ONLINE SURVEILLANCE AND FREEDOM OF EXPRESSION IN KENYA

BY

MEDIKA MEDI

K50/12242/2018

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF MASTER OF ARTS IN COMMUNICATION STUDIES, SCHOOL OF JOURNALISM AND MASS COMMUNICATION, UNIVERSITY OF NAIROBI

AUGUST, 2021

DECLARATION

Declaration by the Candidate

This research is my original work and to the best of my knowledge has not been presented for an academic award in any other university or Institution.

Signature:  ..... 15TH NOVEMBER 2021

Medika Medi Date

K50/12242/2018

Declaration by the Supervisor

This research project has been submitted for examination with my approval as the University Supervisor.

..... 15/11/2021

Dr. George Gathigi Date

Department of Journalism and Mass Communication

University of Nairobi, Kenya

DEDICATION

This research project is dedicated to my father George Osoreh and mother Nancy Njeri

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATION

ACHPR: African Charter on Human and Peoples' Rights

AI: Artificial Intelligence

CAK: Communication Authority of Kenya

CoK: Constitution of Kenya

DPA: Data Protection Act

FH: Freedom House

GISW: Global Information Society Watch

HRD: Human Rights Defenders

ICCPR: International Covenant on Civil and Political Rights

ICT: Information Communication Technology

IGP: Inspector-General of Police

INCLO: International Network of Civil Liberties Organizations

KNBS: Kenya National Bureau of Statistics

NIS: National Intelligence Service

UPR: Universal Periodic Review

ABSTRACT

Individual privacy is one of the building blocks in exercising freedom of expression in the online and offline space. Lately, findings from Kenya National Bureau of Statistics (KNBS) and Communication Authority of Kenya (CAK) have indicated there has been a sharp increase of online usage and cybercrime. Specifically, unauthorized surveillance which propagates breach of privacy and data mining. Similarly, Privacy International, Article 19 and Defenders Coalition have equally documented the rise of online surveillance which curtails freedom of expression in Kenya. This study investigated the impact of online surveillance on Freedom of Expression as a fundamental right in the Kenyan Constitution. Notably, this study surveyed the technological protection mechanism and predisposed vulnerability of online platforms and inquired about the mechanisms in place to protect freedom of expression online. On methodology, this was purely exploratory study which employed qualitative methods of data collection and analysis while using John Stuart Mill Doctrine of Freedom of Expression (2005) and Erving Goffman Frame Analysis (1974) as grounding theoretical framework. The research has taken into consideration all the ethical research concerns from validity of the methodology to data analysis, voluntary participation and respect for anonymity and confidentiality. According to the findings, there is widespread surveillance of personal interactive sites and internet-connected devices in Kenya. This is done while most Kenyans are unaware their data is being mined and sold without their consent. No one's privacy should be violated indiscriminately. Based on the findings, the research recommends that protective and progressive laws are essential. Lastly, while the laws are being enforced and legislated, they should not be applied selectively; they must be consistent across the board, including citizens and elected officials.

CHAPTER ONE

INTRODUCTION

1.1 Online Surveillance

Surveillance refers to the process of observing a person, group, place or an ongoing activity continuously with the aim of gathering information. In Kenya, any form of surveillance is treated as breach of privacy rights as captured under International instruments and Treaties that Kenya is a signatory to. The International Covenant on Civil and Political Rights under Article 17 seeks to protect citizens of its member states from any unwarranted surveillance; Article 17. (1.) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2.) Everyone has the right to the protection of the law against such interference or attacks.

Meanwhile Section 15 (1) of the Kenya Information and Communications stipulates, "Subject to the provisions of the Act or any other written law, a licensee shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data." Despite these laws, governments around the world have been seen to increasingly purchase sophisticated equipment for monitoring online behaviour of citizens. Such general surveillance is currently prevalent in many countries both powerful authoritarians and less powerful or developing states like Kenya to track dissident voices (Freedom House, 2019).

The aspect of privacy supports and reinforces the freedom of expression as right as has been captured under the Bill of rights, chapter four of the Kenyan constitution. Therefore, aspects in the "private sphere" when forcefully taken away then it affects other

fundamentals rights like freedom of association. The free will of communicating freely is affected or taken away. It is widely recognized that the democracy of a society has freedom of expression as a major cornerstone. This enables citizens to freely "organize, participate as well as communicate" in the absence of arbitrary intrusion. Therefore, any form of surveillance is taking or denying citizens this rights way

1.2 Nexus between Online Surveillance and Freedom of Expression

The tool that plays a fundamental role in conducting online surveillance is Artificial Intelligence (AI). A computer algorithm that performs calculations, applies knowledge and improves productivity through the access of electronic data and surveillance of real aspects of life. Artificial intelligence is developed through computer coding process with an aim to solve and simplify a complex operation to simple through learning on provided data or permitted surveillance. (Global Information Society Watch, 2019).

Therefore, so long as the consumer is using artificial intelligence driven platforms then the algorithm has a significant function in determining limitations to online freedom of expression. Kenyans express this freedom online through the culture of sharing videos, text and sound files via interactive applications such as Zoom, Skype, Google meet, YouTube, Microsoft office, Google search engine, Facebook, Twitter, LinkedIn, Instagram and WhatsApp respectively. These applications are predominantly installed in computers which run on windows operating system, Imac Operating system and android operating system which runs on laptops and cellphones electronic gadgets. Using this platform means one's location, movement, browsing data history and bio data can be accessed lawfully or unlawfully.

Kenya has made significant strides towards strengthening and protecting its citizens against surveillance. However, issues have emerged around various policies and

practices like the Tourism Prevention Act, 2012 as well as online regulations that give telecommunication and government agencies far-reaching capabilities in conducting mass surveillance.

1.3 Problem Statement

In Kenya, communication professionals rely mostly on telecommunications gadgets in the process of receiving and reporting news. However, there is a high level of uncertainties on how private and secure the conversation is even though the laws in Kenya protect individual privacy. There is always a possibility that individual communications may be intercepted or surveilled. This high level of discordance of the online users' need to communicate and the fears and concerns of surveillance are a phenomenon that needs to be interrogated deeply and addressed. The study assessed online surveillance, looking at its impact on Freedom of Expression in Kenya.

1.4 Research Objectives

The overall objective was to explore the impact of online surveillance on freedom of expression. This will be achieved through two sub-objectives which are:

1. Asses the exposure of online surveillance and its impact on freedom of expression
2. To identify measures to prevent online surveillance and protect freedom of expression online.
3. To explore the limits of oversight institutions in maintaining law and order online

1.5 Research Questions

This study was guided by three broad research questions:

1. What is the level of online surveillance that majority of Kenyans are exposed to?

2. What are current legal and technological frameworks being used to govern freedom of expression online and privacy?
3. What are the permissible and limits of oversight institutions in Kenya maintaining law and order online?

1.6 Rationale

The research findings reveal the extent to which online surveillance is being conducted in Kenya and how it's effecting freedom of expression online. The findings are important to communication professionals, especially journalists' understanding of the environment on which they are working. Further, it in turn adds more evidence on existing knowledge and offer clarity on issues of surveillance, data mining, invasion of privacy, the level of cybersecurity which are key determinants on media freedom online and offline. It is cognizant that Artificial Intelligence is the current nerve of new media technologies, search engines, facial recognition, digital identity, users' behaviour and the upcoming self-driven telecommunications gadgets like surveillance drones. However, little is known about the limitation of the Artificial Intelligence online surveillance functionality. Therefore, the findings act as an auxiliary on existing gaps and device proper mechanism and frameworks to facilitate freedom of expression online being driven by integrity, accountability, and transparency.

1.7 Significance of the Study

This study sought to further elaborate how secure and safe the online platforms are in Kenya while one is exercising freedom of expression. This has a direct impact on journalists, communications professionals and most importantly media autonomy which enhances its societal role as the watchdog.

1.8 Scope and Limitation

The study population were avid online users like journalists, developers of online applications, state and non-state oversight actors of online platforms within Nairobi, Kenya. The research only focused on participants who use English as their main language of communication.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

The section reviewed the status alongside the laws on Freedom of expression within Africa, in Kenya and the rest of the world. Further it examined the laws that are enablers of this fundamental right as stipulated in Kenya's Constitution and its operational framework. The chapter also elaborated on the protection of this freedom and legal parameters set out on exercising this right online. Thereafter it established the pros and cons of exercising this right online.

2.2 Freedom of Expression

The ICCPR, Article 19 guarantees everyone the rights to seeking, receiving, and conveying ideas and information irrespective of boarders whether verbal, written or print, in art form, or any chosen means. Individuals as well as groups have rights to engage in or participate in choices that influence their life as a result of this right. It is acknowledged as an essential right and a crucial instrument to uphold the rule of law, combat corruption, while protecting other global rights. This right to information has long been recognized as a critical component of long-term development.

2.3 Surveillance

Surveillance is the close monitoring of suspects undertaken by law enforcement when investigating crimes. Surveillance as described in Oxford dictionary, refers to careful watching of a place or person often by the police due to an established crime or expected crime. Firms involved in surveillance provide technology to law enforcement and intelligence agencies. These can be technologies that aid in the process of Lawful or

Unlawful Interception, offered to operators for compliance purposes, or marketed directly to government agencies to provide more broad-scale, untargeted, and invasive capabilities. The figure below illustrates the type of actors involved in acts of surveillance.

Figure 1: Overview of actors involved in surveillance architecture

Industry actors involved in surveillance architecture

Actor	Technology/Services	Example
ISPs/Telecommunications Operator	Internet and telephone services. Either government-owned or private with diverse shareholders	AT&T, Vodafone, Comcast, Orange, Telecom Egypt, Uzbektelecom
Submarine cable providers	Submarine cable operators / Landing points operators. Generally financed by consortia of operators	TATA-3, China Unicom, Hibernia, Level 3, Atlantic Crossing, Huawei Marine
Telecommunications Network Equipment Vendors	Standard network nodes such as switches and gateways, some of which are designed to be capable of interception, or designed for network monitoring	Ericsson, Nokia, Huawei, ZTE, Cisco, Bluecoat
Surveillance companies	Surveillance technologies sold exclusively to government agencies or telecommunications companies for government purposes	Verint, NICE Systems, Qosmos, Trovicor, Hacking Team, NeoSoft, VasTech, Palantir
Contractors & PMSCs	Consulting and staff	Booz Allen Hamilton, BAE, SAIC, Chertoff Group, ManTech
Distributors	Partners and resellers of surveillance technologies	Elamen, Ezzy Group

Source: The Global Expansion of Artificial Intelligence Surveillance by Privacy International.

Technology can and should play a significant role in allowing people to express themselves freely without violating the rights of individuals or organizations. However, with the passage of time, we have witnessed the deployment of different types of surveillance, which has limited the enjoyment of freedom of expression. Some of these type of surveillance include what has been captured by the figure below:

Figure 2: Types of surveillance technology

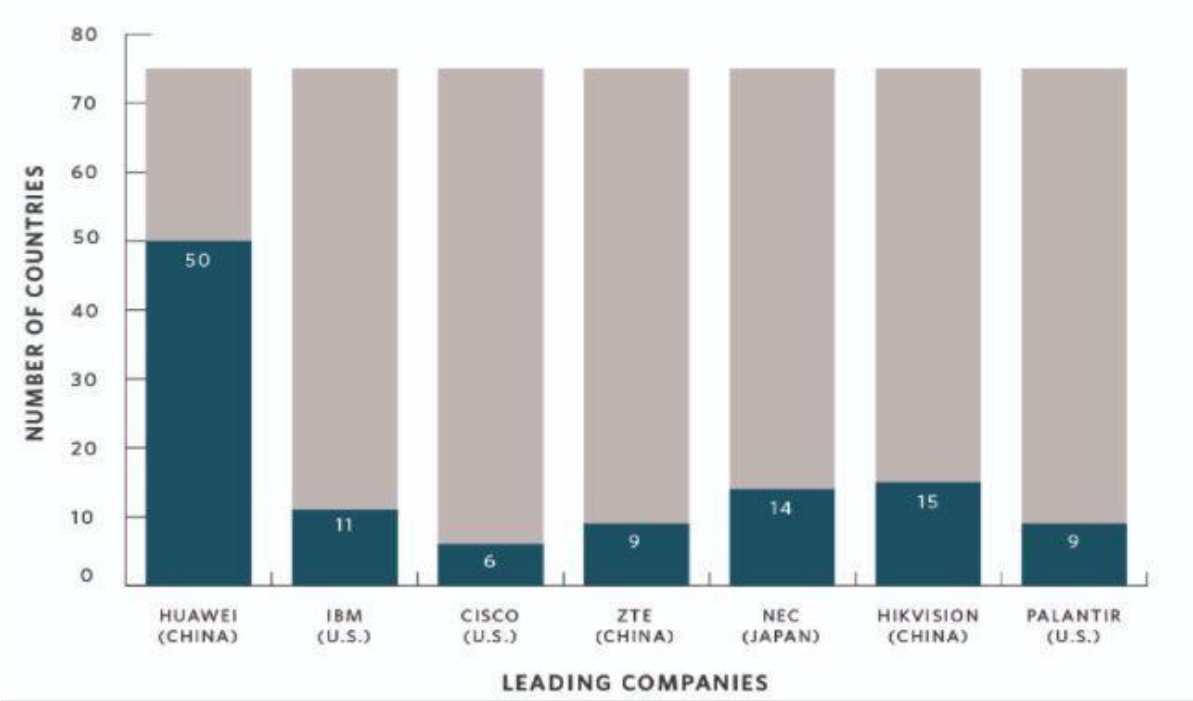
Source: The Global Expansion of AI Surveillance by Privacy International.

Analysis is a form of surveillance that establishes patterns and meanings on the collected data. This type of surveillance is mostly aided by both humans and automated software. Further, when spyware is installed on a communication device to extract data or control a specific function of the device, this is referred to as intrusion. One form of surveillance that is dominant when you are installing new application in your personal phone. While for phone monitoring is a type of surveillance in which the communication between two devices is monitored and documented. The communications is mostly intercepted between the networks of the two phones using specialized device. Another predominant type of surveillance is the location monitoring where they use Global Positioning System (GPS). A navigation system that harmonizes position, velocity and

time data for sea, air and land travel using satellites, a receiver and algorithms. While for Internet monitoring is when the Internet Service Providers, internet users and software developers screens the behavior pattern of the persons using the internet platform. The monitoring center encompasses all forms of surveillance into one hub. This is a center where the operations and supervision of all types of surveillance happens. Using biometric data is one of the analysis monitoring technic. To break it down, biometric refers to the Individuals' bodily and behavioral characteristics are described by the term 'biometrics.' This includes voice, fingerprints, retina, face and iris patterns, hand geometry or DNA profiles. Globally nations use biometrics in a diversity of applications, including national ID schemes border control and voter registration. Biometrics are also used in humanitarian and development initiatives like immigrant registration, as well as by private companies like banks. Counter surveillance is reacting to an identified surveillance as form of deterrence most of this actions are done by governments and conglomerates who have ecosystems and resources necessary for such actions as technique to access or collect information termed as intelligence.

Surveillance, by definition, intrudes on people's privacy. In particular, it has an impact on individuals since it combines both digital and physical monitoring of persons in order to track their actions.

Figure 3: Leading companies contributing to Surveillance



Source: The Global Expansion of AI Surveillance by Carnegie.

China is a big promoter of surveillance techniques for spying across the world. Mass surveillance related to Chinese corporations, mainly Huawei, Hikvision, Dahua, and ZTE, is available in 63 nations, 36 of these nations are part of the Chinese Belt and Road Initiative. There is no other firm that comes close to Huawei in providing Artificial Intelligence to governments across the world with NEC Corporation of Japan being the second biggest. To entice governments to buy Chinese equipment, Chinese product offers are sometimes backed with attractive loans. These strategies are especially important in nations such as Kenya, Mongolia, Uganda, and Uzbekistan, where this technology would otherwise be unavailable. This raises serious concerns on subsidization on procurement of modern restrictive equipment by the government of China.

Liberal democratic countries use artificial intelligence capabilities for surveillance more aggressively than authoritarian governments to patrol borders, catch prospective lawbreakers, keep track of individual conduct, as well as dealing with terrorism. This does not automatically imply abuse of these capabilities rather, quality of governance is the most crucial element in deciding whether governments would use this technology for oppressive reasons. This ought-to give some confidence to those living in democratic states.

2.4 The State of Freedom of Expression in the World

The COVID-19 pandemic emerged when there was already a lot of restrictions and denunciation of opposing voices. Many governments throughout the world have exploited the health issue as a justification to further restrict offline and online freedom of speech.

Figure 4: Progress on the Right to Information globally

Source: The Global Expression Report 2019/2020

Globally, there is a reduction in freedom of speech and expression. Over 3.9 billion people in the world reside in nations where free speech is threatened, the greatest number to be recorded. According to Global Expression (2021) Report's metric, countries with higher population density are falling towards crisis and authoritarianism against freedom of expression. These are frequently also countries classified as crisis countries such as China with 1.4 billion people, India with 1.4 billion people, Bangladesh with 163 million people, Russia with 144 million people and Turkey with 83 million people having economical, political and power within and beyond their boarders. Media landscapes that are free, pluralistic, and diversified allow journalists to critically check on public and private powers, which helps citizens to stay enlightened thus active within the community

In 2019, there were two hundred and thirteen shutdown of internet within thirty-three nations, which translates into 1,706 days without Internet connectivity, compared to 188 shutdowns in 2019. In India alone, there were 121 occurrences. This is according to the Global Expression Report's metric. During these shutdowns it was difficult for the media and activists of human rights to monitor and consequently report on national conditions. In India, this led to significant breech of both international humanitarian and human rights regulations where citizens were also denied access to critical information.

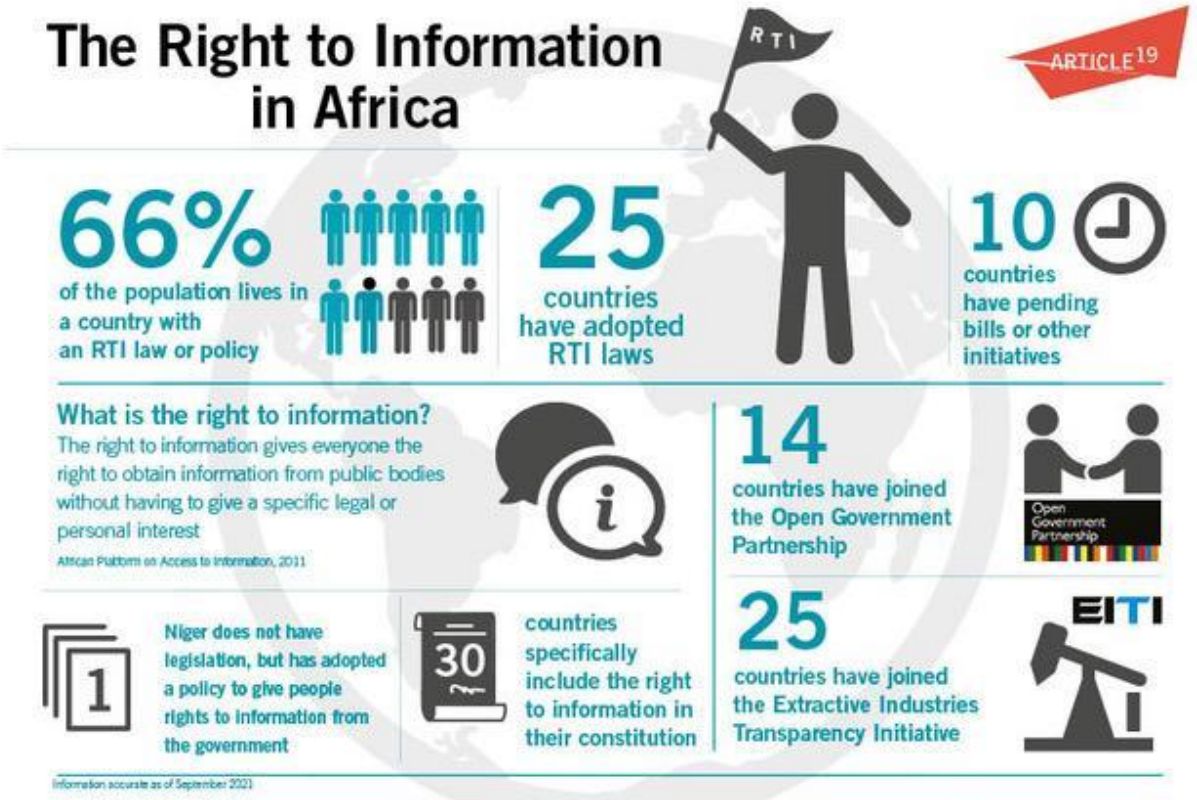
2.5 Freedom of Expression in Africa

2.5.1 Status of freedom of Expression in Africa

More than 40% of Africans today reside within nations with limited freedom of speech. Numerous African countries are continuously creating very difficult climate for communication practitioners and citizens to enjoy freedom of expression by deploying various forms of surveillance which helps them to identify the dissent voices. As a result, journalists are constantly threatened as a consequence of their profession, and killings

have been recorded in several African countries (The Global Expression Report 2019/2020).

Figure 5: Status of the Right to information in Africa



Source: The Global Expression Report 2019/2020

In Ghana, a masked gunman assassinated a documentarist journalist by the name Ahmed Hussein- Suale in Accra in January 2019. Top politicians were hostile to Hussein Suale's exposé on corruption in Ghanaian football. In Tanzania, masked gunmen in disguised vehicles kidnapped investigative journalist Eric Kabandera. The Dar es Salaam Special Zone Police eventually confirmed keeping him for the reason of examining his citizenship, which is a regular practice used to block and intimidate government critics. The environment of freedom of expression in Zimbabwe has not changed even with the

departure of Robert Mugabe's from power in 2017. They are still using the old restrictive legislation to conduct surveillance to journalists. Under President Mnangagwa's leadership disguised individuals grabbed six activists days prior to protests, interrogated and tortured, and then abandoned in distant regions. Samantha Kureya, familiar as Gonyeti, faced abduction, undressed, abused, and made to consume sewage water.

Several African nations have recently passed legislation and policies that target and restrict the media, independent journalists, non-governmental organizations and their work which heavily depend on freedom of expression. Some of these nations include Burundi, Tanzania, Uganda, Ethiopia, Sudan, Zambia, Rwanda, South Sudan and Sierra Leone, with more on the way. These measures vary from costly and severe bureaucratic procedures for registration, accessing work permits, ready to accept forms of surveillance, disclosure of source of funds, limiting work zones or permitting state intervention in activities.

2.5.2 Surveillance Laws in Africa

Strengthening technical capacity: Most African countries are continuously strengthening technological capabilities for intercepting and monitoring digital communications in recent years. This has included, along with many other things, the installation of device such as apps which allows remote surveillance, installing video tracking techniques with possibility of recognizing images, imposing mandatory equipment to be obtained by communications firms at their cost having capability of intercepting private conversations and sharing with the state-security bodies.

African nations are building enormous databases containing a variety of personal data, along with biometric data, which are typically connected to State Identity cards, voter identification and individual subscriber identification card information. The information gathering efforts and interconnected information systems has increased the

accuracy by governments in identifying persons, making communication surveillance and tracking target activities simpler.

Imposition of Liability on Intermediaries: In Rwanda; Cameroon; Uganda; Zimbabwe and Zambia telecommunication companies and ISP firms are required to aid in monitoring and tracking by facilitate government surveillance for as long as necessary. Noncompliance with these regulations usually results in harsh consequences. Failure to comply with the need to facilitate interception in Uganda is punishable by a fine of five hundred and eighty-three dollars equivalent of not more than 5-years in prison while Zambia's is six thousand six hundred and forty-three dollars. Cameroonian law contains the same provision. The interception legislation in Zimbabwe has no provision for scrutiny by the judge but rather such powers are conferred on the communications minister.

Procurement and Installation of Surveillance Technology: Studies indicate that several nations have purchased technology that enables governments to listen on personal conversations, access personal telephone conversation data, SMS messages, and GPS services. Kenya among other nations like Zimbabwe, Nigeria, are alleged as among the ones utilizing tracking and monitoring spyware. This is according to the (Circles Report, 2020). The Circles findings come on the footsteps of previous research indicating that African countries were already using spyware, notably that from the NSO Group called Pegasus. The Citizen Lab, a Canadian internet rights organization, stated in September 2018 that it has discovered Pegasus viruses within forty-five nations; Kenya included among other countries like Morocco, Rwanda, Egypt, among the countries represented. Governments regularly utilize Pegasus to monitor journalism and communication professionals, activists and political opponents.

According to reports, officials from Ethiopia actively scouted the European market for modern surveillance technology, purchasing equipment to spy on Ethiopians residing in and outside Ethiopia after 2011. FinSpy technology, was procured from a company based in the United Kingdom. Human rights activists and journalists in Chad reported being given a report detailing all of their personal phone calls and SMS messages after being detained. According to an Amnesty International (2020-2121) investigation, commercial telecommunications firms in Chad admitted eavesdropping and phone monitoring techniques, claiming that the government justified it for national security concerns.

Collection of Biometric Data, including Subscriber Identification Module, Card Registration: Personalized data gathering, processing, and dissemination greatly aids in identifying monitoring targets citizens as well as actual monitoring. In numerous countries, the requirement for collecting wide range of customers' data is mandated by law. Judging by the amount of personal data acquired, maintained and disseminated, lack of proper monitoring systems has severely harmed citizens' capacity to interact and enjoy their freedom of expression. Concerns regarding the abuse of information, improper implementation of rules and flaws in control of communication interception legislation have been amplified.

2.6 Freedom of Expression in Kenya

Articles 33, 34, and 35 of the Constitution of Kenya, 2010 guarantee, respectively, freedom of expression, freedom of the media, and freedom of access to information. Further, it is worth noting political and regulatory frameworks have a considerable influence on media firms' organizational survival. The media rely on existing laws that safeguard freedom of speech in order to perform their watchdog duty of educating citizens. When the rule of law is recognized and maintained, it allows the public freedom

of expression. According to World Justice Project (2020) Kenya has a Rule of Law Index score of 0.45 with the minimum being 0 and maximum being 1. Freedom House classified it as partially free with a score of forty-eight out of one hundred (Freedom House, 2019). Pervasive corruption and violence by security personnel gravely impair political rights and civil liberties, and media personnel and activists endure restricting legislation and threats.

The freedom of expression is guaranteed under Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR) which provides that "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." (2011)

In 2011, the Human Rights Committee established under the ICCPR, issued a General Comment on Article 19 which expounded on the scope of the freedom of opinion and freedom of expression. It stated that freedom of expression includes the freedom to express oneself in political discourse, commentary on one's own and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, religious discourse, commercial advertising. The Committee clarified that the scope of Article 19 (2) of the Covenant includes expression that may be regarded as deeply offensive provided that it is within the limits of Article 19 (3) and 20, "The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals." and Article 20 (1), Any propaganda for war shall be prohibited by law. (2) Any advocacy of national, racial or religious hatred

that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

The Committee also pointed out that Article 19(2) protects all forms of expression and the means of their dissemination, which expression includes spoken, written and sign language and such non-verbal expressions as images and objects of art. These include books, newspapers, pamphlets, posters, banners, dress, legal submissions. They also include all forms of audio-visual as well as electronic and internet-based modes of expression. The Committee also extensively elaborated on the interplay between freedom of expression and the media; freedom of expression and political rights; the right to access information and the parameters within which freedom of expression may be restricted; and the relationship between article 19 and 20 of the Covenant. These standards set by the Human Rights Committee shall inform the basis on which Kenyan legislation is analyzed herein.

At the regional level, freedom of expression is guaranteed under Article 9 of the African Charter on Human and Peoples' Rights (ACHPR) which provides protective measures for citizens. "Every individual shall have the right to receive information (2.) Every individual shall have the right to express and disseminate his opinions within the law. Article 9 of ACHPR (1986)

Kenya has domesticated the international and regional standards on the right to freedom of expression in the Constitution and various legislation. The Constitution guarantees the right to freedom of expression, freedom of the media and the right to access information. The right to freedom of expression is guaranteed under Article 33 which provides that "*(1) Every person has the right to freedom of expression, which includes (a) freedom to seek, receive or impart information or ideas; (b) freedom of*

artistic creativity; and (c) academic freedom and freedom of scientific research."
Constitution of Kenya (2010)

Article 34 of the Constitution guarantees the freedom of electronic, print and all other types of media. It bars the state from exercising control over or interfering with any person engaged in broadcasting, the production or circulation of any publication or the dissemination of information by any medium; or penalizing any person for any opinion or view or the content of any broadcast, publication or dissemination. It also guarantees the freedom of establishment of broadcasting and other electronic media subject to licensing procedures that are necessary to regulate the airwaves and other forms of signal distribution; and independent of control by government, political or commercial interests. Further, it provides that state-owned media must be free to determine the editorial content of their broadcasts or other communications independently; be impartial; and afford fair opportunity for the presentation of divergent views and dissenting opinions.

Article 35 of the Constitution provides that every citizen has the right of access to information held by the State or information held by another person that is required for the exercise or protection of any right or fundamental freedom. It also provides that every person has the right to the correction or deletion of untrue or misleading information that affects the person. Further, it makes it mandatory for the state to publish and publicize any important information affecting the nation. These provisions of the Constitution give effect to the provisions of Article 19 and 20 of the ICCPR; the General Comment on Article 19; and Article 9 of the African Charter on Human and Peoples' Rights.

2.7 Protection of Information and Communication in Kenya

During the 2017 election, there was an outrage on the misuse of personal data for political campaigning. This led to renewed advocacy for a protection framework that came to give birth to the Computer Misuse and Cybercrimes Act, 2018 and The Data

Protection Act, 2019. Cybercrimes Act, 2018 prohibits phishing, where it makes it a punishable act to create or operate a website or send a message through a computer system with the intention to induce the user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system. Whereas the Data Protection Act, 2019 came into force later in the year, the Act gives effect to the constitutional protection on privacy. The Act takes a principles based model as opposed to rules. It provides the overarching principles under which data processing should take place as well as mechanisms to encourage compliance with the principles. The law also includes criminal offenses and penalties for non-compliance with the compliance aspects such as false reporting of activities, processing without consent, non-compliance to a notice issued by the Commissioner. Unlawful disclosure of personal data or offer to sell such data is also a criminal offense. At the same time, any person can make a complaint to the data processing commissioner on data processing activities.

2.8 The nexus between Freedom of Expression and Online Surveillance

In Kenya, connection between Internet surveillance and freedom of speech is perceived to come in when the enforcers will site the legal limit of freedom of expression and alleged accusation or matter being investigated. However, it should be noted the laws in Kenya don't expressively permit the enforcers or security operators to conduct online surveillance.

Additionally, some of the laws have been used before as a gateway to justify online surveillance. These laws include *National Intelligence Service Act, 2012* where one major article on this law that is used ambiguously as justification to conduct online surveillance if security or enforcers are taken to court is that it was for national interest. *Prevention against Terrorism Act, (2012)* is another law that is perceived to give the

security actor's leeway to conduct online surveillance. Thirdly, *Preservation of Public Security Act, (1960)* is law that security operations can use as a justification for conducting online operations. While it is essential for the dissemination of false reports to be prohibited and controlled, the rest of this provision gives room for a blanket limitation of the rights to information and speech.

The International Covenant on Civil and Political Rights permits limitation of the freedom of expression and freedom of information by law when it is necessary for the respect of the rights or reputation of others and the protection of national security, public order, public health and public morals. The African Charter on Human and Peoples' Rights sets out similar standards. However, it does not provide permission for governments or provide sectors to conduct online surveillance.

The International Network of Civil Liberties Organizations (INCLO) published two reports titled *Spying on Dissent* which focused on surveillance technologies around the world and a second report titled *Surveillance and Democracy*. In these reports the Kenyan government is adversely mentioned in curtailing freedom of expression, an essential attribute on investigative journalism. The findings in these reports indicate that any advocacy or communications in Kenya that seems to undermine the state positions may tend to put under surveillance. The reasons why most investigative stories are not aired and peaceful demonstration even before they begin will be turned violent by National Police Service. In the same manner, fundamental rights and freedoms are also sacrificed.

2.9 The nexus between Freedom of Expression and Online Technologies

The right to freedom of expression may both be exercised online and offline depending on the choice of the user and intent. Nonetheless, the connection of Freedom of Expression and online technologies is mostly embedded on the format of the message

and the nature of technology the center and receiver is predisposed on.The advancement of Artificial Intelligence technology has made it easy for monitoring of online platforms (Freedom House, 2019). Regardless communications process has been immensely made easy and cheap than before. This has been majorly spearheaded by technological advancement which has created multiple platforms from social media to the internet ecosystems. The world has been reduced to a global village. The benefits and challenges of communication technologies on media freedom is both experienced in global context and within the Kenyan boarders.

As seen surveillance, has become a cornerstone of oppressive states around the globe by continually posing selected monitoring for open democratic societies. The essential commitments of due process, transparency and citizen oversight are non longer respected. longer works. This is a result of the new scope and intrusiveness of the surveillance, that's manufactured from breathtaking technological advances which have opened completely new home windows into citizens' sports and personal lives. This exponential enlargement of virtual digital surveillance powers has delivered full-size tension that intelligence accumulating can be harming democracy itself, weakening democratic techniques and establishments in nations in which they're regularly taken for granted, and impeding or undermining the improvement of democratic systems in nations that have best lately emerged from extra authoritarian structures and abusive surveillance regimes.

2.10 Theoretical Framework

The grounding theoretical framework is from the work of John Stuart Mill on Freedom of Expression. Larry (2001). The second theory of Erving *Goffman Frame Analysis (1974). According to* John Stuart Mill the truth exercised through freedom of

expression can be revealed through civic debate, so society in including government should not put a boundary to the practice of free public debate so as not to hinder the realization of the truth. In his view, the spread of untrue opinions should also be endured. He urged that lies compete with the truth, and only through this competition can the truth and values be developed and be defended. Summarily he concludes that Freedom of expression enables people to come to a clear and vivid understanding of the truths about the world.

According to Goffman (1974), a frame is a cultural way of defining realities allowing people to make reasonable understanding of events and objects around them. Framing is mostly influenced by external factors such as social contract, knowledge, and the intention that one needs to communicate. The basis of framing differs from one individual or organization even if the source of data has the same facts. When news or information is presented to every member of the audience it evokes a different type of framing understanding. This type of interpretation of information and having the liberty to frame a new frame is synonymous with exercising freedom of expression in a modern democracy. Therefore, some people in power will be interested in conducting surveillance to know or stop what people want to publish about them knowing if they don't control it anything can be said about them.

Free speech, free debate, diverse perspectives and the negotiation or discussion to agree or free expression are all the major proponents of democracy which majorly is controlled by laws. Therefore, the immediate environment of an organization or an individual determines how framing is formed and interpreted. When a regime is totalitarian then cognitively information consumers and content generators are not as free to form their own liberal frames but coerced to conform within a certain type of framing that the state approves. This means freedom of expression is substantially controlled

through surveillance such as online platforms. When a regime is liberal then the society has a lot of divergent views giving a free pass to citizens to develop their own frames thereby exercising freedom of expression. This research investigated how online surveillance impacts on the framing of messages protected freedom by the Constitution of Kenya.

CHAPTER THREE

METHODOLOGY

3.1 Philosophical paradigm

This research uses pragmatism research philosophy which primarily focuses on facts, results and experience of the phenomenon and therefore the proponents of the research are that knowledge is derived from the experience of online surveillance and freedom of expression from participants. Nonetheless, this philosophy provides the liberty of choosing the best research methodology for collecting and analyzing data.

3.2 Study Design

Exploratory research that employs qualitative methods to collect and analyze data was used in the study (Kothari & Garg, 2019). This research design is appropriate in providing an opportunity for considering different aspects emanating from the problem statement under investigation. Through this design, key forms of online surveillance will correctly establish their relationship with the freedom of expression.

3.3 Study site

The study focus area was on online surveillance and how it promotes or limits freedom of expression. The premise is the correlation between online surveillance and freedom of expression, investigating how online surveillance has become either an enabler or deterrence. Thematic aspect as well as related aspects regarding data protection within online spaces are discussed. The foundation theoretical framework used was framing theory which assisted in defining the role of freedom of expression in facilitating transmission of messages from the sender to the receiver within online communication space. The population sample emanated from journalists, avid users of online space,

software developers and oversight institutions of online spaces based in Nairobi, Kenya. The importance of these population is that they each provide expert diverse view point of freedom of expression and issues of surveillance.

3.4 Research Approach

The study used a qualitative approach in assessing information from journalists, ICT developers and expertise from an oversight institution deemed appropriate in assessing behaviour, attitude and opinions (Kothari & Garg, 2019). Therefore, through qualitative research the findings explain the drivers of certain actions of online surveillance and the effects it predisposes the excessing freedom of expression thematically. Nonetheless, the approach gives a detailed reason as to why surveillance has been used and deemed necessary.

3.5 Research Method

The main methods of data collection included Individual interviews, focused group discussions and secondary content analysis. Individual interviews and focused group discussions were important for this study for the reasons they provided participants to express their own ideas in different situations without subjective limitation. An interviewer was allowed to probe or seek clarity on matters that were of concern and great quantity of data was collected within a short amount of time. Nonetheless, it provided an opportunity of triangulation of information thereby providing an opening to establish the interconnectedness within thematic topics. The research method is as well embracing the grounding theory of framing where participants are given opportunity to provide thematic unlimited information within every thematic topic under discussion. Thereafter secondary content data analysis used to give inferential insights on global norms and practice on the phenomenon under investigation.

3.6 Data needs, types and sources

The data collected from the sample population using Individual interviews and focused group discussions offered Primary data which was qualitative data. Data was also gathered through reading and review of the Constitution of Kenya and relevant laws within the context of surveillance and freedom of expression. This includes but not limited to communication regional treaties, minutes from meetings, surveys, letters, contracts, reports, emails, strategies, and newsletters.

3.7 Population, sampling procedure and Data collection

A non-probability process called purposive sampling was employed to draw the sample from the target population. The sampling criteria was driven by the annexation of knowledge within the field of study and recognition of the variables within the research topic. This includes the thematic area of surveillance, online users and freedom of expression.

Selection of target population was informed by research objectives and questions as captured in chapter one which generated the following qualifications criteria for the population; should be an active user in collecting, sharing and disseminating information. Should be knowledgeable and experienced on Information Communication Technology (ICT) and have technical skills in development, and operation of online applications. Work with a constitution mandated organization with mandate to oversight the use operation of media on ICT and AI platforms.

The sampling size was 10 participants which was informed by (Creswell, 2007) recommendations. Creswell (2007) proposed 3–5 participants for a case study, 10 for a phenomenological study and 15–20 for grounded theory study. The justification for using 10 participants was because this size is suitable to achieve a meaningful data with richness that is essential for in-depth and significant analysis.

3.8 Data Analysis and Presentation

The research used a triangulation approach to analyze the data thematically (Braun & Clarke, 2006). The steps on data analysis is as follows: The transcript data collected from the focused group discussions and informant interviews was categorized thematically to offer a description of what freedom of expression online is and issues of surveillance emanating from the target population; assessment on similarities and divergence on major and minor thematic issues, this was done through triangulation using research questions as a guiding formula; the major thematic issues are evaluated against the problem statement and ascertain if some categories can be merged to minimize sub-categories while focusing on research objective; validation of the data analyzed.

The final analyzed information was compared with what is on original transcripts to ensure coherency and veracity; summarily, the data from journalists, ICT developers and experts from oversight institution was examined in depth through correlations. Journalist findings on exercising freedom of expression online was matched with the findings emanating from the ICT developers and oversight expert on what mitigation mechanism by law and by technical operations that have been adopted to secure communication process within online spaces. The analysis from this comparison was thereafter put in a litmus test by finding out on any connections with best required standards.

In presenting the findings, each thematic analysis had a conclusion. The analysis results were supported by data from document analyzed as drawn from the master transcript. Representative quotes were also used to present excerpts that provide the closest representation of the findings. Lastly, the research conclusion and recommendation were presented using themes obtained from the analysis of the

information obtained from document analysis, focus group discussions as well as interviews.

3.9 Ethical Considerations

The research aimed to ensure the findings are universally accepted while protecting privacy rights of every participant of this research. Nonetheless, the research notes the topic under investigation is a security concern therefore ethical concerns are of best importance when collecting, analyzing data and presenting the findings, (Bryman & Bell, 2007). As such, the researcher ensured there was a deliberate consistent correlation of research topic, objective, questions, data analysis and conclusions throughout. Additionally, all the shortcomings of the research were documented and reported. Individual participation in interviews and focused group discussion was based on voluntary basis only and their expressive consent and making sure anonymity was adhered. The Consent Form annexed was shared with the participants in an effort to demonstrate the researcher commitment and knowledge on ethical consideration.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

Analysis of data alongside discussion of findings are presented in this chapter. Interviews and focused group discussions were conducted online utilizing zoom and Google Meet as a result of Covid-19 and in accordance with government-mandated mitigating measures. The interview guide in the appendix was used to acquire the primary data. The findings are interpreted and discussed in connection to the study objectives in this chapter.

4.2 Online Surveillance

In light of this, interviewees were asked how online surveillance is carried out and who are the more prominent perpetrators of online surveillance in online spaces. The investigation discovered that obtaining a cell phone number is all that is required to monitor it. It was also discovered that international corporations who have made significant investments in ICT, technologists, mobile lending companies that leverage financial technology, and the government all have a high likelihood or capability of conducting surveillance.

The National Intelligence Service (NIS), which is subject to the least supervision, wields the most monitoring powers inside the government. The Intelligence and Security Committee oversees the National Intelligence System. A nominee of the Kenya National Commission on Human Rights, a lawyer with practicing certificate, senior public servant, a former intelligence officer and a high court judge constitute the Intelligence Service Complaints Board established by the NIS Act, 2012.

The investigations also revealed that, with the approval and cooperation of telecommunications carriers, the police and the National Intelligence Service (NIS) can gain formal access to Kenyans' communications data, allowing it to collect both data and content without the telecoms firms' knowledge. The investigations also reported the existence of undercover NIS operatives in the country's major internet and telecommunication service providers.

The study also revealed that mobile lending businesses monitor registered users' smartphone data in order to create a financial persona for applicants. To make lending judgments, machine learning algorithms examine all data points on a cell phone. M-Pesa transaction SMS, call behaviour, and device details are all included.

According to the data, developers from the commercial sector collaborated with the government to create contact tracing apps that rely on location technology thus making it easier to gather various forms of personal information about people, such as their names, ages, genders, localities, and coronavirus symptoms, among other things. The Jitenge MoH Kenya app is one of the most popular. Applications for symptom reporting and monitoring as well as contact tracking. This software is intended to supplement the COVID-19 home isolation and care recommendations. Health care workers may keep an eye on these people and send monthly updates to the Jitenge system. County and national fast response teams can obtain these reports. Jitenge app is proven to be in violation of international privacy rules, according to the study.

Cambridge Analytics scandal report could have exposed the cruel reality regarding information security and manipulation of data on interactive sites, however the matter is embedded within the platforms themselves. That is the risk of extracting intelligence from then insignificant data. Several of the capabilities are whole new, hoping on Artificial Intelligence and pattern analytics to map people' relationships "by

hyperlink analysis," attribute that means or angle to social media posts victimization tongue processing, and mine data for info about "past, present or future locations.

4.3 Invasion of Privacy and Data Mining

According to the findings, most Kenyans forget that knowledge is power and will naively click "ok" on privacy regulations to geo-locate where we want to eat and play games with our pals on mobile applications to pass the time. This happens most often when we install apps from the Google Play or App Store. The study was able to distinguish between the four main user roles that might be used to investigate data mining privacy issues, and each user role had its own perspective on the subject.

One of a data provider's (cell phone user's) main concerns was whether he can restrict the sensitivity of the data he is willingly to transmits to others. Primary aim of a data collector is to ensure that the sensitive information gathered is protected and updated without changing its real meaning. The data miner uses artificial intelligence to extract usable information from the data collected by the data collector while maintaining anonymity. The decision-maker is concerned about whether the mining findings are reliable enough for them to make sound decisions.

The study also discovered that in some circumstances, the data provider must choose amid the loss of confidentiality and the advantages of data mining participation. A research or camera shopping website, for example, can provide customized product recommendations to a journalist based on the demographic information and browsing conduct of the user. Although a journalist's personal preferences may be revealed, he will have a better shopping experience. Data provider might be agreeable to offer his personal data to a trustworthy data collector who assures that the provider's personal information will not be divulged to an unauthorized third party in exchange for some benefits, such as tailored service and monetary enticements.

When this study looked at the compliance of Jitenge App contact tracing apps on the Google Play store, it used Exodus Privacy's audit system for Android smartphone application and looked at its terms of reference and permissions. According to the findings, many apps collect extreme extra private data than is essential for their affirmed function.

These treacherous authorizations pose an information security danger since they allow admission to information or data that would then be restricted, such as reserved and possibly sensitive user data like sensitive personal information that includes all government issued identification numbers, such as National Hospital Insurance Fund (NHIF) number National Social Security Fund (NSSF) number and National Identification (ID) number, all financial account information including payment card information and health insurance numbers, individual medical records, genetic and biometric information. Any data taken from an online or offline consumer sample, whether it is externally or internally generated by browsing history such as credit reports and credit history, user accounts information such as username password security questions or answers and other password recovery data, Personal photos, digitized signature, disability information, names of family members, confidential work address, personal certified certificates, location of where you work, and emergency contact information which may not be directly applicable to the fundamental functionality of the application or required by the Kenyan law. They are breaking the data minimization and purpose limitation principles of data privacy regulations by doing so.

This means that in Kenya, telecommunications ecosystems was used to track smartphones of people assumed of having COVID-19 as a way of enforcing a fourteen day mandated segregation or anyone arriving in Kenya through any points of entry, such

as airports, who pledged to self-quarantine in real time. According to other allegations, the National Intelligence Service tracked patients' travels using phone data.

These people were not supposed to turn off their devices, because breaking such official rules could lead to detention in government-run monitoring centers. According to a report released in March 2020, a lady traveling from the United Kingdom to Kenya who violated the self-quarantine mandate by going to work was traced using her phone and hauled away to a government medical institution.

As a consequence, the procedure of using telecommunications ecosystem and information for quarantine surveillance and contact tracing to assist in the monitoring and enforcement of social separation raises serious concerns about privacy and expression rights. Therefore it is serious to guarantee that these practices are implemented with proper safeguards for citizens' rights and that they don't become routine after the COVID-19 crisis has passed.

The above experience indicates that personal information that users freely provide becomes a valuable commodity. Personal data is frequently compared to oil in the sense that "it powers today's most profitable businesses". However, the consumers or internet users who source it frequently have little understanding of how much information is being collected, by who, which type of individuals have access to it, and how much it is worth. Every day, hundreds of companies that the online user may not even be aware of collect data on them, some more intimately than others. This information can then be passed on to academic researchers, hackers, law enforcement agencies, and foreign governments, as well as manufacturing companies attempting to sell something.

The interchange between the information provided and the services received may or may not be worth it, but another industry collects, analyzes, and sells the information without giving anything at all. These companies are termed as data and information

brokers. Sources of information emanates from browsing information, the public online sites the user visits, property registers and legal proceedings. Further, they collect medical records, browsing history, social media connections, and online purchases. Depending on where the online user lives, data brokers can even buy the information from online companies. “Why do you think you have to fill or create an online account of almost all the websites you need a service from?”

The information data collected by brokers or companies that work on analytics may be inaccurate or out of date, however, it can be extraordinarily valuable to businesses, marketers, investors, and individuals. It is estimated that United of America companies alone spent more than 19 billion USD in 2018 gathering and evaluating consumer data, according to (Interactive Advertising Bureau, 2018). Even with the new Data Protection Act of 2019, we still have inadequate laws regulating how social media companies can collect data about their users. This notwithstanding in many cases the Kenyan government can legally request digital data from companies even without a court order.

Scholars from numerous academic disciplines scrutinize social media posts and other user-generated data to learn more about humankind. Davidowitz (2017) contends in his research that Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are Really. For instance, he states, less than twenty percent of individuals acknowledge they watch porn, but there are more Google searches for "porn" than for "weather."

Personal data is also used by artificial intelligence researchers to train their smart algorithms. Every day, billions of videos, photos, audio, and text are uploaded to sites like Facebook, Instagram, TikTok and Twitter by users all over the globe. They are then fed into machine learning algorithms, which can study what to look for in a photo or

automatically determine whether or not a post violates Facebook's hate speech policy. Their selfies literally teach robots new tricks. Congratulations.

4.4 Personal Data Collection in the Future

Nowadays, personal data is mainly collected through screens when people use computers and smartphones. In the near future, new data collection devices such as censored clothing, smart speakers and well-being monitors will become prevalent. Data will likely be collected from things like face-recognition-enabled surveillance cameras mounted in public places. That future has already begun in many ways: Taylor Swift fans have collected facial data, and Amazon echoes can be heard in millions of homes. The decision has not yet been arrived at, though, a way to navigate this new data-crammed reality will need to be made in future. Such questions that consumers will need an answer are: should schools be authorized to digitally track their teenage applicants? Do we really need airport companies and medical insurance agencies tracking our twitter posts? Academicians, state officials, political leaders, artists and parents will reflect on these questions and lots more on the same.

Every year scientists are pushing the boundaries of what is possible with artificial intelligence that are related to surveillance, we should learn to understand personal information that is not even real, at least in the intelligence that it does not come from humans. Artificial Intelligence, for example, are already there producing "forged" information to train other intelligence systems. A technology called deep fake enables hoaxers and propagandists to use interactive sites photographs to create visual and videos depicting events that never happened. Now one can create millions of synthetic faces that do not belong to anyone and alter the meaning of identity stolen. This dishonest data could further misrepresent interactive sites and other parts of the internet leading the user tovtry and find out if there really is a Tinder match or the person they followed on

Facebook. Regardless of whether data is generated by computer systems or by humans, one of the most urgent issues will be how it is analyzed. It is important not only to gather data, but also to draw conclusions and make predictions based on it. Surveillance artificial intelligence uses personal information to make extremely important judgments, such as whether someone should keep their health care benefits or be released on bail. These judgments are easily skewed, and researchers and scientists such as Google are working to make algorithms more transparent and unbiased. Technology companies are also beginning to realize that personal information collected must be regulated. Microsoft has called for federal regulation of face recognition software, while Apple CEO Tim Cook has suggested that the FTC step in and establish a clearinghouse where all data brokers must be registered. However, not all of Big Tech's proclamations may be genuine.

A good number of organizations and researchers argue it is now no longer sufficient for the States to be the only ones to honestly guard private information. Consumers (Data generator) want to have rights to own their statistics and be compensated while it is being used. A good number of organizations pay users in an exchange for sharing statistic specific statistics with them. It’s worth considering that permitting citizens to take returned possession possibly wouldn’t resolve each trouble posed by issues of breach of privacy. It may additionally be the incorrect manner to border the trouble. Scandals have come out in the current years from Google’s shady region monitoring practices according to (The New York Times: Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, 2018). The research verified that online users nonetheless do not understand all the methods how their facts are traded, being sold and shared. Until the New York Times (2014) published its findings about the business of selling psychological profiles of American voters to political campaigns, the largest known leak in Facebook history, acquired the private Facebook data of tens of

millions of users. The allegations concerned Trump Consultants' use of Facebook data. Christopher Wylie, a co-founder of Cambridge Analytica who worked there until 2014, described the company as a "arsenal of weapons."

Perfect security does not exist, and it is impossible to prevent every potential data breach. But how concerned should online users especially journalists or human rights defenders be if their personal data has been stolen or leaked? To answer that question, it is helpful to understand the history of data breaches. With context, consumers can determine whether they need to take additional precautions following a security incident. A new wave of organizations that deal with data and information are marketing a noticeable offer to online users. Their proposal is that the online users including journalists and human rights defenders need to be respected by being given the right to partly own their data and at least get profits out of it through helping marketers. Some of these messages include " Sign up for this kind of apps and the customers will touch you directly, presenting cryptocurrency tokens in trade for records like your financial institution transactions, clinical history, or the fluctuations of your clever thermostat." In summary, lawmakers are grappling with how the future will look like especially with the transparency in algorithmic decision-making which mostly is associated with surveillance. This technology keeps on changing every day at the speed at which the laws are being legislated. Some of these questions are that there isn't a "right to explanation" for how a machine came to a conclusion about your life. Some researchers are conceptualizing what such a right should look like in the future while the Technology agencies around the world also are initiating a conversation on how to gather and use private information needs to be regulated.

4.5 Legal frameworks governing Freedom of Expression Online

The United Nations General Assembly (2013) stated in its resolution 68 that people's rights must be respected online just as they are offline, and it advised nations across the globe to respect freedom of expression and defend the right to confidentiality in digital communication. The Assembly also acknowledged that exercising one's right to personal privacy is critical to realizing one's right to liberty of expression and the ability to exercise one's beliefs without interference and that it is one of the basics of a self-governing civilization.

Privacy guidelines are significant. As a result they define the methods and practices relating to the acquisition and storage of personal information. According to the study's findings a comprehensive data and information protection declaration should contain at least an description of the establishment and application, possible uses of the data collected, the type of information put together, the legal basis for the information collection, how the data is conceded on to third parties, the data to be protected, how the data is going to be used, the duration of the data storage and data theme.

International human rights law provides the collective framework by which any interference with citizens' rights must be measured. The ICCPR states that no citizen may be subjected to arbitrary or unlawful interference with his or her private life, family, home or privacy or unlawful attacks on his honor and reputation. It also states that everyone has the right to legal protection from such interference or attack. The right to privacy is not absolute, any example of interference ought to be prescribed with the aid of using presiding law and which might be essential in a democratic society with inside the pursuits of countrywide protection of public safety. Where such regulations are made, the government ought to display their necessity of reason.

Confidentiality and expression are intertwined in the digital age, and online privacy is a gateway to the safe exercise of freedom of expression. Article 19 of the ICCPR and the Universal Declaration of Human Rights protect all people. The right and limitation to have freedom of expression means the following: Provided by law: Any limit must be precisely worded so that a citizen can adjust their behavior accordingly. The law should be available to the public and it must not be too vague or too broad to allow officials missing using the law. Need and proportionality, the government must bears the burden of proof for a direct and immediate connection between the utterance and the threat. The government must as well demonstrate that the restraint it is seeking is the least preventive option of the scenario in focus. Legitimacy, it must be limited in its application to situations where the interests of the entire nation are at stake.

The Jitenge MoH Kenya Application has no confidentiality policy in Kenya. The Google Play store paper labeled as a "privacy policy" is an essential parameter for program implementers and legislators. The government of Kenya's inability to have a detailed privacy policy for the application prior to data collection and processing shows a violation of data protection laws and principles to guarantee that only authorized individuals have access to personal information and to assess whether protections, such as database security, are in place. Private players built both coronavirus contact tracing apps, which were then deployed in collaboration with both governments. While public-private partnerships are encouraged, there is a necessity to build on the proactive and clear disclosure of information, financial allocations, data sharing agreements, procurement documents and contracts among other things.

4.6 Technological frameworks governing Freedom of Expression Online

The study revealed that the Internet as a platform and its technological ecosystems plays a vital function in improving citizens access to information and aiding freedom of

expression and distribution of data and information in general because of availability and capability to store and disseminate massive quantities of data.

Similarly, many new obstacles to media development have arisen as a result of digital technologies. The range of options afforded by interactive sites, smart phones, and internet services, in particular, is unequaled in broadcasting history. Citizens can have worldwide access to data and information thanks to technological advancements. The amount of information available to the public is shocking. Simultaneously, internet safety and governing organizations have posed new threats to sovereignty of expression.

At the same time, the danger of harm posed by Internet material and communications to the enjoyment and gratification of human rights and freedoms, mainly the right to privacy, is superior than the risk posed by traditional media. Defamatory and other sorts of blatantly illegal statements, such as hate speech and speech encouraging violence, can be widely spread and can sometimes be found online indefinitely.

4.7 Telecommunication and Oversight Institution Role Online

The findings showed Kenya’s law enforcement employees are formally present within internet or telecommunication operators' vicinity with the understanding of the providers. According to former Safaricom CEO, the late Bob Collymore and Privacy International, the National Intelligence Service (NIS) agents are also casually present at the internet firms' facilities, in undercover.

Information analyzed further showed that telecommunications and internet providers companies end up handing over their clients’ information because they believe they cannot refuse requests from government authorities, in part due to the law's ambiguity and the internet and telecommunication industry's standards. Several telecommunications companies expressed concern that their licenses might be canceled if they did not comply, either explicitly or implicitly.

Telecommunications companies frequently believe that they have a social responsibility to defend national safety. According to a senior officer at one of Kenya's telecommunication operators, "no one is going to say no." "Think about it," says the interviewer. "Who am I to say no if any of the attackers at Westgate had our the mobile operator's money SIM card? "What I'm supposed to say or do?" says the interviewer.

4.8 Discussion of Findings

According to the findings, despite the government of Kenya's efforts to reinforce and embed privacy protection both in its legislative and jurisdictive frameworks, there is growing anxieties about definite surveillance behaviour by some government institutions, policies, and laws, for example the implementation of the Early Warning Systems (NEWS) Act, Prevention of Terrorism Act, 2012 and the Network and Early Warning Systems Act. These policies are frequently included in government plans to tackle terrorism, cybercrime, fraud, and corruption.

The Open Society Justice Initiative, Amnesty International and Human Rights Watch are among other Kenyan and international organizations, that have expressed concern about reports of human rights violations by technology companies, multinational corporations, and the law enforcers personnel in the pretext of counterterrorism operations usually giving threats to journalist and Human Rights Defenders for exercising their individual rights of freedom.

Monitoring technologies and surveillance, as well as invasive, refined and hidden surveillance programs, are extremely powerful instruments in the hands of the State, and they are hypothetically vulnerable towards misuse. It has been mainstreamed by the Kenyan law which mandates for a jurisdictive approval for communications interference and only Parliament Act can limit privacy. The Information and Communications Regulations give state authorities broad powers to collect and access phone users' data.

However, fears are that judicial structures are being abused and that citizens' privacy is being compromised.

Researchers found similar and systematic spyware by name Blue Coat which were installed in several nations telecommunication systems, including Kenya, according to a study brief issued by the University of Toronto's Citizen Lab in January 2013. Blue Coat enables for the monitoring and surveillance of user activities on a variety of platforms, including Facebook, Twitter, Google Mail, and Skype.

Section 31 of the Kenyan Information and Communications Act prohibits licensed telecommunications operators from implementing the technical requirements necessary for lawful eavesdropping. Further, Section 15(1) of the Information and Communications (Consumer Protection) Regulations of Kenya 2010 states that a licensee (licensed under the KIC Act) may not monitor, disclose, or permit monitoring of a licensee to disclose, allow a licensee to conduct surveillance.

Human rights organizations and other CSOs have repeatedly informed Kenya State Officials and the global community about the plight of journalists and Human Rights Defenders in the country. Although this is not a new issue, the focus on it in Kenya's previous UPR assessment in 2010 indicates that, while it is not a new issue, it still deserves attention since the State authorities and officials have unsuccessful refused to take the required actions to take remedial actions towards the aforementioned situation.

The right to have a private life has developed to include the government duties relating to the protection of personal data as advances in Information Communication Technology (ICT) have permitted previously unimagined modes of collecting, keeping, and exchanging personal information. Many domestic legislatures have integrated data protection concepts into national legislation, as do a number of international agreements.

Non-state and State actors' deficiency of openness and accountability creates fears of indefinite monitoring and data exploitation, as well as the government’s inability to support the citizen’s rights.

Numerous access to information and data demands from Kenyan individuals and human rights organizations are ignored by government institutions in Kenya. A constitutional petition (No. 218 of 2020) was filed in July 2020, detailing the Kenyan government's refusal to "proactively disclose and publicize crucial facts concerning the COVID-19 pandemic and the government’s reaction." The petition also detailed several instances of state entities, including the Inspector-General of Police, Ministry of Interior and Ministry of Health failing to comply with Access to Information Act, 2016.

CHAPTER FIVE

DISCUSSION AND CONCLUSION

5.1 Introduction

The research summary, results, and suggestions are presented in this chapter. The results are decisively interpreted in light of the research study goals, which are centered on the impact of internet surveillance on freedom of speech in Kenya.

5.2 Summary of findings

The research findings shows that the personal information journalists, human rights defenders and other users provide knowingly or unknowingly becomes a precious commodity. The photos users upload online, the questions they ask on search engines expose mankind's deepest prejudgments and their location histories show investors which commodities and stores attract the most buyers. Seemingly harmless activities like staying at home and watching a movie generate mountains of information, a treasure that is later gathered by companies of all kinds. Personal data is often compared to oil “it powers today's most profitable businesses" but the consumers who source it often have little knowledge of how much information is being collected, who can see it, and how much it is worth. Every day hundreds of companies that online users may not even know exist are collecting data about them, some more intimately. That information can then flow to academic researchers, hackers, law enforcement agencies and overseas, as well as many companies trying to sell things.

The data of this research suggests that broad surveillance of freedom of expression for journalists and citizens will almost certainly result in more arrests, especially in countries which have weak freedom of expression or places where policing and oversight

institutions do not adhere to the rule of law. In Kenya the internet platforms, particularly social media and these include Facebook, Twitter, Telegram, Signal, Instagram and blogs allows communicators to reach a large audience for less cost. These platforms have similarly given a very effective and affordable ecosystem for malicious players to conduct cybercrime activities, specifically surveillance and spread misinformation. Most of these cybercrime activities in Kenya and the wider East Africa region are done through proxies. Specifically politicians are enlisted as the major violators of people's freedom of expression when they hire technologists with access to the government's machinery. The findings further indicate that some of the telecommunication companies or employees in Kenya are serial offenders of curtailing communicators' freedom of expression either directly or indirectly swaying online public opinion in their favour.

Evidence has shown that the government of Kenya has built and continues to build an ever developing connection with China over the years, in terms of acquisition of loans, imports and exports of products and services which most have direct connection to technology infrastructure. It is worth noting that China is a world front-runner in development initiatives, use, and export of internet and monitoring surveillance techniques. Semptian, a Chinese company, claims that their Aegis surveillance system gives users a complete view of the virtual world and the ability to keep and analyze infinite data. The company claims to track over 200 million Chinese citizens, making up a quarter of the country's online consumers. The firm even sells a device dubbed a "national firewall," which is modeled after the so-called "Great Firewall" that regulates internet traffic. If truly this technology exists then it means Kenya’s best friend on technology is the People's Republic of China.

5.3 Conclusions

No one's privacy, family, home, or communication must be subjected to arbitrary intrusion. The Universal Declaration of Human Rights is a key document that has frameworks which spells out the rights of all people everywhere. Application of this declaration with the rights that it advocates does not and should not be applied selectively, it is similar across the board and that includes citizens and office bearers. The use of automated technologies, surveillance artificial intelligence to enable widespread monitoring of people's personal cell phones, laptop computers, and interactive sites user accounts is out of hand. Majority of Kenyans are unwittingly opting into a data goldmine that can now be readily accessed. Kenya's government, which is being led by President Uhuru Kenyatta (2013-2022) is embarking on an ambitious project to digitize every service provision. Through the project dubbed "Huduma Namba" the process has been marred and continues to be faced with endless legal battles being led by Civil Society Organizations in Kenya on the quest to secure citizens' rights.

Similarly, the private sector in Kenya has invested substantially and continues to invest in technology platforms that partake the probable to monitor Kenyans, limiting liberty. A considerable number of politicians in Kenya have a stake in these companies and are mostly driven by profits and securing personal ambition without consideration of public interest. The same companies that value ethical value promise to safeguard our data from surveillance and interception. Nevertheless, most of the data collected by these companies is freely available, and mass scraping programs can easily harvest all of those sources since some of them do not invest immensely on firewalls. In other circumstances the private companies collide with law enforcement and intelligence institutions to gather and create a narrative for specific target individuals whom they believe do not conform with how the system thinks they should. Part of the people targeted are journalists, human

rights defenders, with strong independent voices and daily operations of civil society organisations.

5.4 Limitations of the Study

The research is exploratory that employed qualitative research methods to collect and analyze data (Kothari & Garg, 2019). This research strategy was suitable since it allowed for the consideration of many elements of the problem statement under examination. The link between main types of internet surveillance and freedom of expression was accurately established.

Because the findings are confined to Kenya, the information cannot be extended to other countries or used to provide solutions outside of Kenya's borders. The research concentrated on interviewing some of the extremely busy and technical staff members who had critical concerns, while ensuring that their identities were kept completely confidential for security reasons.

This was due to the fact that the sort of response to the questions was classified. The participants decided the majority of the interview platforms and schedules as a consequence of Covid-19, stakeholders involved, capability of the parties mentioned, and the sensitivity of the knowledge requested. However, the research was able to gather the evidence needed to reach a substantive conclusion and recommendation.

5.5 Recommendations

5.5.1 Governments of Kenya

With the aim to protect and uphold freedom of expression, this research suggests that Kenyan government takes administrative, legal, financial, and practical stages to safeguard the complete independence of data protection agencies. Second, proper monitoring and protection in telecommunication legislation, including court warrants, are

needed to check the wide search capabilities provided to technical innovators, corporations with access to Kenyans data.

Examine all COVID-19 pandemic measures and systems, including data collecting programs, systems, and applications, to verify that they fully adhere to the three-part criteria under international human rights legislation, as well as data protection concepts such as data protection and privacy by design. Data and documentation pertaining to public-private partnerships, including but not limited to agreements, procurement papers, data sharing agreements, and financial allocations for ICT investments, should be disclosed and made available beforehand.

5.5.2 To private companies

According to the findings, private companies operating independently or in collaboration with Kenyan government to create and implement current and new technology, goods, and services for development and to combat COVID-19 should respect human rights. They should, in particular, adhere to Kenya's constitution, global human rights standards, such as the United Nations Guiding Principles on Business and Human Rights, and national legislation safeguarding confidentiality, data protection, access to information and freedom of expression.

Advance and execute all-inclusive data protection policies and procedures to govern their personal data collection, processing, and storage. Integrate data protection principles into the design, development, and deployment of technologies, such as data retention, determination limitation, data minimization and informed permission. Before cooperating with government requests for personal information, seek court orders from the officers. They should refuse to cooperate with unauthorized, or prohibited data requests from states agencies.

Actively and continuously submit accountability and transparency reports that detail when online user data or information has been demanded and shared with state agencies and other private institutions the types of user data requested and shared, in what way the data was shared, risks to customers' data, prevailing grievance mechanisms, and measures in place to protect customer data.

5.5.3 Policymakers

Use of network monitoring technologies and the acquisition of user data by government agencies and law enforcement should be strictly regulated. To maintain democratic norms, any government or law enforcement network monitoring program must be subject to strict scrutiny and operate in the open, especially via ongoing interaction with local populations. Surveillance of peaceful protests or individuals' membership in nonviolent political organizations should not be utilized as a proactive measure. States agencies should not conduct blanket collection of social media data as part of immigration or visa assessments. The technical limitations and known inaccuracy rates of such technology, relevant oversight agencies should conduct human rights audits of the tools themselves and their use, and release their results to the public. They should further be empowered to impose penalties, and require that those harmed be granted remedy

5.5.4 To online users

A data provider, also known as an online user can take the following steps to block the collector's access to it. By emptying the browser's cache, erasing cookies, and clearing application use data, the user can remove the traces of his online activity. Online user can use an anti-tracking extension when surfing Internet to prevent trackers from gathering cookies. Disconnect, Do Not Track Me, and Ghostery are some of the most

popular anti-tracking add-ons. Script and advertising blockers are used. These browser extensions can prevent ads on websites and inactivate scripts and widgets which transfer the user's information to an unknown third party. NoScript, AdBlock Plus and FlashBlock are just a few examples. The use of encryption software. To ensure that individual online conversation between two parties is not captured by third parties, a user can scramble his emails, instant messaging, or other forms of web traffic using encryption tools like MailCloak and TorChat. To safeguard data saved in digital equipment like personal computers, phones, and tablets, an online user should constantly use anti-malware software or anti-virus. Use sockpuppets as a way to disguise one's actual activity and falsify his data. A sockpuppet is a fictitious online persona through which a member of an online community pretends to be someone else. Using numerous sockpuppets, data generated by one person's activity will be interpreted as belonging to multiple people. Masking one's identity with security software. When a user registers for a website or makes an online purchase, he is frequently requested for personal information like a credit card number, email address and phone number. MaskMe, a browser plugin developed by Abine, Inc., an online privacy firm, can assist users in creating and managing aliases (or Masks) of their personal information. Users can use these aliases in the same way they do when such information is needed, but websites will not be able to obtain the true information. Users' privacy is safeguarded in this way. Keep work and personal life separated. Understand how you can be attacked online and how to establish countermeasures such as identifying the goals attackers may have such as money recognition, political instigated, or knowledge on your work. Always ask yourself the following questions: Might you have acquired new information which comes with various online threats, who often do you meet within the week or month where the avenues of attack might come from. Strategize your offline and online security concerns

from an all-around perspective. The following table provides guidance on how to mitigate possible threats that mostly lead to access of data to online users:

Mobile theft, Solution: Your phone bag pack should be included in your outfit. An IMEI is a unique serial number assigned to each smartphone. Make a recording of it and save it for legal purposes.Your phone bag pack should be included in your outfit. An IMEI is a unique serial number assigned to each smartphone. Make a recording of it and save it for legal purposes.

Passwords hack, Solution: Make a strong password with at least eight characters that include a mix of letters, numerals, and special symbols that do not form instantly recognizable words or phrases. Never use the same password twice and remember the credentials containing personal information should not be used. Please do not rely on Windows passwords to keep your information safe. They are easily damaged. It is always a good idea to set a reminder to change your passwords at least once a month. Make sure the passwords aren't the same as the ones you use to access your primary email account. It is important that you install the latest updates for your operating system, applications, and browser as they become available. Most of the updates contain security fixes and are essential to prevent hackers from accessing your data and using it for malicious purposes. This is easily overlooked and most devices offer automatic updates so you are never left unprotected. Use a BIOS password to secure the computer during startup.

Utilize a two-step verification procedure. Because of the two layers, even if someone steals your password, they will not be able to access your account. This process prompts the user who is attempting to login to enter the primary password, after which a completely separate code will be sent to the user's default phone via text or call and must be entered in such that you gain access to the account. Since no password is generally required to access public WiFi, it serves as a hub and platform for minor cybercrime as it

lacks security functions. Therefore, it is highly recommended not to connect your computer to public Wi-Fi networks as these are popular targets for hackers who want to spread malware or access your data. Another way to keep hackers away from your phone or computer is to turn the wifi, Bluetooth, file-sharing features, or literally, switch your computer or cell phone off when you are not using them. It seems common practice to put our devices on hold, but this makes them more visible and more vulnerable to hackers. The computer can break a hacker's connection to your network.

Destruction of information, Solution: Make sure you backup your data on a regular basis. Utilize a well-known and trusted antivirus and firewall. Be aware that Phishing emails are fake emails that appear legitimate in order to steal personal information and install malware in your computer or phone. They keep getting more sophisticated and can easily fool people that they are from real people and companies that know. Please note the following: Examine the sender's address. Does it appear to be correct, or is it from an unknown account?Is the sender addressing you by your first name? If the e-mail begins with "Dear customer," or if you only use your first initials, this could indicate that the e-mail is a forgery.When the email requests immediate details or payment, it is best to contact the company directly. The majority of businesses do not have such practice within their companies or organisations. Were you expecting such an email. If you do not expect to receive an email from such a sender, therefore this could be a signal of a forged email. It is always best to call the sender on an already existing phone number in your phone and speak with him directly. Try and reference a previous engagement and be keen on listening to how they narrate your interactions. When installing new software or purchasing a computer with pre-installed software, always proceed with caution. Use only the software required for your job and remove everything else. When you want to buy something from a website you've never used before or submit

personal information. The best thing to do is double-check before proceeding. How? Look for reviews from previous customers on reputable review platforms. It is best to avoid using this website if you are unsure. It is also a good idea to verify that a website is encrypted before entering any financial or personal information. If a website is encrypted, check the address bar to see if it starts with “https” and is accompanied by a closed padlock icon.

5.5.5 Recommendations for further Studies

This research concentrated on how online surveillance is being conducted in Kenya and how it’s affecting freedom of expression online. As a result, the research recommends that a thorough investigation be conducted into which multinational corporations are responsible for providing knowledge, infrastructure, and services to private institutions with the capability of surveilling its citizens, an act that curtails freedom of expression. As previously established, there was limited understanding on who the external creators and providers of technical surveillance knowledge in Kenya. As a result, determining the source of surveillance architecture would give insights into what are their products' shortcomings are and how independent voices might circumvent unlawful snares.

REFERENCES

"Inside Kenya's Death Squads", Al Jazeera Investigates, December 2014, available at: http:// interactive.aljazeera.com/aje/KenyaDeathSquads/

Access to Information Act, 2016.

Article 19. (2017, March 9). The Global Principles on Protection of Freedom of Expression and Privacy.

CitizenLab, Planet Blue Coat: Mapping Global Censorship and Surveillance Tools, Research Brief, Number 13, January 2013, University of Toronto, MUNK School of Global Affairs. Available at: https://citizenlab.org/wpcontent/uploads/2013/01/Planet-Blue-Coat.pdf

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approach*es (2nd ed.). Sage Publications, Inc.

Davidowitz, S. S. (2017). *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are*. HarperCollins.

Human Rights Committee, 102nd Session, July 2011, General Comment No.34 on Article 19.

Kenya Anticorruption Commission Report. (2007, September 9). "Bugged - Police Can Now Listen to Your Phone Talks," *The Standard*, available at: http://allafrica.com/stories/200709100352.html

Kenya's Data Protection Act, 2019

Kothari, C.R., & Garg, G. (2019). *Research Methodology: Methods and Techniques*. New Age International Publishers.

Media Innovation Centre. (2021). Media viability in Kenya. Graduate School of Media and Communications, Aga Khan University and DW Akademie.

Media Innovation Centre. (2021). Media viability in Tanzania. Graduate School of Media and Communications, Aga Khan University and DW Akademie.

Media Innovation Centre. (2021). Media viability in Uganda. Graduate School of Media and Communications, Aga Khan University and DW Akademie.

Mhaka, T. (2020, November 12). How social media regulations are silencing dissent in Africa, *Al Jazeera*.

National Intelligence Service Act (2012). available at: http://kenyalaw.org/lex/rest//db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/N/National%20Intelligence%20Service%20Act%20No.%2028%20of%202012/docs/NationalIntelligenceServiceAct28of2012.pdf

Okuttah, M. (2012, March 20). CCK sparks row with fresh bid to spy on Internet users, *Business Daily*. Available at: http://www.businessdailyafrica.com/Corporate-News/CCK-sparks-row-with-fresh-bid-to-spy-on-Internet-users-/-/539550/1370218/-/x6adjmz/-/index.html

Privacy International & Article 19 (2018). *Privacy and Freedom of Expression In the Age of Artificial Intelligence.*

Privacy International & National Coalition of Human Rights Defenders in Kenya (2018). Universal Periodic Review Stakeholder Report: 21st Session: *Privacy and Freedom of Expression In the Age of Artificial Intelligence.*

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue A/HRC/17/27, https://undocs.org/en/A/HRC/17/27

Surveillance and Human Rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/41/35, https://undocs.org/A/HRC/41/35

The Constitution of Kenya, (2010) Chapter four: *The Bill of Rights.*

The Nation. (2016, December 11). "How the Recce unit to protect Kenyatta was mooted and trained," available: at: http://www.nation.co.ke/news/How-the-Recce-unit-to-protect-Kenyatta-wasmooted/1056-3481946-9rv3rc/

The right to privacy in the digital age, General Assembly, A/RES/68/167, https://undocs.org/A/RES/68/167

Wambui, M. (2020, June 17). Kenya: Hope as Three Kenyans Develop App for Contact Tracing, All Africa.

ANNEXES

Interview Guide

Semi structured interview guide
Provide: Expertise / Region Online user/ICT Developer/ Oversight adjudicator
Length: 20- 40 Minutes
Provide / Expertise / Region
Would you like to participate in this interview? Verbal Consent was obtained from the study participant Verbal Consent was NOT obtained from the study participant
Key questions to ask participants 1. Briefly tell us about yourself and your work? 2. In your understanding, what does online surveillance entail? 3. In your understanding, on freedom of expression? 4. Why is online surveillance important in your work? 5. As an online user what are your concerns about online surveillance and your freedoms? 6. What do you see as sources of surveillance in your work? 7. How do you protect your communication privacy and security as an online user 8. What communication tools do you use in your everyday work and how would you rate their level of security? 9. In what ways can an online user secure and protect their communication? 10. What protective measures have you adopted to ensure your communication security and privacy? 11. What kind of surveillance have you ever been under because of your work? 12. What kind of online threat have you faced and how did you address them? 13. What level of control do you have over your information? 14. Do you have anything else to add? **(probe close-ended questions)**

Declaration of Consent by Participant

Researcher: Medika Medi

Cell: +254721724264

Purpose of the study

The study aims to explore the impact surveillance on freedom of expression through examining how safe online platforms are against unwarranted surveillance and provides probable legal and technological solutions on existing gaps.

Your rights as participant

I……. declare that I have understood my rights on relation to this research exercises, which includes, confidentiality and anonymity, the right not to answer any question if wish not to, the right to withdraw my participation without any consequences whatsoever and I'm in agreement with any type of recording or transcription of my responses, as long as they are kept confidential and used for this research only.

Pursuant to above, I hereby declare that I am participating in this research at will, and I am above 18 years of age.

Participant's name:

……

Debriefing Form

Thank you very much for your valuable input into this research. Your response will contribute to the existing gap of knowledge on freedom of expression and online surveillance.

In case you have any queries regarding any aspect of this study please contact the researcher via cell phone number +254721724264 or email medikamedi@gmail.com

The researcher will be happy to share with you the final report once completed and approved.

Thank you.