communication by ensuring that their telecommunication systems are technically capable of supporting lawful interception at all times. Non-compliance by service providers is punishable by a fine not exceeding UGX2.24 million (US$896) or imprisonment for a period not exceeding five years or both and it could also lead to the cancellation of an operator's license.

In 2014, it was reported that the Uganda police had set up the cybercrimes unit, "with the intention of fighting cybercrimes", and had its staff trained by foreign experts in monitoring cybercrimes.[6]

Although the extent of the surveillance capabilities of the Government of Uganda is unclear, a 2015 investigative report by Privacy International (PI) provides evidence of the sale of intrusion malware FinFisher by Gamma International GmbH ('Gamma') to the Ugandan military. The malware was used to infect communications devices of key opposition leaders, media and establishment insiders over period between 2011 and 2013. The secret operation was codenamed Fungua Macho ('open your eyes' in Swahili).[7]

According to the report, covert FinFisher's access points in form of Local Area Networks (LAN) were installed within Parliament and key government institutions. Actual and suspected government opponents were targeted in their homes. Hotels in Kampala, Entebbe and Masaka were reported to have been compromised to facilitate infection of targets' devices.[8] Fake LANs and wireless hotspots were set up in apartment estates and neighborhoods where many wealthy Ugandans and expatriates live.[9]

6 http://www.monitor.co.ug/News/National/Activists-cry-foul-as-police-set-up-cyber-crime-unit/688334-2249294-r8ixtjz/index.html
7 https://www.defenddefenders.org/wp-content/uploads/2016/03/The-Right-to-Privacy-in-Uganda-Uganda.pdf
8 https://www.privacyinternational.org/node/656
9 Ibid

The tool chosen as the 'backbone' of the Fungua Macho operation, FinFisher, was intrusion malware at the time manufactured by the Gamma Group of companies, headquartered in the United Kingdom. Once infected, a person's computer or phone can be remotely monitored in real time. Activities on the device become visible. Passwords, files, microphones and cameras can be viewed and manipulated without the target's knowledge.[10]

Now more than ever, the safety and security of the online community, particularly human rights defenders have become critical. This is because more and more people are embracing digital tools, especially the Internet to enjoy their right to freedom of expression as well as meaningfully participate in political decisions.

On its part, the government seems to be threatened by the ability that online platforms afford the citizenry and has thus chosen to undertake systematic surveillance, backed by retrogressive pieces of legislations. And unfortunately, many online community members, including Human Rights Defenders, are not aware of the nature and extent of digital threats and online surveillance they are being subjected to, nor do they have the knowledge and skills to help them take the necessary measures to protect themselves, their data and communications from unlawful interference.

10 https://privacyinternational.org/sites/default/files/Uganda_Report.pdf

2.0 STUDY OBJECTIVE

For Unwanted Witness, it was therefore critical to undertake a nationwide study to establish the perceptions, the types and knowledge level of the digital threats and online surveillance among HRDs in Uganda.

Specifically, the study sought to:

Establish the knowledge levels of digital threats and online surveillance among HRDs in Uganda

Understand the type and level of impact these digital threats and online surveillance has on the lives and work of HRDs in Uganda

Identify the existing strategies being used by HRDs to circumvent and mitigate the consequences of digital threats and online surveillance

Propose innovative strategies for HRDs to use in circumventing and mitigate consequences of digital threats and online surveillance

Beyond the objectives, the study also sought to interrogate the following research questions:

What perceptions do HRDs have about digital threats and online surveillance in Uganda?

How knowledgeable/informed are HRDs on the digital threats, including online surveillance that they face?

What are the main digital threats faced by HRDs in Uganda?

What/who are the most at risk RHDs in Uganda to digital threats and online surveillance?

What impact are digital threats and online surveillance having on the work and lives of HRDs in Uganda?

How prepared are HRDs in dealing with increasing digital threats and online surveillance?

What strategies and tools are HRDs in Uganda using to circumvent and mitigate the consequences of digital threats and online surveillance?

What new innovative strategies/tools can HRDs in Uganda adopt to circumvent and mitigate the consequences of digital threats and online surveillance?

3.0 RESEARCH METHODOLOGIES

The study used mixed methods of data collection, analysis and integration of both qualitative and quantitative data at two different levels:

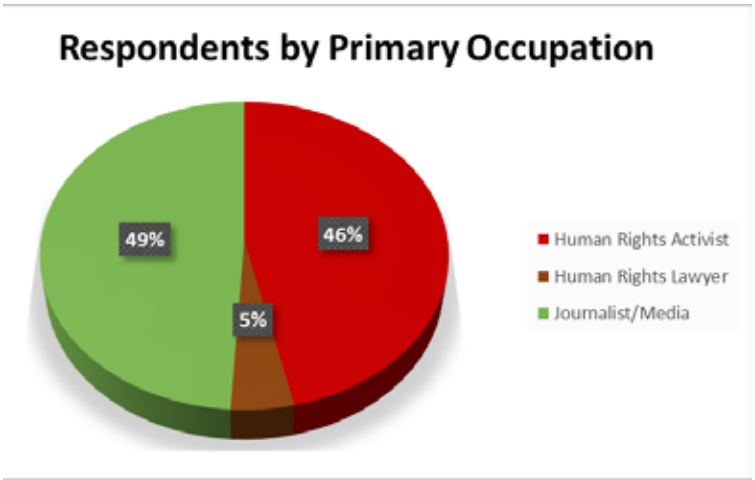
Literature Review

The study reviewed and analysed existing relevant literature on the perceptions, attitudes and practices of HRDs towards digital security and online surveillance, as well as literature about the general state of safety and protection of HRDs. Reviewed literature included the various laws and policies such as the Anti-Terrorism Act 2002; The Regulation of Interception of Communications Act 2010; reports from organisations such as Privacy International, Freedom House; Unwanted Witness; and newspaper reports.[11]

Key informant interviews

The study also involved conducting in-depth interviews (IDIs), involving detailed discussions with purposively selected key informants. An interview guide was prepared with questions to facilitate the conversation with the key informants, who were selected through majorly referral from among human rights lawyers, human rights defenders and journalists.

Distribution of respondents by primary occupation



11 See footnotes for detailed list of literature reviewed.

Primary occupation	Respondents	Percent
Human Rights Activist	71	46.4
Human Rights Lawyer	7	4.6
Journalist/Media	75	49.0
Total	153	100.0

At 49%, journalists constituted the highest number of respondents, followed by human rights activists at 46% and lastly human rights lawyers at 5%.

Scope of the Study

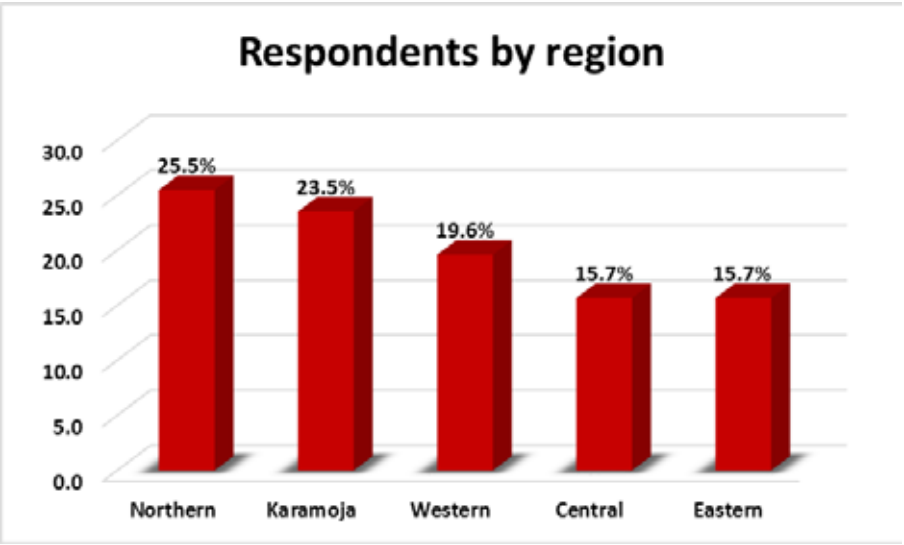
In terms of scope, this was a nationwide survey covering five sub-regions of Uganda, namely Eastern, Karamoja, Northern, Western and Central. In terms of issues, the study sought to explore the perception and knowledge levels of HRDs on digital threats; how these threats have impacted the life and work of the HRDs, key tools and strategies used by the HRDs to circumvent the threats, as well as new and innovative tools and strategies that the HRDs can adopt.

Sample size and sampling procedure

The study reached a total of 153 purposively selected respondents for the interview-administered questionnaires. In order to reach these respondents, the study used a multi-stage sampling strategy where the country was divided into five regions – Northern, Karamoja Southern, Eastern, Western and Central.

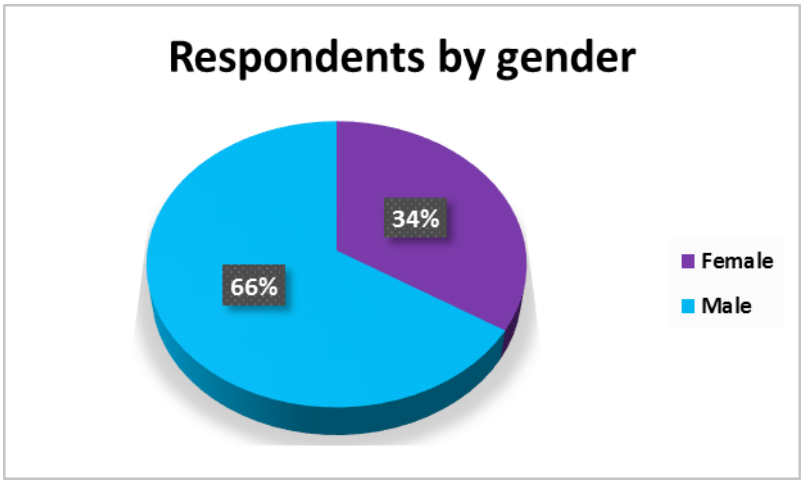
Distribution of respondents by regions

Region	Respondents	Percent
Central	24	15.7
Eastern	24	15.7
Karamoja	36	23.5
Northern	39	25.5
Western	30	19.6
Total	153	100.0



Distribution of respondents by gender

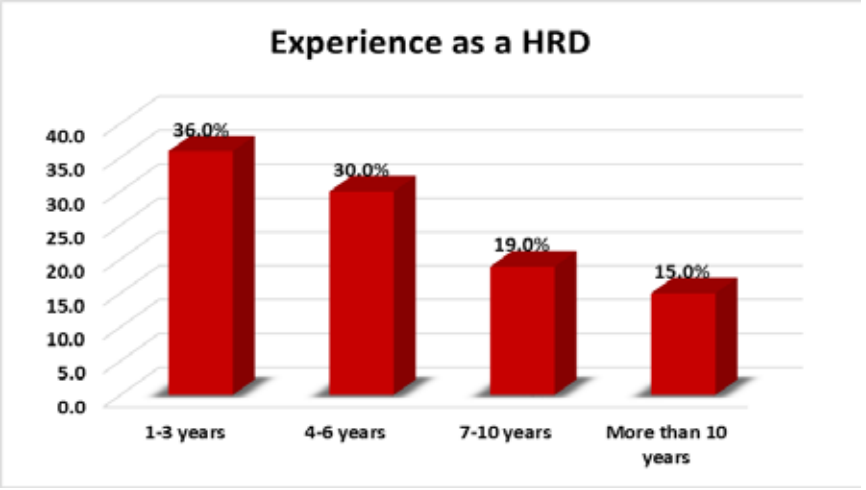
Gender	Frequency	Percent
Female	52	34.0
Male	101	66.0
Total	153	100.0



From the above figure, of the 153 respondents, 66% of them were males and 34% were female. There were fewer women willing to participate than men.

Distribution of respondents by experience working as a human rights defender

Experience as a HRD	Frequency	Percent
1-3 years	55	36.0
4-6 years	46	30.0
7-10 years	29	19.0
More than 10 years	23	15.0
Total	153	100.0

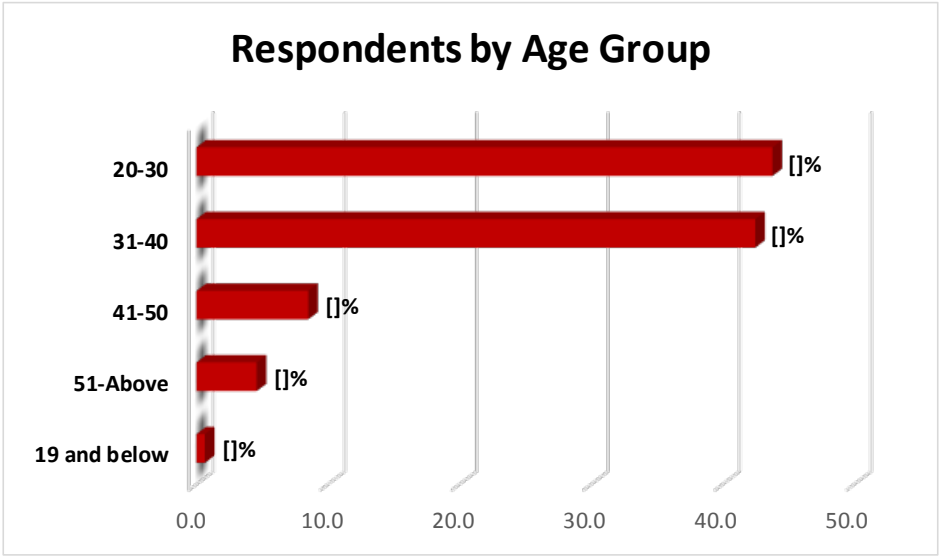


Majority of the respondents interviewed (36%) had between 1-3 years' experience as HRDs, followed by those with 4-6 years' experience at 30%. The percentages decreased significantly as the number of years increased, with only 15% of those interviewed having had more than 10 years' experience.

Distribution of respondents by age

Age Group	Respondents	Percent
19 and below	1	0.7
20-30	67	43.8
31-40	65	42.5
41-50	13	8.5
51-Above	7	4.6
Total	153	100.0

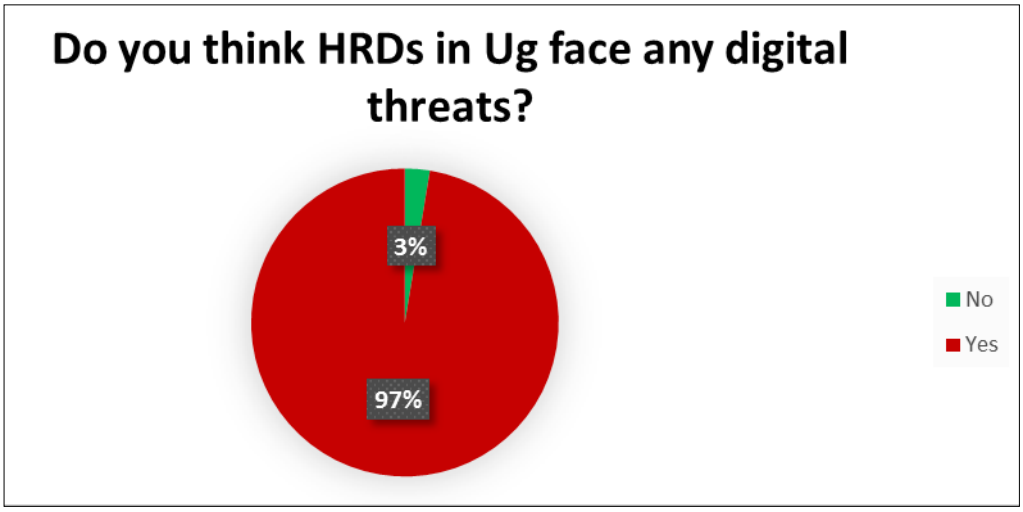
From the above table and figure, majority (44%) of the respondents were between 20-30 years old, followed by those aged between 31-40 at 43%.



4.0 STUDY FINDINGS

4.1 Knowledge and Perceptions of HRDs about digital threats and online surveillance in Uganda

From the findings, the majority of the respondents (97%) think that HRDs face a lot of digital threats and are subjected to online surveillance.



In terms of regions, all respondents from both Western and Karamoja regions said that HRDs face digital threats and are subjected to online surveillance, while in the Central, Eastern and Northern, over 95% said that HRDs face digital threats.

Distribution of respondents' perceptions of digital threats by region

Region	No	Yes	Total (n)
Central	4.2	95.8	24
Eastern	4.2	95.8	24
Karamoja	0.0	100.0	36
Northern	5.1	94.9	39
Western	0.0	100.0	30
Total	2.6	97.4	153

In terms of age distribution, all the respondents aged 41 and above believe that HRDs face digital threats and are subjected to online surveillance, while 6% and 2% of those aged between 20-30 and 31-40 respectively think that HRDs do not face any digital threats.

Distribution of respondents' perception of digital threats by age

Age group	No	Yes	Total (n)
19 and below	0.0	100.0	1
20-30	4.5	95.5	67
31-40	1.5	98.5	65
41-50	0.0	100.0	13
51-Above	0.0	100.0	7
Total	2.6	97.4	153

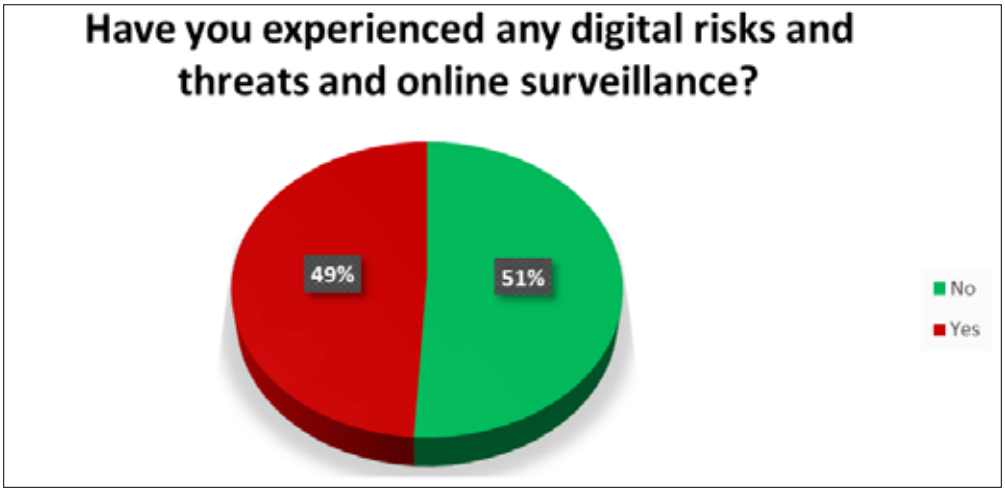
The respondents who said that HRDs face digital threats were asked to mention the key digital threats. In no particular order, below is the list of threats that were mentioned.

Arbitrary arrests, threats to life, imprisonment, kidnap, detention

- Forged charges
- Hacking of personal accounts
- Monitoring of social media posts by authorities
- Blocking social media i.e. during elections
- Threatening emails, phone calls, sometimes confiscation of the gadgets like computers
- No right to privacy - Re registration of sim cards and making it easy to share all of your data.
- Limited freedoms of expression through regulations by government, Hacking, shutting down internet
- Break-ins into offices
- Intimidation after publishing some stories
- Torture
- Online surveillance
- Multiple cyber legislations
- Prevention from accessing certain information
- Social media harassment

4.2 Experience with digital threats and online surveillance

During the study, respondents were also asked if they have experienced any digital threats and online surveillance in the course of their work. Almost half of the respondents (49%) said that they have been victims of the digital threats, with 51% responding in the negative.



In terms of regional distribution, majority of the respondents from Eastern (75%), and Northern (54%) said that they have been victims of digital threats, while in the Central, Karamoja and Western, the majority of the respondents (53%), 61%, and 60% respectively said that they have not experienced any digital threats.

Distribution of experience to digital threats by regions

Region	No	Yes	Total (n)
Central	58.3	41.7	24
Eastern	25.0	75.0	24
Karamoja	61.1	38.9	36
Northern	46.2	53.8	39
Western	60.0	40.0	30
Total	51.0	49.0	153

In terms of age, majority of those aged 31 and above said that they have ever been victims of digital threats and online surveillance, with all respondents aged 51-above answering yes, followed by those aged 41-50 at 69% and those aged 31-40 standing at 52%.

Distribution of experience to digital threats by age

Age group	No	Yes	Total (n)
19 and below	100.0	0.0	1
20-30	62.7	37.3	67
31-40	47.7	52.3	65
41-50	30.8	69.2	13
51-Above	0.0	100.0	7
Total	51.0	49.0	153

When it came to profession, majority of human rights lawyers (57%) and human rights activists (54%) said that they have personally fallen victim to digital threats and online surveillance.

Distribution of experience to digital threats by profession

Primary occupation	No	Yes	Total (n)
Human Rights Activist	46.5	53.5	71
Human Rights Lawyer	42.9	57.1	7
Journalist/Media	56.0	44.0	75
Total	51.0	49.0	153

Of the respondents who said that they have ever experienced any digital threats or online surveillance, 63% said that the threats were related to their work while 37 % said the threats were random.

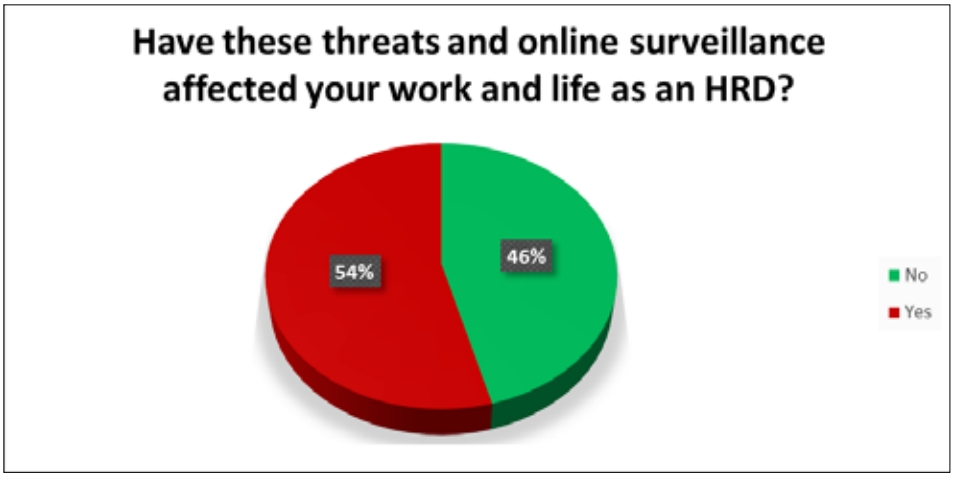
"Besides, sending me threatening messages directly on email and other social media channels, I have experienced scenarios where I have been tracked up to my residence. Some email addresses have been hacked into, and instead used by thugs to email my workmates in search for more information pertaining our activities, explains a male human rights activist from Mubende.

"Internet hacking (email), tapping of telephone conversations, receiving of anonymous emails and calls where somebody is soliciting assistance for money," explains a female respondent from West Nile.

"The attacks were related and I feel that they caused the loss of my laptop because I would always find some threatening messages in my email accounts," explains a male journalist in Masaka

4.3 Impact of digital threats and online surveillance to HRDs

The majority of the respondents (54%) stated that the threats have had an impact on their work and lives as human rights defenders.



In terms of regional distribution majority of respondents in the Northern (64%) and Western (73%) regions reported that the digital threats had affected their work and life as HRDs, while a bigger percentage in Central (54%), Eastern (58%) and Karamoja (58%) felt that the threats have not affected their work and life as HRDs.

Distribution of the impact on the HRDs' work and life by region

Region	No	Yes	Total
Central	54.2	45.8	24
Eastern	58.3	41.7	24
Karamoja	58.3	41.7	36
Northern	35.9	64.1	39
Western	26.7	73.3	30
Total	45.8	54.2	153

On the other hand, the majority of the respondents aged 31-40 and 51-above reported that the digital threats affected their work and life. While those aged 19 and below (100%); 20-30 (54% and 41-50 years (54%) reported that the threats have not affected their work and life as human rights defenders.

Distribution of the impact on the HRDs' work and life by age

Age group	No	Yes	Total
19 and below	100.0	0.0	1
20-30	53.7	46.3	67
31-40	36.9	63.1	65
41-50	53.8	46.2	13
51-Above	28.6	71.4	7
Total	45.8	54.2	153

And when it came to profession, majority of the human rights lawyers (75%) and journalists (59%) reported that the digital threats had had an impact on their work and life as human rights defenders.

Distribution of the impact on the HRDs by profession

Primary occupation	No	Yes	Total
Human Rights Activist	50.7	49.3	71
Human Rights Lawyer	42.9	57.1	7
Journalist/Media	41.3	58.7	75
Total	45.8	54.2	153

"Sometimes I feel threatened to pursue particular issues and so are some of my partners," explains a male human rights activist from Karamoja

"I'm not open to all people anymore because I fear for my life," explains a female journalist from Karamoja.

"Some of our targeted community members get threatened from releasing information they deem sensitive thus affecting my work," explains another male human rights activist from the Eastern region.

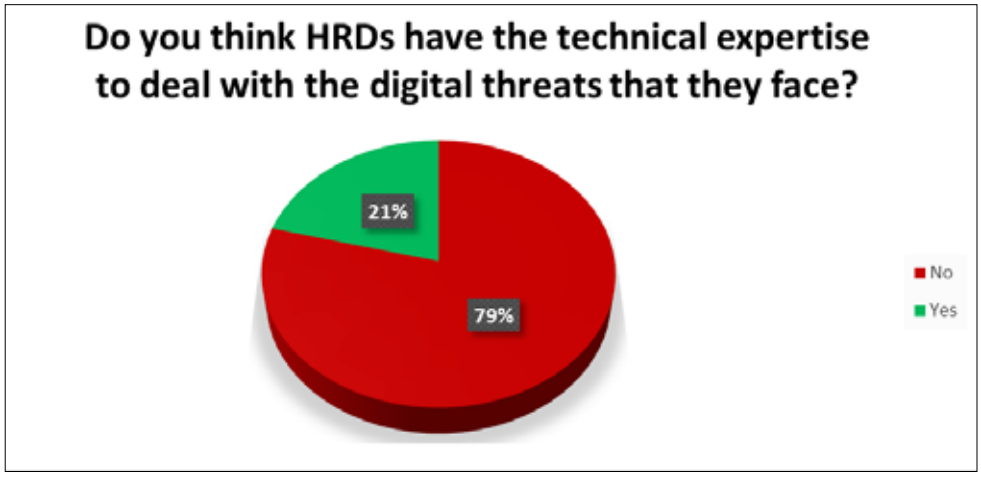
"People whom I regard as my sources are afraid of divulging information," explains a male journalist from Central region

"Fear to report directly to bodies, fear to avail contacts to unknown persons because of possible threats, I'm now fearing other partners who are not known to me," explains another female human rights activist from West Nile.

"There is a time when I had to relocate my family to another area and much as you have to communicate, the fear bogs you down because you feel that your life and work are all at stake," explains a male human rights activist from the Western region.

4.4 Level of preparedness of HRDs in dealing with digital threats and online surveillance

Asked whether they think HRDS have the technical expertise to deal with the increasing digital threats and online surveillance. Majority of the respondents (79%) felt that the human rights defenders are lacking in the knowledge, skills and tools to circumvent the threats.



Across all regions, majority of the respondents noted that the HRDs do not have the technical expertise to deal with the digital threats that they face.

Distribution of respondents on the technical expertise of HRDs by region

Region	No	Yes	Total (n)
Central	66.7	33.3	24
Eastern	100.0	0.0	24
Karamoja	91.7	8.3	36
Northern	69.2	30.8	39
Western	70.0	30.0	30
Total	79.1	20.9	153

The pattern was the same across all age groups except those under 19, which had only one respondent.

Distribution of respondents on the technical expertise of HRDs by age

Age group	No	Yes	Total (n)
19 and below	0.0	100.0	1
20-30	83.6	16.4	67
31-40	78.5	21.5	65
41-50	76.9	23.1	13
51-Above	57.1	42.9	7
Total	79.1	20.9	153

In terms of profession, the three categorisations – majority of the human rights activists, human rights lawyers, and journalists at 76 %, 86% and 80% were all in agreement that they do not have the competence to deal with the digital threats that they face in the course of their work.

Distribution of respondents on the technical expertise of HRDs by profession

Primary occupation	No	Yes	Total (n)
Human Rights Activist	77.5	22.5	71
Human Rights Lawyer	85.7	14.3	7
Journalist/Media	80.0	20.0	75
Total	79.1	20.9	153

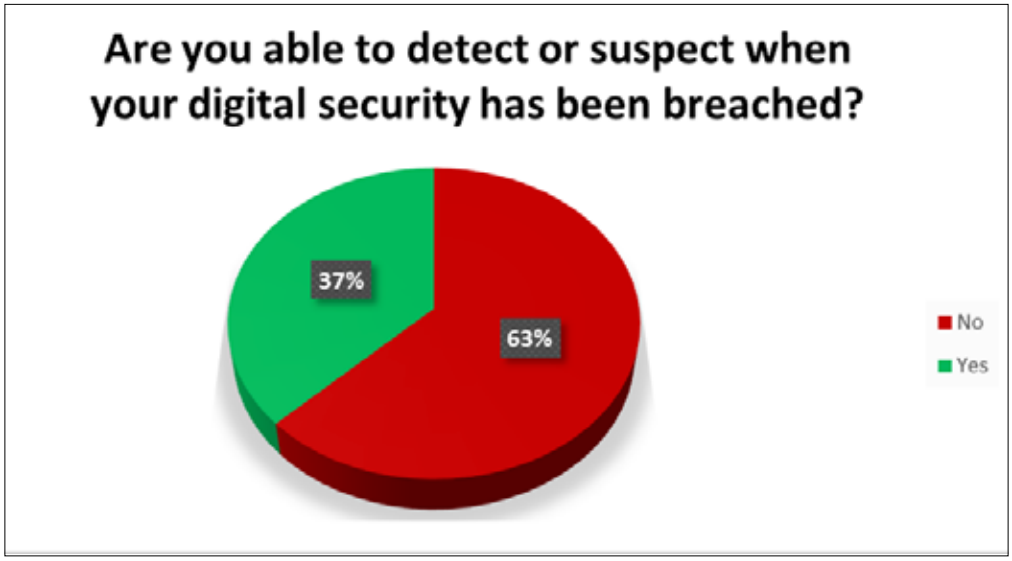
Respondents were also asked to mention any skills that human rights defenders may have to deal with the digital threats that they face. Below is a list of the skills mentioned.

What technical expertise do HRDs have to deal with the digital threats that they face?

- We also have trained IT personnel who help us overcome these digital threats
- Some HRDs have undergone some ICT training so it is somehow easy for them to deal with the digital threats but on the other hand some HRDs are green about the technical expertise.
- Through trainings, most HRDs have been equipped with skills to deal with these digital threats.
- They use passwords
- Some HRDs like me opted for digital security and whenever I am accessing my account, I get a code.
- Blocking some of their accounts or even change the platform
- Encryption of messages being sent, updating passwords for online accounts, backing up of data.
- Making backups of data
- ICT specialists are able to increase digital security through various ways like enforcing complicated passwords for the system
- Email notifications, Change of passwords, change of behaviour/operation of my computer or phone, unknown or strange emails or updates in my inbox or social media pages.
- I can repair my phone just in case it developed a mechanical problem
- Encryption tools

4.5 Capacity to detect digital threats and secure online communication

During the study, respondents were also asked if they had the capacity to detect when their digital security was being breached. Majority of the respondents (63%) said that they do not have the capacity.



Additionally, majority of the respondents (52%) said that they have the necessary skills and tools to secure their online communication.

Among the skills and tools mentioned include;

- Backing up my data and changing passwords
- Changing passwords for my computer and for social media platforms as well.
- I use VPN browser
- The primary skills I have are installing anti-virus on my computer to detect and block viruses and change of passwords.
- I log out my accounts whenever I finish accessing my social media and emails to avoid imposters and I also use Virtual Private Network to safely access internet last but not least I usually change my passwords.
- I use stronger and secure passwords
- Securing emails through use of various methods like thunderbird, encrypting data, setting up strong and secure passwords, etc.
- We have CCTV Cameras, but this is useful after danger to identify who the culprit was, but cannot detect danger to safeguard
- Encryption of messages being sent, updating passwords for online accounts, backing up of data. Etc.
- Backups, I employ 2-step verification in case of Gmail account
- We use Safe Folder Guard (Software) to protect our information.
- "Two step verification on Emails.
- Security changes on phone or encryption."
- "Change passwords often
- Do not respond to anonymous callers"

In term of regional distribution of self-reported skills and tools, a slight majority of respondents in the Eastern (54%), Karamoja at 53%, and Western at 57% reported having the skills while in the Northern region, 51% of the respondents said that they don't have the skills and tools needed to secure their online communication. In the Central, there was a split among those who reported possessing the skills and tools with those who don't.

Distribution of possession of skills and tools by region

Region	No	Yes	Total (n)
Central	50.0	50.0	24
Eastern	45.8	54.2	24
Karamoja	47.2	52.8	36
Northern	51.3	48.7	39
Western	43.3	56.7	30
Total	47.7	52.3	153

In terms of age distribution, the majority of respondents aged 20-30 (52%) and 41-50 (54%) reported lacking the skills and tools needed to deal with the digital threats, while for the rest of the age groups, the majority of the respondents said that they possess the necessary skills and tools.

Distribution of possession of skills and tools by age

Age group	No	Yes	Total (n)
19 and below	0.0	100.0	1
20-30	52.2	47.8	67
31-40	44.6	55.4	65
41-50	53.8	46.2	13
51-Above	28.6	71.4	7
Total	47.7	52.3	153

Distribution of possession of skills and tools by profession

Primary occupation	No	Yes	Total
Human Rights Activist	45.1	54.9	71
Human Rights Lawyer	42.9	57.1	7
Journalist/Media	50.7	49.3	75
Total	47.7	52.3	153

Among the strategies used by the respondents to secure their online communication included;

- Backing up my data and changing passwords
- Changing passwords for my computer and for social media platforms as well.
- I use VPN browser
- The primary skills I have are installing anti-virus on my computer to detect and block viruses and change of passwords.
- I log out my accounts whenever I finish accessing my social media and emails to avoid imposters and I also use Virtual Private Network to safely access internet last but not least I usually change my passwords.
- I use stronger and secure passwords
- Securing emails through use of various methods like thunder bud, encrypting data, setting up strong and secure passwords, etc.
- Using Proper Grammar.
- We have CCTV Cameras, but this is useful after danger to identify who the culprit was, but cannot detect danger to safeguard
- Encryption of messages being sent, updating passwords for online accounts, backing up of data. Etc.
- Backups, I employ 2-step verification in case of Gmail account
- We use Safe Folder Guard (Software) to protect our information.
- "Two step verification on Emails.
- Security changes on phone or encryption."
- "Change passwords often
- Do not respond to anonymous callers"

4.6 Lack of organizational digital safety and security plan

Respondents were also asked if their organizations had a digital and security plan/policy in place in case they or their colleagues were faced with any danger. The majority of the respondents (84%), said that their organizations did not have such a plan or policy.

In terms of regional distribution, majority of respondents from all the regions said that their organizations do not have a digital safety and security plan/policy to activate in case of danger.

Distribution of existence of digital safety and security plan/policy by region

Region	No	Yes	Total (n)
Central	100.0	0.0	24
Eastern	87.5	12.5	24
Karamoja	88.9	11.1	36
Northern	71.8	28.2	39
Western	76.7	23.3	30
Total	83.7	16.3	153

The trend was the same when the respondents were disaggregated by profession, with all the human rights lawyers reporting a lack of a digital safety and security plan.

Distribution of existence of digital safety and security plan/policy by profession

Primary occupation	No	Yes	Total (n)
Human Rights Activist	80.3	19.7	71
Human Rights Lawyer	100.0	0.0	7
Journalist/Media	85.3	14.7	75
Total	83.7	16.3	153

5.0 CONCLUSIONS

From the findings, it is clear that majority of the HRDs are ill equipped to deal with the rampant digital threats and online surveillance cases that both the state and non-state actors subject them to regularly. The majority of the respondents noted that the threats are related to their work as human rights defenders.

Across all the regions, there was consensus that HRDs face all sorts of digital threats including online surveillance. And probably because of the nature of their work, the majority of the human rights activists and lawyers reported having experienced more digital threats than their counterparts the journalists.

The impact of these threats has been felt more by the journalists and human rights lawyers with majority of respondents in these two categories saying so. On the other hand, fewer human rights activists reported being affected (life and work) by the threats.

Also, because of the threats, 83% of the respondents reported that they have changed the way they approach their work and life as human rights defenders.

"Unless I know you well, I may not give you information about me and the organization and restrict your access to my contacts and emails," explains a female human rights activist from West Nile.

"I have no privacy yet I would want to go about my work privately," explains another human right activist from Western Uganda.

"Unless I know you well, I may not give you information about me and the organization and restrict your access to my contacts and emails,"

At an organizational level, the majority of the respondents (84%) noted that they do not have a digital safety and security plan/policy in place when faced with danger. This is a very big number and it is concerning because in most cases, it is the organizations that provide a safety net for the individual HRDs. Without organizational policies in place, many HRDs are further exposed to danger and become vulnerable when attacked or threatened.

6.0 RECOMMENDATIONS

To the Government

The government should amend retrogressive laws and policies, such as the Regulations of Interception of Communications Act 2010, and the Anti-Terrorism Act 2002, that give broad powers for the interception of communication and surveillance, because these are open to abuse.

The government should expedite the passage of the Privacy and Data Protection Bill, 2015 to guarantee the right to peoples' privacy and their data.

Human Rights CSOs

Civil society should also seek to empower HRDs with the necessary tools, knowledge and skills to reduce their vulnerability to digital threats, including online surveillance in the course of their work.

Civil society working with HRDs, including the media should advocate and demand for the repeal and annulment of retrogressive laws and policies that legalize online surveillance and interception of communication

Civil society organizations should urgently consider putting in place security plan/policy to secure activists inline of duty.

7.0 ANNEX: INTERVIEW GUIDE FOR KEY INFORMANTS

Dear respondent,

Thank you for accepting to participate in this study, commissioned by the Unwanted Witness. The study seeks to establish the perceptions, the types and knowledge level of the digital threats and online surveillance among Human Rights Defenders in Uganda.

Participation in this study is voluntary. You have a choice to opt out of the interview at any point. The information you provide will be kept confidential and will not be shared with anyone other than the research team and Unwanted Witness. We therefore request that you feel free to provide frank and honest answers.

Preliminary

Gender: M (____) F (_____)
District/Region: _____/_____
Age Group:
19 and below (__)
20 – 30 (__)
31 – 40 (__)
41 – 50 (__)
51 – Above (__)

Primary Occupation:
Journalist/Media (____)
Human Rights Activist (____)
Human Rights Lawyer (____)

Experience as a HRD

1 – 3 years (___)

4 – 6 years (___)

7 – 10 years (___)

More than 10 years (___)

Section A: Knowledge and perceptions of digital threats and online surveillance

Do you think HRDs in Uganda face any digital threats, including online surveillance?

Yes		No	

If yes, what kind of threats? _____

_____

Have you ever experienced any digital risks and threats and online surveillance?

Yes		No	

If yes, do you think these threats and online surveillance were related to your work as an HRD, or they are random? Please explain

_____

_____

If yes, what kind of threats do you normally face? List as many as you can remember.

_____

_____

What strategies does the government use to conduct online surveillance on HRDs?

_____

_____

Section B: Type and level of impact of digital threats and online surveillance on HRDs

Have these threats and online surveillance affected your work and life as an HRD?

Yes		No	

If yes, please explain how? _____

_____

Have you changed the way you work and relate with others due to digital threats?

_____

_____

Section C: Existing strategies used by HRDs to circumvent and mitigate digital threats

Do you think HRDs have the technical expertise to deal with the digital threats that they face? Are you able to detect or suspected when your digital security has been breached?

Yes		No	

If yes, please explain how? _____

Do you have any skills and tools on how to secure your online communication?

Yes		No	

If yes, please explain some of the strategies/skills you employ

Do you or your organization have a digital safety and security plan/policy in place if you or your colleagues are in danger?
000000

Yes		No	

If yes, kindly explain what you mean?

If yes, do you think these safety measures are sufficient?

Yes		No	

IfNo,howcantheybebeefedup/enhanced?

Do you make backups of your data?

Yes		No	

How often to do you change your passwords?

Daily

Weekly

Monthly

After three months

Annually

Never

Do you know any organisations (national and international) that support HRDs facing threats and attacks because of their work?

Yes		No	

If yes, which organisations do you know?_____

Section D: Innovative strategies for HRDs

If you are offered an opportunity for training in digital security and protection, what kind of tools skills would you need?

_____

_____

Do you have any additional comments?

_____

_____

Thank you

Block 381, Plot No. 26, Nsibambi village
P.O.Box 71314 Clock Tower K'la
Tel: +256 414 697635
Email: info@unwantedwitness.or.ug
Unwantedwitness-Uganda
@unwantedwitness
unwantedwitness