Strathmore
UNIVERSITY

A STUDY OF MASS SURVEILLANCE OF COMMUNICATIONS THROUGH DEVICE MANAGEMENT SYSTEMS AND THE RIGHT TO PRIVACY.

Submitted in partial fulfilment of the requirements of the Bachelor of Law Degree, Strathmore University Law School

By

Mitchelle Gathoni Kigo

129198

Prepared under the supervision of

Eva Nyambura Maina.

March 2024

Word count: 9,266.

TABLE OF CONTENTS.

ACKNOWLEDGMENT

I would like to express my gratitude to the Almighty God for granting me the grace and wisdom to undertake this research project. I would also like to thank my supervisor for her guidance throughout this process and her dedication to ensuring that I successfully carried out this project. Lastly, I would like to thank my family and friends for the love, patience and support throughout this process.

DECLARATION

I, MITCHELLE GATHONI KIGO, do hereby declare that this research is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree of diploma. Other works cited or referred to are accordingly acknowledged.

Signed: .....

Date: 06/03/2024

This dissertation has been submitted for examination for examination with my approval as University Supervisor.

Signed: .....

EVA NJAMBURA NAINA

6.03.2024

ABSTRACT

The tension between mass surveillance and the right to privacy has become increasingly complex as communication technologies extend to every aspect of daily human life. This research paper investigates the implications of mass surveillance of communications through device management systems and the individual's right to privacy. An interdisciplinary approach incorporating legal, ethical, technological and social dimensions is employed to provide a holistic understanding of the phenomenon. It examines the mechanism by which the device management systems facilitate mass surveillance focusing on their capabilities, limitations and potential abuses. The paper also delves into the legal framework governing mass surveillance practices and their alignment and tensions between national security interests, individual privacy and law enforcement objectives. Ethical considerations surrounding mass surveillance are examined, seeking to uncover the moral dilemmas inherent in communication surveillance practices. The research also delves into the societal impacts of mass surveillance including its effects on social cohesion and the exercise of fundamental rights. It investigates the public perception of surveillance practices and the trade-offs between privacy and of national and government interests. This paper contributes to the scholarly dialogue on mass surveillance and individual privacy by offering insights into the implications of surveillance activities through device management systems. It aims to inform policymakers and the general public about the complexities inherent in mass surveillance practices and the imperative of safeguarding the right to privacy in the digital age.

LIST OF CASES

1. Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.
2. Communications Authority of Kenya v Okiya Omtatah Okoiti & 8 others [2020] eKLR
3. Cyprian Andama v Director of Public Prosecutions & another [2019] eKLR.
4. Khalifa & another v Principal secretary, Ministry of Transport & 4 others (2022) eKLR.
5. Coalition for Forum and Democracy (CORD) & 2 others v Republic of Kenya & 10 others [2015] eKLR.
6. Nubian Rights Forum & 2 others v Attorney General & 6 others [2020] eKLR

LIST OF LEGAL INSTRUMENTS

1. Constitution of Kenya (2010)
2. Kenya Information and Communications Act (Act No. 441C of 1998)
3. Kenya Information and Communications (Consumer Protection) Regulations (2010).
4. Prevention of Terrorism Act
5. Registration of Persons Act (Act No. 107 of 1949)
6. Data Protection Act (Act No. 411C of 2019).
7. Security Laws (Amendment) Act, (Act No. 19 of 2014

CHAPTER 1: INTRODUCTION

1.1 Background

Mass surveillance involves acquiring, processing, generating, analysing, using, retaining or storing information about a large population without considering whether they are suspected of wrongdoing.[1] It uses systems or technologies that collect, analyse and generates data on a large population instead of limiting surveillance to individuals who are reasonably suspected of wrongdoing.[2] Intelligence agencies and law enforcement conduct mass surveillance through various means and methods such as mass interception of communications, access to bulk communications stored by telecom operators and others and mass hacking among others.[3] Mass surveillance can subject a population to systematic interference with their right to privacy.[4] Mass surveillance subjects people to unlimited state authority and control by monitoring people's lives.[5] It may also enable potential unchecked state power and control over individuals.[6]

In Kenya, there has been a warning by a global human rights organization, Privacy International, on the installation of a tracking device named the Device Management Systems on mobile phone networks which will subject the population to indiscriminate monitoring thereby opening Kenyans to mass surveillance.[7] A device management system enables organizations to maintain and administer devices such as physical computers and mobile devices among others.[8] It helps to ensure that devices are secure, updated and comply with organizational policies.[9] Their goal is to

---

[1] https://www.privacyinternational.org/learn/mass-surveillance on 9th September 2023.

[2] https://www.privacyinternational.org/learn/mass-surveillance on 9th September 2023.

[3] https://www.privacyinternational.org/learn/mass-surveillance on 9th September 2023.

[4] https://www.privacyinternational.org/learn/mass-surveillance on 9th September 2023.

[5] https://privacyinternational.org/learn/mass-surveillance#:~:text=Mass%20surveillance%20is%20indiscriminate%20surveillance,is%20reasonable%20suspicion%20of%20wrongdoing on 9th September 2023.

[6] https://www.privacyinternational.org/learn/mass-surveillance on 9th September 2023.

[7] https://www.businessdailyafrica.com/bd/economy/state-linked-to-mass-mobile-phone-surveillance-plot-3992454 on 9th September 2023.

[8] https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management on 9th September 2023.

[9] https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management on 9th September 2023.

protect data from unauthorized access.[10] The system aggregates data collected by mobile devices and monitors and controls their operation.[11]

The Constitution of Kenya under Article 31 provides that every person has the right to privacy which includes not having the privacy of their communications infringed.[12] Furthermore, Article 24 of the Constitution stipulates that the rights or fundamental freedom in the Bill of Rights shall not be limited except by law and only to the extent where the limit is justifiable and reasonable, and based on human dignity, equality and freedom in an open and democratic society.[13]

Section 31 of the Kenya Information and Communications Act provides that a licensed telecommunication operator who otherwise in the course of their business intercepts any message sent through a licensed telecommunication system discloses to any person the message or any statement or account intercepted commits an offence.[14] Additionally, the Kenya Information and Communications Regulations stipulate that a licensee or any person ought not monitor and disclose the content of any information of a subscriber by tapping, listening, storage or any other kind of interception or surveillance of communication.[15]

In 2016, the Communications Authority Kenya began the implementation process of the Device Management System which was intended to be installed in phones in Kenya.[16] The purpose of the Device Management System is to help deal with fraud in telecommunications, identify all active devices on public telecommunications networks, isolate illegal devices and create a whitelist of legitimate devices.[17] The Communications Authority of Kenya invited mobile network providers in the implementation process of the Device Management System since they

---

[10] https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management on 9th September 2023.

[11] E Braten, 'Autonomous IoT Device Management Systems: Structure Review and Generalized Cognitive Model,' Internet of Things Journal, 2021, 4275.

[12] Article 31, Constitution of Kenya (2010).

[13] Article 24, Constitution of Kenya (2010).

[14] Section 31, Kenya Information and Communications Act (Act No 411A of 1998)

[15] Section 15, Kenya Information and Communications (consumer protection) regulations (2010)

[16] https://restofworld.org/2023/kenya-device-management-system-digital-rights-activists/ on 5th March 20124.

[17] https://gadgets-africa.com/2023/12/04/ca-phones-kenya/#:~:text=The%20Communication%20Authority%20of%20Kenya%20%28CA%29%20intends%20to,end%20the%20proliferation%20of%20counterfeit%20devices%20and%20theft. on 5th March 2024.

were able to identify and block blacklisted devices.[18] Mobile network providers such as Safaricom Limited raised concerns on issues such as privacy, confidentiality and consumer concerns that would arise from a third party having custody over their consumer's personal information.[19]

In Okoiti v Communications Authority of Kenya & 8 others [2018], the petitioner claimed that the government's justification for the device management system eavesdropping on private communications is that the device management system is required to monitor and identify stolen handsets, counterfeit phones and devices.[20] The petitioner claimed that the government was silent on the fact that the proposed device management system is capable of spying on calls and texts and can also review mobile money transactions.[21] Therefore, Kenyans' right to privacy will not be enjoyed in so far as usage of their mobile phones is concerned.[22] The respondents claimed that the device management system was necessary to deal with counterfeit and illegal devices.[23] The High Court held that the Communications Authority of Kenya's plan to implement device management systems to access mobile service subscribers' information was a threat and breach of the constitutional right to privacy.[24] The Communications Authority of Kenya appealed the case to the Court of Appeal. In the Court of Appeal, the judgment by the High Court was set aside to allow the construction of the Device Management System while ensuring the protection of the freedom of privacy.[25] The matter was later appealed to the Supreme Court in Law Society of Kenya v Communications Authority of Kenya & 10 others. The appellant argued that the Court of Appeal failed to conduct the Article 24 of the Constitution of Kenya test on limitations.[26] The Supreme Court dismissed the petition made by the petitioner challenging the Court of Appeal's judgment on grounds that the Appellant lacked locus standi in the matter thus

---

[18] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR

[19] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[20] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[21] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[22] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[23] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[24] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[25] Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others [2020] eKLR

[26] Law Society of Kenya v Communications Authority of Kenya & 10 others (2020) eKLR.

allowing the Communication Authority of Kenya to continue developing a device management system.[27]

Several bodies such as the Law Society of Kenya still raise concerns the device management system shall limit the right to privacy of communications as mobile phone conversations are extremely private and ought not to be monitored by the agents or third parties involved in the installation and use of these systems.[28] However, the Communications Authority of Kenya supports the rollout of the device management systems amid claims that the telecoms will be given watchdog access to customers data as they fight against counterfeits.[29]

1.2 Statement of problem

Article 31 of the Constitution of Kenya provides that the privacy of communications of every person ought not to be infringed. The Kenya Information and Communications Act and Kenya Information and Communications Regulations provide for intercepted communications and how intercepted communications ought to be handled. The installation of device management systems on mobile devices will enable the collection, storage and monitoring of information from unsuspecting Kenyans causing a threat to the right to privacy given that mobile phone conversations ought to be private. Installation of device management systems may lead to unregulated government power and control over individuals. It may also lead to extortion, coercion and discrimination to an individual by the government or agencies carrying out this surveillance. This study thus investigates whether mass surveillance of communications through device management systems is a justifiable limit to the right of privacy in Kenya.

1.3 Research questions.

1. Whether there exists a trade-off between key government objectives and privacy concerns in the context of mass surveillance in Kenya.
2. What are the potential privacy concerns and effects of the collection, storage, use and disclosure of information through mass surveillance in Kenya.

---

[27] Law Society of Kenya v Communications Authority of Kenya & 10 others (2020) eKLR.

[28] https://www.businessdailyafrica.com/bd/economy/state-linked-to-mass-mobile-phone-surveillance-plot-3992454 on 9th September 2023.

[29] https://www.businessdailyafrica.com/bd/economy/state-linked-to-mass-mobile-phone-surveillance-plot-3992454 on 9th September 2023.

3. Whether the interception of communication through device management systems leads to the interference of an individual's right to privacy and if the interference is justifiable.

1.4 Research objectives.

1. To understand whether there is a trade-off between key government objectives and privacy concerns in the context of mass surveillance in Kenya.
2. To analyse the potential privacy concerns and effects of the collection, storage, use and disclosure of information through mass surveillance in Kenya.
3. To understand whether interference of communication through device management systems leads to interference of an individual's right to privacy and if the interference is justifiable.

1.5 Hypothesis

Through adopting device management systems, Kenyans will be exposed to state surveillance which can limit their right to privacy. The device management system is used to intercept, collect and record the communication of individuals. Mass surveillance may be necessary to ensure national security and curb terrorism and crime. However, the surveillance of communication of individuals is a threat to the privacy of an individual as the communication collected may be abused by the watchdogs. Mass surveillance is unnecessary on an unsuspecting population as it exposes one to the risk of having their personal information accessed by third parties without any reasonable cause. The illegitimate and arbitrary surveillance of an individual through their communication without their knowledge is unlawful as it threatens one privacy.

1.6 Justification.

Mass surveillance through the device management system affects people by limiting their right to privacy. The collection, storage, and monitoring of information from the unsuspecting public may result in the information being used for unjustified reasons. This study will be useful as it aims to understand the right to privacy to assess whether mass surveillance of communications of individuals is justified. This study will aid policymakers and lawmakers in constructing and implementing laws and regulations that protect individuals right to privacy in relation to mass surveillance. It will also help adjudicators in applying the required threshold when deciding cases on mass surveillance of communications. Lastly, the study will help other researchers and scholars to understand how mass surveillance affects democratic societies.

1.7 Theoretical framework.

Jeremy Bentham and Michel Foucault are well known for the panopticon theory. The prison panopticon is a design where a prison is circular with cells on the circumference.[30] There was an inspector at a tower at the centre of the prison who oversaw the activities of the prisoners in their cells.[31] The prisoners had no idea that they were being watched.[32] An illusion of constant surveillance is made to the prisoners. Even though the prisoners are not constantly being watched, they are made to believe that they are being watched.[33]

The panopticon aimed to keep the inmates under continuous and close observation.[34] The prisoners did not know when and if they were being watched but there was an impression that they were being watched continuously.[35] Consequently, this would encourage discipline among the prisoners which would lead to a change of behaviour.[36] Bentham's idea was that discipline would be normalized and an inspector would eventually no longer be needed.[37] His theory was not all-seeing and the need for continuous inspection was to make the need for watching and the panopticon obvious.[38] The main idea was that the prisoners would be aware that they might be watched. [39]Bentham suggested that power should be visible and unverifiable.[40] The tower at the

---

[30] Miller R, Miller J, 'Jeremy Bentham's Panoptic Device,' 41, The MIT press, 1987, 3.

[31] Halborg S, 'Panopticon: a critique', in Foo F (ed) *UCL Jurisprudence Review*, 28 Law Journal library, 1995, 3.

[32] Neil M, 'The dangers of surveillance,' 126 Harvard Law Review 7, 2013, 16.

[33] Halborg S, 'Panopticon: a critique', 1995, 3.

[34] Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', Leiden University Press 05, 2007, 8.

[35]Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', 36.

[36] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

[37] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

[38] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

[39] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

[40] Foucault M, ' Discipline and punish: The birth of the prison,' Knopf Doubleday Publishing Group, 1995, 201.

centre is constantly visible to the prisoners but the prisoners cannot verify whether they are being watched[41]

Foucault's concept of panopticism theorizes surveillance as having an all-seeing inspector.[42] He refers to Bentham's panopticon concept as a disciplinary control.[43] The panopticon combines power and control.[44] He defines panopticism as a form of power applied to individuals that involves continuous supervision through control, discipline, punishment, remuneration and correction by changing them in accordance with certain norms.[45]

For Foucault, the panopticon was a means to instigate a state of conscious and permanent visibility that would ensure the automatic functioning of power to the prisoners.[46] The destruction of privacy plays a huge role in the loss of freedom, individuality and autonomy.[47] The subjects would automatically alter their behaviour to meet the demands.[48] The process creates habits, rituals and how things are done which creates norms of behaviours.[49] Being normal is being able to conform to the norm created.[50] Foucault argues that disciplining the

---

[41] Foucault M, ' Discipline and punish: The birth of the prison,' 201.

[42] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

[43] Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', Leiden University Press 05, 2007, 8.

[44] Foucault M, ' Discipline and punish: The birth of the prison,1995.

[45] Foucault M, ' Discipline and punish: The birth of the prison,1995.

[46] Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', Leiden University Press 05, 2007, 8.

[47] Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', Leiden University Press 05, 2007, 9.

[48] Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', Leiden University Press 05, 2007,37.

[49] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

[50] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

individual is a governmental utopia where discipline produces subjected "docile bodies'.[51] Power is identified with modification of behaviour.[52]

The rise of modern surveillance technology makes panopticism practicable on a larger scale and turns society into a superpanopticon.[53] Foucault suggests that goals of efficiency, automation and continuous functions are in play now.[54] The subject of surveillance is being watched with the aim of which can be controlling and disciplining them into a certain behaviour. [55] The application of the panopticon asserts power over individuals.

1.8 Literature review.

When communications are subject to surveillance, members of the public lose the capacity to control their choices and social relationships.[56] This leads to a change in the character of the person and the relationship.[57] Surveillance brings about the risk of coercion, discrimination and blackmail.[58]

1.8.1 The trade-off between privacy and security concerns.

Privacy establishes a normative framework for deciding who should have the ability to access and alter information.[59] On the other hand, security is the technological means that moderates the request to access or control.[60] Security determines which privacy choices are implemented and

---

[51] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

[52] Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016, 12- https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2 on 16th September 2023.

[53] Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', Leiden University Press 05, 2007,38.

[54] Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', Leiden University Press 05, 2007,38.

[55] B Schermer, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', Leiden University Press 05, 2007, 38.

[56] Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016, 36 https://link.springer.com/article/10.1007/s10676-016-9392-2 on 23rd September 2023.

[57]Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016, 36 https://link.springer.com/article/10.1007/s10676-016-9392-2 on 23rd September 2023.

[58] Neil M, 'The dangers of surveillance,' 126 Harvard Law Review 7, 2013, 1936.

[59] Bambauer D, 'Privacy v Security,' Arizona Legal Studies, Discussion paper number 13-06, 2013, 669 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208824

[60] Bambauer D, 'Privacy v Security,' 669.

privacy also determines how security measures will be implemented.[61] Placing security and privacy concerns in the wrong category causes an insurmountable conceptual difficulty.[62]

The trade-off between privacy and security can be seen in two ways. Firstly, it can be seen as privacy causing a barrier to effective security measures.[63] This view justifies privacy intrusion as necessary to improve security.[64] Secondly, it can be viewed as where individuals gain more security by accepting their privacy to be intruded.[65] Surveillance-oriented system technology and security policy usage are based on the assumed necessity to trade off privacy for security.[66] There is statistical evidence against the trade-off between privacy and security at the individual level.[67]

1.8.2 Government control and power through mass surveillance.

Upon the acquisition of data by third parties through surveillance, the Government gains power over individuals. This power can either be used for coordination or control of the person or individual. By being able to supervise subjects, those in power acquire the means to exercise a greater deal of control.[68] Surveillance puts the government in a position to use mass surveillance to interfere with its citizens information and this entails domination.[69] It leads to domination where there are no regulations to block the interference.[70] The political power of the governments can change the social context of citizens such that certain kinds of relationships are made impossible and unavailable.[71]

---

[61] Bambauer D, 'Privacy v Security,' 669.

[62] Bambauer D, 'Privacy v Security,' 670.

[63] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between security and privacy,' in Friedewald M(ed), *Surveillance, privacy and Security*, 1ed, Routledge, London, 2017, 260.

[64] S Stefan, ' A game of hide and seek? Unscrambling the trade-off between security and privacy,' 260.

[65] S Stefan, ' A game of hide and seek? Unscrambling the trade-off between security and privacy,' 260.

[66] S Stefan, ' A game of hide and seek? Unscrambling the trade-off between security and privacy,' 260.

[67] S Stefan, ' A game of hide and seek? Unscrambling the trade-off between security and privacy,' 259.

[68]Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016, 36 https://link.springer.com/article/10.1007/s10676-016-9392-2 on 23rd September 2023.

[69]Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016, 36 https://link.springer.com/article/10.1007/s10676-016-9392-2 on 23rd September 2023.

[70]Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016, 36 https://link.springer.com/article/10.1007/s10676-016-9392-2 on 23rd September 2023.

[71]Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016, 36 https://link.springer.com/article/10.1007/s10676-016-9392-2 on 23rd September 2023.

Government surveillance is a power that has the potential to be massively abused.[72] By constantly monitoring people, mass surveillance makes it possible for unchecked state power and control over individuals.[73]

1.8.3 Privacy concerns and effects of communication surveillance in a democratic society such as Kenya.

Surveillance is against the law even if the information collected is not used illegitimately.[74] Secret surveillance is seen as illegitimate.[75] The knowledge that one is being observed and recorded generally inhibits freedom.[76] An assumption is made that democratic governments try to resist interfering illegitimately with their citizen's communication.[77] Democratic societies should discard the idea that the government is acting reasonably by recording telephone activity with or without consent.[78]

Access to a device can enable an intruder to manipulate a device by altering, adding or deleting files.[79] This makes it possible faking of evidence to incriminate or blackmail an individual.[80] Public surveillance has been used to identify and track political dissenters.[81] Even where the device management systems are used to combat terrorism and crime, they have often been used illegitimately by putting a crackdown on those who express dissenting views such as journalists, politicians and human rights defenders.[82]

---

[72] Neil R, 'The dangers of surveillance,' 1961.

[73] https://privacyinternational.org/learn/mass-surveillance#:~:text=Mass%20surveillance%20is%20indiscriminate%20surveillance,is%20reasonable%20suspicion%20of%20wrongdoing on 23rd September 2023.

[74] Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016, 34 https://link.springer.com/article/10.1007/s10676-016-9392-2 on 23rd September 2023.

[75] Neil R, ' The dangers of surveillance ,' 1935.

[76] Schermer, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance', 2007, p 1.

[77] Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016, 34 https://link.springer.com/article/10.1007/s10676-016-9392-2 on 23rd September 2023.

[78] Neil R, 'The dangers of surveillance,' 1961.

[79] UNGA, The right to privacy in the digital age, UN A/Res/75/176 (16th December 2020).

[80] UNGA, The right to privacy in the digital age.

[81] UNGA, The right to privacy in the digital age.

[82] UNGA, The right to privacy in the digital age.

Mass surveillance is not necessary and proportionate in a democratic society as there are less invasive measures and there is curiosity if a democratic society can survive under constant surveillance.[83] Mass surveillance creates an environment of suspicion and threat that is inconsistent with democratic values and principles where one is innocent until proven guilty.[84] Mass surveillance through the intruding of privacy poses a threat to democracy as it may lead to a form of social control because the government has a lot of power.[85] This data may be used to interfere with one's choices.[86]

1.9 Contribution of this study

This study will contribute to the analysis of mass surveillance and the resulting limits or threats to the privacy of an individual or group and whether the limits are justifiable. This is an issue against data protection and digital surveillance. It will aid in understanding where digital surveillance is a justified limit to the right to privacy. It will also help in understanding the gap in the law that leads to this issue. To install device management systems on telephones in Kenya, this study will contribute to the discussion on how mass surveillance through device management systems leads to a limit on the privacy of an individual. It will show how the government and other agencies that participate in digital surveillance use information that is collected and recorded. Through understanding the above-mentioned. This study will complement other scholars' work as it will give a Kenyan perspective on the same issue. The study will also look at the Kenyan court decisions and statutes to determine whether the threshold being used in Kenya is the same as those in scholarly work.

1.10 Methodology

This study aims at analysing the dangers of mass surveillance through the installation of device management systems in mobile phones and whether the threats posed by this are a justifiable limit to the right to privacy of Kenyans. The study will rely on a qualitative analysis of mass

---

[83] https://privacyinternational.org/learn/mass-surveillance#:~:text=Mass%20surveillance%20is%20indiscriminate%20surveillance,is%20reasonable%20suspicion%20of%20wrongdoing on 2nd October 2023.

[84] https://privacyinternational.org/learn/mass-surveillance#:~:text=Mass%20surveillance%20is%20indiscriminate%20surveillance,is%20reasonable%20suspicion%20of%20wrongdoing on 2nd October 2023 .

[85] Bonello R, 'Mass surveillance and the right to privacy,' published LLM thesis, Universiteit Leiden, Leiden 2016, 17

[86] Bonello R, 'Mass surveillance and the right to privacy,' 2016, p 17

surveillance through device management systems and how this limit one's privacy rights. The qualitative research will be carried out from both primary and secondary sources. The primary sources include statutes such as the Kenya Information and Communications Act and Kenya Information and Communications (consumer protection) Regulations and constitutional provisions such as the Constitution of Kenya (2010). The secondary sources include chapters on books, journal articles, case law and reports. The study will also take a deductive approach. The first chapter will show how mass surveillance and the right to privacy correlate and set the premise for the study. The subsequent chapters will then show how the main claim is derived from the premises.

The study will also take a doctrinal approach. An analysis of the constitution of Kenya, the Kenya Information and Communications Act and Kenya Information and Communications (consumer protection) Regulations will be carried out. This will aid in understanding and setting a standard for the eventual claim that installing device management systems will subject Kenya's population to mass surveillance which could threaten the right of privacy.

Lastly, the study will be desk-based research. The research will mostly involve research from primary and secondary sources as opposed to a field study.

1.11 Chapter breakdown

Chapter 1 of this study will contain the background to the study, statement of problem, research questions, research objectives, justification hypothesis, theoretical framework, literature review and the methodology intended to be used. Chapter 2 will analyse whether there is a trade-off between security and privacy concerns in the context of mass surveillance in Kenya. Chapter 3 of the study will analyse the potential privacy concerns and effects of the collection, storage, use and disclosure of intercepted communication in Kenya.

Chapter 4 of the study will analyse whether the interception of communication by the device management system leads to interference of an individual's right to privacy and whether the interference is justifiable. Chapter 5 will contain the recommendations that ought to be adopted to regulate mass surveillance through device management systems, as well as the conclusion.

CHAPTER 2: WHETHER A TRADE-OFF EXISTS BETWEEN KEY GOVERNMENT OBJECTIVES AND MAINTAINING PRIVACY CONCERNS IN THE CONTEXT OF MASS SURVEILLANCE IN KENYA.

Introduction

The trade-off between privacy and other key government objectives involves balancing the right to privacy with broader government objectives. Some of the key government objectives include national security, combating terrorism, fighting crime, combating money laundering and preventing counterfeit devices among others. The concept of trade-off becomes meaningful when one assumes an inherent conflict between intrusiveness and effectiveness of security.[87]

Privacy entails how the law allocates the power over information.[88] Privacy advocates that individuals have the right to freedom from intrusion of personal information and communication. The right to privacy is not absolute as it can be overridden by other interests.[89] A trade-off exists only when there is a compromise between either privacy intrusion or the efficiency of security measures.[90] When privacy is intruded for the purpose of ensuring security, there is a trade-off since privacy has been traded for security.

2.1 Relationship between privacy and security.

The relationship between privacy and security causes tension between each other as there is often a trade-off between the two. Increased security measures such as mass surveillance may breach an individual's privacy. Privacy establishes a normative framework for deciding who should have the capability to access and alter information while security implements those choices.[91] Privacy entails how the law allocates the power over information.[92] On the other hand, security

---

[87] Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention,' 105 American Political Science Review 1, 2011, 65

[88] Bambaeur D, 'Privacy and security,' 673.

[89] Miller S, 'Privacy, Encryption and Counter-terrorism,' 141.

[90] Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention,' 64.

[91] Bambaeur D, ' Privacy and security,' 669.

[92] Bambaeur D, 'Privacy and security,' 673.

determines who can access, use and alter data.[93] Therefore, security acts as an interface layer between information and privacy.[94]

Security is the set of technological mechanisms that intervene between the requests for access or control.[95] Security measures such as surveillance programs involve the collection of massive amounts of data. Security determines the privacy choices that can be implemented while privacy dictates how security options can be implemented and how they ought to develop.[96] Technological advances in surveillance are determined by the privacy choices that are implemented.

Most scholars treat security and privacy as interchangeable or intertwined.[97] Daniel Solove comes closest to distinguishing security and privacy. He contends that security executes protection and is less encompassing compared to privacy.[98] Some critics find it difficult to reconcile privacy and security.[99] As a result, placing security and privacy concerns in the wrong category may cause an insurmountable conceptual difficulty.[100]

Privacy can reasonably be overridden by security interests especially where people's lives are at risk.[101] The trade-off between privacy and security can be seen in two ways. Firstly, it can be viewed as privacy causing a barrier to effective security measures.[102] This view justifies privacy intrusion as necessary to improve security.[103] Secondly, it can be viewed as where individuals gain more security by accepting their privacy to be intruded.[104] Surveillance-oriented system technology and security policy usage are based on the assumed necessity to trade off privacy for

---

[93] Bambaeur D, 'Privacy and security,' 676.

[94] Bambaeur D, 'Privacy and security,' 676.

[95] Pozen D, 'Privacy-Privacy Trade-offs,' 83 The University of Chicago Law Review 1, 2015, 221.

[96] Bambaeur D, 'Privacy and security,' 669.

[97] Bambaeur D, 'Privacy and security,' 669.

[98] Bambaeur D, ' Privacy and security, 672.

[99] Pozen D, 'Privacy-Privacy Trade-offs,' 221.

[100] Bambauer D, 'Privacy v Security,' 2013, 670.

[101] Miller S, 'Privacy, Encryption and Counterterrorism,' 142.

[102] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between security and privacy,'260.

[103] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between security and privacy,' 260.

[104] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between security and privacy,' 260.

security.[105] There is statistical evidence against the trade-off between privacy and security at the individual level.[106] If there is privacy intrusion without the effectiveness of security measures then there is no trade-off.[107]

There is an assumption that security policies find it necessary to trade privacy for security.[108] This assumption contends that for security to improve, privacy must be reduced or intruded. From a political point of view, the trade-off puts privacy as a barrier to effective security measures and justifies privacy intrusion as a necessity to improve security.[109] Political leaders may find it necessary to intrude on people's personal information so as to improve the national security of a nation. On an individual level, the trade-off entails that an individual will gain more security if they allow more of their privacy to be intruded.[110]

Privacy can be breached where it is anticipated by the subject or where with due process it is decided that it is required for the preservation of another basic right.[111] The Data Protection Act, 2019 provides that a data processor or data controller shall ensure that personal data is collected for an explicit, legitimate and specified purpose and not further processes in a manner incompatible with the said purposes.[112]Privacy is a fundamental right but it can be limited in accordance with Article 24 of the Constitution of Kenya. Cyprian Andama v Director of Public Prosecution & another provides for a three-part test under Article 24 of the Constitution of Kenya on the limitation of a right.[113] The limitation must be under the law, must have a legitimate aim and must be necessary.[114]

---

[105] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between security and privacy,' 260.

[106] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between security and privacy,' 259.

[107] Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention,' 64.

[108] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between privacy and security,' 2017, 259.

[109] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between privacy and security,' 2017, 260.

[110] S Stefan, 'A game of hide and seek? Unscrambling the trade-off between privacy and security,' 2017, 260.

[111] Veatch R, ' Response: Limits to the right of privacy: Reason, not rhetoric,' 4 The Hasting Centre 4, 1982, 7.

[112] Section 25, Data Protection Act (Act No. 411C of 2019).

[113] Cyprian Andama v Director of Public Prosecutions & another [2019] eKLR.

[114] Cyprian Andama v Director of Public Prosecutions & another [2019] eKLR.

On a local level, law enforcement and intelligence agencies are required to comply with specific legal frameworks while gathering and processing personal data for the purpose of national security.[115] On a global scale, there is tension between the need for digital data for investigations across borders and the need to respect a country's sovereignty.[116]

In Khalifa & another v Principal Secretary, Ministry of Transport & 4 others the court held that any restriction on information that ought to be justifiable on grounds of national security must have the genuine purpose and effect of protecting a legitimate national security interest.[117] A justifiable restriction is legitimate if the purpose is to protect a country's existence or territorial integrity against the use of force or threat.[118]

The Data Protection Act provides that the collection of data from another source is necessary for the prevention, investigation, detection, prosecution and punishment of crime and the collection, storage or use of the personal data shall be for a lawful, specific and explicitly defined purpose.[119] The Act also exempts the processing of personal data if it is necessary for national security or public interest.[120]

Since the 9/11 attacks, governments have been acquiring consumer and internet activity databases that private businesses have acquired for security purposes.[121]An example in the United States of America is when the National Security Agency wiretapping program was difficult to challenge due to the invocation of national security interests.[122] The government argued that the surveillance measures were necessary for protecting the people from terrorists and maintaining national security. Therefore, it was difficult to challenge the program due to the

---

[115] Busser E, ' Big Data: The conflict between protecting privacy and securing nations,' A twenty-first century arms race,' Atlantic Council, 2017,5.

[116] Busser E, ' Big Data: The conflict between protecting privacy and securing nations,' A twenty-first century arms race,' 16.

[117] Khalifa & another v Principal secretary, Ministry of Transport & 4 others (2022) eKLR.

[118] Khalifa & another v Principal secretary, Ministry of Transport & 4 others (2022) eKLR.

[119] Section 28, Data Protection Act (Act No. 411C of 2019).

[120] Section 51, Data Protection Act (Act No. 411C of 2019).

[121] Neil R, ' The dangers of surveillance,' 27

[122] Neil R, ' The dangers of surveillance,' 27

necessity of national security. This contributes to the debate on government surveillance and national security interests.

2.2 Privacy and Counterterrorism

Citizens, policymakers and scholars approach the formation of counterterrorism policies as a balancing act between the alleged privacy values and security concerns.[123] However, privacy clashes with some social values.[124] The widely accepted assumption in scholarly debates is that reducing privacy protections increases national security from terrorism.[125]

Richard Posner points out that a government is entitled to data for the limited purpose of national security.[126] The justification for reducing privacy is that security increases from terrorism as anti-terrorist agencies can easily gain access to information and collect information related to terrorism prevention.[127]

Privacy encompasses control over information about a person and freedom from surveillance.[128] Surveillance technology enables us to combat issues such as terrorism.[129] Privacy is considered the price paid for security.[130] An example of situations where privacy is reduced is when governments collect massive personal information on people so as to gain insights into behaviour

---

[123]Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention, 64.

[124] Pozen D, 'Privacy-Privacy Trade-offs,' 221.

[125] Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention,' 64.

[126] Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention,' 65.

[127] Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention,' 65.

[128] Skaug H, 'The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security,' 68 Technology in Society, 2022, 2.

[129] Skaug H, 'The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security,' 2.

[130] Skaug H, 'The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security,' 2.

patterns which helps them to identify terrorists.[131] When the public becomes aware of this, massive protests are carried out by the people.[132]

The Prevention of Terrorism Act, 2012 provides that the right to privacy shall be limited to the extent of allowing the privacy of a person's communication to be investigated, intercepted or otherwise interfered with.[133] It also provides the right to privacy shall be limited for the purpose of intercepting communication directly relevant in detecting, deterring and disrupting terrorism.[134] Despite the counterterrorism strategy in Kenya, terrorism is still a major threat to Kenya's national security.[135] Some counterterrorism measures have enabled human rights abuses.[136] Kenyan legislation on counterterrorism does not address any issues on privacy but addresses issues on association.[137]

Privacy International released a report which accused Kenyan security agencies of violating the right to privacy and using information collected to commit human right abuses.[138] The United Nations Special Rapporteur notes that some security measures taken by some governments in order to combat terrorism may fuel discrimination against certain groups due to their migration status, religion or ethnic origin.[139] In Kenya, the government launched an operation to increase the policing of certain ethnic minorities and Muslim communities as a response to terror attacks.[140]

---

[131] Skaug H, 'The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security,' 3.

[132]Skaug H, 'The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security,' 3.

[133] Section 35(3), Prevention of Terrorism Act (Act No. 59B of 2012)

[134] Section 36A, Prevention of Terrorism Act (Act No. 59B of 2012)

[135] Kamau J, 'Is Counterterrorism Counterproductive? A case study of Kenya's response to terrorism, 1998-2020,' 28 South African Journal of International Affairs 2, 2021 https://www.tandfonline.com/doi/full/10.1080/10220461.2021.1924252 on 11th February 2024.

[136] https://www.counterextremism.com/countries/kenya-extremism-and-terrorism on 11th February 2024.

[137] https://www.counterextremism.com/countries/kenya-extremism-and-terrorism on 11th February 2024.

[138] https://www.counterextremism.com/countries/kenya-extremism-and-terrorism on 11th February 2024.

[139] Universal Periodic Review, The Right to Privacy in Kenya, 2019, 3.

[140] Universal Periodic Review, The Right to Privacy in Kenya, 2019, 3.

Democratic societies face inevitable trade-offs in the face of potential terrorist attacks.[141] In Coalition for Reform and Democracy & 2 others v the Republic of Kenya, the petitioners argued that section 36A of the Prevention of Terrorism Act was an infringement on the right to privacy as it allowed for the mass interception of communication by national security organs.[142] The Security Laws (Amendment) Act amended the Prevention of Terrorism Act by introducing section 36A. It provides that national security organs may intercept communication for the purpose of detecting, deterring and disrupting terrorism and the right to privacy shall be limited under the section for the purpose of intercepting communication directly relevant in detecting, deterring and disrupting terrorism.[143] The court held that although section 36A of the Prevention of Terrorism Act limits the right to privacy, it is justifiable in a free and democratic state and has a rational connection with the intended purpose as provided for.[144]

Conclusion.

In conclusion, the trade-off between key government objectives and maintaining privacy concerns in the context of mass surveillance reveals a varied relationship. The relationship between privacy is not balanced as privacy is often traded for security. There is also some difficulty in balancing an individual's right to privacy and broader societal interests. There seems to be an assumption that privacy has to be given up so that the government can achieve its key objectives such as security and counterterrorism. Finding a balance between privacy and key government objectives in the context of mass surveillance may be very necessary.

---

[141]Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention,' 64.

[142] Coalition for Forum and Democracy (CORD) & 2 others v Republic of Kenya & 10 others [2015] eKLR.

[143] Section 69, Security Laws (Amendment) Act, (Act No. 19 of 2014).

[144] Coalition for Forum and Democracy (CORD) & 2 others v Republic of Kenya & 10 others [2015] eKLR.

CHAPTER 3: WHAT ARE THE POTENTIAL PRIVACY CONCERNS AND EFFECTS OF THE COLLECTION, STORAGE, USE AND DISCLOSURE OF INFORMATION THROUGH MASS SURVEILLANCE IN KENYA.

Introduction.

The collection, storage, use and disclosure of information through mass surveillance has brought about privacy concerns and their effects. Some concerns arise with the invasion of personal information such as social stigmatization, profiling of individuals and data breaches. Surveillance of electronic communication either by public authorities or private individuals is prohibited.[145]

This chapter will discuss the potential privacy concerns that mass surveillance through the device management system may bring about. It will discuss the effects of collecting, storing, using and disclosing information through mass surveillance. It will also discuss certain theories that will help in understanding privacy and surveillance.

3.1 Theoretical framework and understanding of privacy.

Intersubjective theories of privacy focus on privacy as a common value that is necessary to enable individuals' activities within communities.[146] It entails enabling social interaction as it is necessary for individuals within a community to freely interact with each other to protect an individual's relationship with others. It shifts the view of harm to focus on how a community is affected by surveillance and how such surveillance has a derivative effect on public engagement before focusing on the individual.[147] This theory will aid in understanding the importance of privacy in a community. This theory recognizes privacy as both an individual right and a shared value within a community. Individuals in a community all benefit when each person's privacy is respected. Surveillance can bring about some implications on public engagement.

Theorists such as Regan argue that privacy is more of an attribute of social relationships and information systems on the basis that privacy holds a public value, a collective value and a

---

[145] Watt E, 'The right to privacy and the future of mass surveillance,' 21 The International Journal on Human Rights 7, 2017, 778 https://doi.org/10.1080/13642987.2017.1298091 on 10th December 2023.

[146] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 3 University of Toronto 3, 2015, 5.

[147] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 6.

common value.[148] This suggests that privacy is not only an individual interest but also a broader societal interest. The way an individual handles their private information may have implications in the public space and on the wellbeing of a community. The private autonomy of an individual and the autonomy shown in engaging in public action are co-original.[149] They exist simultaneously and are interconnected. An individual's capacity for private autonomy and engagement in public activities are interconnected.

On the other hand, a scholar known as Nissenbaum focuses on privacy as being a right where the expectations on the flow of personal information are mostly met.[150] She determines whether an intrusion has occurred through her work on contextual integrity where integrity is preserved when informational standards are met and is violated if the standards have been breached.[151] Nissenbaum lies more toward legally established standards that are widely accepted in communities because judges are responsible for determining whether contextual integrity based on an informational standard infringes on an individual's reasonable expectation of privacy.[152] The community that an individual belongs to is used to determine an inappropriate intrusion into personal activities. [153]This may be problematic due to reasons such as new technology, differing accounts of what should constitute a reasonable expectation of privacy and signal intelligence-based surveillance goes beyond national boundaries.[154]

3.2 Privacy concerns and effects of mass surveillance.

The collection of information on the relationship between individuals and groups may weaken human and organizational bonds in the public sphere.[155] The information on the relationship between individuals is collected by the Device Management Systems as they intercept communications between individuals. The threat or knowledge of surveillance may make it

---

[148] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 5.

[149] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 7.

[150] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 5.

[151] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 5.

[152] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 5.

[153] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 5.

[154] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 5.

[155] Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,'

difficult for individuals and groups to communicate freely.[156] It may also make others who are aware of the surveillance hesitant to interact with those under surveillance due to fear of also falling under surveillance.[157] This may limit interactions between individuals, especially in the public sphere due to fear of surveillance. This may lead to a change in the behaviour, composition and focus on the ideas of the public.[158] As a result, surveillance creates an atmosphere of fear, distrust and avoidance of public engagements.[159] An individual's relations in the public sphere and their perception of public participation are affected by surveillance. The social stigma brought about by mass surveillance may lead to alienation and discrimination.

The fundamental interest behind the notion of global privacy is to cope with modern surveillance technologies as technology companies feel that society has abandoned privacy hence encouraging users to dispense with privacy.[160] A petition for global privacy argues that 'a person under surveillance is no longer free and a society under surveillance is no longer a democracy.'[161] It suggests that a person under surveillance loses their freedom and a society under surveillance loses its democratic nature. The petition also argues that democratic rights should apply to the virtual space as they do in the real space.[162] It further suggests that democratic citizens should be able to determine the extent to which their personal data may be legally collected, stored and processed and who should be able to do this.[163]

Leakage of personal information collected through mass surveillance may make it possible for profiling of individuals and this information may be used to steal or misuse a person's dignity, blackmail or threaten.[164] Profiling also causes stigmatization as a result of singling out

---

[156] Raab C, 'Surveillance: Effects on privacy, autonomy and dignity,' in Wright D and Kreissl R (eds) *Surveillance in Europe*, Routledge, London, 2014, 270.

[157] Raab C, 'Surveillance: Effects on privacy, autonomy and dignity,' 270.

[158] Raab C, 'Surveillance: Effects on privacy, autonomy and dignity,' 270.

[159] Raab C, 'Surveillance: Effects on privacy, autonomy and dignity,' 270.

[160] Kampmark B, 'Restraining the surveillance state: A Global Right to Privacy,' 2 The Journal of Faultlines 1,2014, 7.

[161] Kampmark B, 'Restraining the surveillance state: A Global Right to Privacy,' 4.

[162] Kampmark B, 'Restraining the surveillance state: A Global Right to Privacy,' 4.

[163] Kampmark B, 'Restraining the surveillance state: A Global Right to Privacy,' 4.

[164] Haggen J,' Protecting the digitized society- the challenge of balancing surveillance and privacy,' 1 The Cyber Defense Review 1, 2016, 84.

individuals from a group due to suspicion.[165] Those who face stigmatization may disengage from participating in certain public activities and interacting with other people.[166] Profiling leads to discrimination where personal information is misused which may negatively impact a person's life. An example that demonstrates the effect of leakage of personal information is December 2015 in the United States of America, where a database on the personal information of American voters leaked causing a police officer to be concerned that criminals could be able to find his home address.[167] This information can be used to obtain more private information about individuals.[168] Unauthorized access to information collected through mass surveillance compromises the privacy of an individual hence violating their right not to have information regarding their family or private affairs unnecessarily revealed and the right to not have the privacy of their communication infringed. The terror attacks in Kenya have raised issues on the protection of human rights especially since it leads to ethnic and religious profiling. The installation of the Device Management System could expose Kenyans to such fears if their information is leaked.

Storage of information on unsecured servers and registries is a challenge for privacy.[169] Unauthorized access to personal and sensitive information stored in unsecured servers and registries may lead to data breaches. Data breaches can occur due to data on physical media getting lost, stolen or not secured.[170] Data stolen from such servers can be used to defraud and steal the identities of the victims of data breaches.[171] Governments and information technology companies that create data registries that do not protect personal information will face challenges and security issues may arise in the future.[172] The Kenya Information and Communications Act provides that a license granted to a person to provide electronic certification services requires

---

[165] Hadjimatheou K, 'The Relative Moral Risks of Untargeted and Targeted Surveillance,' 17 Ethical Theory and Moral Practice, 2014, 192.

[166] Hadjimatheou K, 'The Relative Moral Risks of Untargeted and Targeted Surveillance,' 194.

[167] Haggen J,' Protecting the digitized society- the challenge of balancing surveillance and privacy,' 83.

[168] Haggen J,' Protecting the digitized society- the challenge of balancing surveillance and privacy,' 83.

[169] Haggen J,' Protecting the digitized society- the challenge of balancing surveillance and privacy,' 10.

[170] Froomkin M, 'Government data breaches,' University of Miami Legal Studies, Research paper Number 20, 2009, 1026 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427964 on 17th December 2023.

[171] Sharma N, Oriaku E and Oriaku N 'Cost and Effects of data breaches, Precautions and Disclosure Laws,' 8International Journal of Emerging Trends in Social Sciences 1, 2020, 37.

[172] Haggen J,' Protecting the digitized society- the challenge of balancing surveillance and privacy,' 84.

them to make use of hardware, software and procedures that are secure from intrusion and misuse.[173] The Act also provides that any person who attempts or acquires unauthorized access to a protected system commits an offense and may be convicted, fined or imprisoned.[174]

Surveillance affects self-development as it extends its reach and enhances the power of social shaping.[175] Surveillance goes against self-development as it alters with the processes of individuals and communities engaging in practices that consist of mutual self-definition that are open-ended.[176] It undermines the open-endedness of this process. Subjectivity exists within social shaping because it controls the process of self-development.[177] The interstices between self-development and subjectivity are larger and the linkages are incomplete.[178] Therefore, surveillance goes against the link between subjectivity and self-development as it seeks to take away the 'breathing room' that subjectivity requires.[179] Surveillance shapes behaviour and the sense of identity when it fosters norms of continual and pervasive observation and tracking.[180] Pervasive networked surveillance also causes division which brings about incivility and intolerance.[181]

Surveillance for informational transparency imposes logic, presumptions and biases by making its subjects more susceptible to prediction, observation and suggestion.[182] This can influence individuals to conform to perceived norms or to alter their behaviour to align with certain expectations. On the other hand, surveillance for the purpose of exposure works to instil a sense of continual observation and this alters the ability of places to function within their identity.[183] A

---

[173] Section 83E(2), Kenya Information and Communications Act (Act No. 2 of 1998).

[174] Section 83Q(3), Kenya Information and Communications Act (Act No 2 of 1998).

[175] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' in Gray D and Henderson S (eds) *Cambridge Handbook of Surveillance,* Cambridge University Press, New York, 2017, 5.

[176] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' 5.

[177] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' 6.

[178] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' 6.

[179] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' 6.

[180] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' 6.

[181] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' 7.

[182] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' 9.

[183] Cohen J, 'Surveillance vs Privacy: Effects and Implications,' 9.

sense of continual observation is created and this can lead to self-regulation. This resembles Jeremy Bentham's panopticon theory.

Article 17 of the International Covenant on Civil and Political Rights (hereafter 'ICCPR') provides that no one should be subjected to arbitrary or unlawful interference with his privacy, home or correspondence.[184] It also provides that everyone has a right to protection against interference or attacks through the law.[185] This aligns with Article 31 of the Constitution of Kenya which recognizes and protects the right to privacy. This article protects people in Kenya from unlawful interference with their privacy. Interference of privacy must be in accordance with Kenyan laws.

In Nubian Rights Forum & 2 others v Attorney General & 6 others, the first petitioner filed a witness statement from an expert witness who raised a concern that the collection of personal data through the National Integrated Identity Management System would bring about fear of mass surveillance.[186] He opined that the government can conduct surveillance on its citizens from the data collected.[187] He expressed that mass surveillance should not be allowed but targeted surveillance may be allowed.[188] The National Integrated Identity Management System is established by section 9A of the Registration of Persons Act.[189] It is supposed to be a single source of personal information of Kenyans and foreign residents in Kenya.[190] The court held that information collected for identification is intrusive and unnecessary hence a violation of Article 31 of the Constitution of Kenya.[191]

The decision in the Coalition for Reform and Democracy & 2 others v the Republic of Kenya case where the court justifies and allows mass surveillance by national security organs to combat terrorism. The court prioritizes national security over individual privacy. Conversely, in the

---

[184] Article 17, International Covenant on Civil and Political Rights, 16 December 1966, 2200A (XXI).

[185] Article 17, ICCPR.

[186] Nubian Rights Forum & 2 others v Attorney General & 6 others [2020] eKLR

[187] Nubian Rights Forum & 2 others v Attorney General & 6 others [2020] eKLR

[188] Nubian Rights Forum & 2 others v Attorney General & 6 others [2020] eKLR

[189] Section 9A(1), Registration of Persons Act (Act No. 107 of 1949).

[190] Nubian Rights Forum & 2 others v Attorney General & 6 others [2020] eKLR

[191] Nubian Rights Forum & 2 others v Attorney General & 6 others [2020] eKLR

decision in the Nubian Rights Forum & 2 others v Attorney General & 6 others case, the court prioritizes an individual's right over government surveillance activities. The contradiction between the two decisions demonstrates the tension between privacy rights and other government interests.

Conclusion.

To sum it all up, the analysis of the potential privacy concerns and effects that may arise from the collection, storage, use and disclosure of information through mass surveillance in Kenya reveals a series of implications that may arise. These concerns show the need for a comprehensive approach to the protection of privacy in light of the evolving mass surveillance technologies. The installation of Device Management Systems could expose Kenyans to such risks unless comprehensive legal and technical provisions are created to protect consumers are put in place.

The intersubjective theories of privacy, Regan's and Nissenbaum's theories provide diverse perspectives on privacy. They highlight the communal nature of privacy and the relationship between private autonomy and public engagement. Additionally, the analysis reveals the surveillance of the relationships between individuals and communities poses a threat to the organizational bonds in the public sphere. The fear or knowledge of surveillance may limit free communication leading to fear and distrust. Democratic citizens ought to have the control over the collection, storage and processing of their personal data in both the virtual and real space so that the global standards of privacy are protected. Leakage of information from mass surveillance poses threats such as profiling and identity theft. Storage of information on unsecured servers increase such risks.

CHAPTER 4: WHETHER THE INTERCEPTION OF COMMUNICATION THROUGH DEVICE MANAGEMENT SYSTEMS LEADS TO THE INTERFERENCE OF AN INDIVIDUAL'S RIGHT TO PRIVACY AND IF THE INTERFERENCE IS JUSTIFIABLE.

Introduction.

The interception of communication through the device management system may lead to an interference with an individual's right to privacy. However, there may be justifiable limits to interference with an individual's privacy that may in turn allow mass surveillance to take place.

The collection of data beyond what is consented to by the individual raises a privacy concern.[192] Threats can leak and extract confidential data stored in the device management systems.[193] The Device Management Systems can collect information from mobile phone users and this allows for mass surveillance by the government and other authorities. Collection of data by the Device Management Systems without an individual's consent or collecting beyond what is consented violates their right to privacy.

This chapter will discuss the principles necessary for surveillance to be lawful. It will also discuss situations where interference of one's privacy is justifiable focusing on national security.

4.1 Principles necessary for lawful surveillance.

International human rights law provides three principles necessary for assessing the lawfulness of surveillance. In Kenya, activities such as surveillance that limit the right to privacy can only be justified when they are prescribed by law, proportionate to the aim pursued and necessary to achieve a legitimate aim.[194]

Firstly, the domestic law of a country must allow for surveillance. The legal requirements of a country should be accessible to the public, clear, precise, comprehensive and non-

[192] Hayes D, ' An effective approach to mobile device management: security and privacy issues associated with mobile applications,' 1 Digital Business 1, 2020, 2.

[193] Rhee K, 'Security Requirements of a Mobile Device Management System', 6 International Journal and its Applications 2, 2012, 355.

[194] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

discriminatory.[195] Regulation 15 of the Kenya Information and Communications(consumer protection) Regulations provides that subject to the provisions of the Kenya Information and Communications Act and any other written law, a licensee is prohibited from monitoring, disclosure or permitting any person to monitor or disclose the content of any information of any subscriber transmitted through licensed systems either by listening, tapping, storage or other kinds of surveillance of communications and associated data.[196] Therefore, surveillance activities through licensed systems are prohibited in Kenya. The installation of device management systems on mobile phone networks enables mass surveillance to occur which is contradictory to the provisions of the Kenyan law.

In Okoiti v Communications Authority of Kenya & 8 others, the petitioner claimed that there was no proper legal framework back the Device Management System.[197] The court held that access to information can only be lawful when it is within the parameters provided for in section 27A of the Kenya Information and Communications Act.[198]

Secondly, the principle of proportionality and necessity is an element of lawful surveillance.[199] Proportionality should consider the effectiveness of the program against its privacy intrusion.[200] The law of a state determines the boundaries of proportionality.[201] The laws in Kenya provide that where applicable a licensee shall establish a mechanism by which customers can know that information is being collected about them through using their telecommunication services and systems and where customers may be able to receive conspicuous notice that the information could be used or is intended to be used without authorization by the entity collecting the data for reasons unrelated to the original communication or could be sold to another entity.[202] In order to establish that the interference of privacy is necessary, a state has to show that the interference

---

[195] Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' The Global Expansion on AI Surveillance, 2019, 12.

[196] Regulation 15(1), Kenya Information and Communications (consumer protection) Regulations (2010).

[197] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[198] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[199] Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' 12.

[200] Cayford M, 'The effectiveness of surveillance technology: what intelligence officials are saying,' 34 The Information Society 2, 2018, 89 https://doi.org/10.1080/01972243.2017.1414721 on 27th December 2023.

[201] Cayford M, 'The effectiveness of surveillance technology: what intelligence officials are saying,' 100

[202] Regulation 15(2), Kenya Information and Communications (consumer protection) Regulations (2010).

with a person's right achieves a social need and it is proportionate to the legitimate aim pursued.[203] The surveillance cannot be more than is necessary to address the urgent social need.[204] Surveillance has to be proportionate and necessary to achieve a public or social need.

Some opine that mass surveillance can never be accepted as proportionate.[205] Interference with privacy must be reasonable and necessary in the circumstances of a state.[206] In a situation where a terror attack is foreseen, surveillance may be reasonable and necessary to prevent the attack from happening. Although there are many disadvantages of mass surveillance, it prevents any single intelligence agency from having disproportionate access to surveillance data.[207]

In Okoiti v Communications Authority of Kenya & 8 others, the High Court was of the view that the proportionality test is a common way of determining whether the limitation of a right is justifiable.[208] The test includes whether legislation establishing the limitation of a right pursues a legitimate objective of sufficient interest to justify the limit of the right, whether the means used towards achieving the objective rationally connected to the objective, whether the means used towards achieving the necessary objective minimally impairs the limited right taking into account different means of achieving the same objective and whether the beneficial effects of limiting the right outweigh the effects of the limitation.[209]The learned judge also opined that the court would have to ask itself whether the end could be reached using less drastic measures.[210] The court held that the Communications Authority of Kenya lacks the statutory mandate of combating with illegal devices.[211] There are other lawful and less restrictive institutions such as the Kenya Bureau of Standards that have not been shown to be insufficient.[212] There are lawful

---

[203] Watt E, 'The right to privacy and the future of mass surveillance,' 782.

[204] Watt E, 'The right to privacy and the future of mass surveillance,'782.

[205] Kampmark B, 'Restraining the Surveillance State: A global Right to Privacy,' 2.

[206] Kampmark B, 'Restraining the Surveillance State: A global Right to Privacy,' 4.

[207] Akin H, 'Politics of Digital Surveillance, National Security and Privacy,' Centre for Economics and Foreign Policy Studies, 2018, 14.

[208] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[209] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[210] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[211] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[212] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

and less restrictive means that can be used to achieve the objective of combating illegal devices other than accessing information of subscribers as this will infringe on their right to privacy.

Lastly, there should be a legitimate interest to justify surveillance.[213] The surveillance action should be necessary to achieve a legitimate aim.[214] Governments may have legitimate reasons to carry out surveillance.[215] These reasons should not have their interests rooted in political repression and limiting individuals' freedoms.[216] This may require a state to demonstrate the risk that surveillance may bring up to an interest in national security or public order.[217] Surveillance should only apply when the interest of a whole state is at risk and not in the interest of the government.[218] The High Court applied this principle in Okoiti v Communications Authority of Kenya & 8 other. It held that reasonableness is determined by considering whether there is a valid and rational connection between the limitation and a legitimate public interest to justify it.[219]

Article 24 of the Constitution of Kenya provides that a right shall not be limited except by law and only to the extent that the limitation is reasonable and justifiable in an open democratic society based on human dignity, equality and freedom.[220] Certain factors are taken into account such as the importance of the purpose of limitation.[221]

4.2 Justifiability of mass surveillance.

States do not enjoy unlimited discretion to subject the people in their jurisdictions to secret surveillance.[222] They cannot adopt any measures they deem appropriate in the name of the struggle against terrorism.[223] They are only tolerable if these means are provided for by the

---

[213] Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' 12.

[214] Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' 12.

[215] Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' 11.

[216] Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' 12.

[217] Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' 12.

[218] Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' 12.

[219] Okiya Omtatah Okoiti v Communications Authority of Kenya & 8 others [2018] eKLR.

[220] Article 24(1), Constitution of Kenya (2010)

[221] Article 24(1), Constitution of Kenya (2010)

[222] Watt E, 'The right to privacy and the future of mass surveillance,'781.

[223] Watt E, 'The right to privacy and the future of mass surveillance,'781.

legislation to achieve these aims and remain within the bounds of what is necessary in a democratic society.[224] Any measure taken in the name of preventing terrorism should be within the bounds of what is necessary in a democratic society.

A legitimate national security threat may justify the intrusion of privacy.[225] National security encompasses the decisions and actions seemingly imperative to protect core values from external attacks.[226] Arnold Wolfers opines that national security is an ambiguous symbol as it lacks uniformity.[227] The concept of national security can be interpreted differently by different governments. Surveillance can be used as a national security strategy and other components such as counterterrorism, criminal profiling and counternarcotics.[228] However, surveillance that enhances security must not be overly intrusive or life-altering.[229] This shows the commitment to maintaining a reasonable balance between privacy and national security.

Surveillance by the government has been under public scrutiny as some argue that it is necessary for increased security and others argue that it is an invasion of privacy.[230] In democracies, public consent is a fundamental feature. The public can eliminate leaders who abuse surveillance powers and misuse state secrecy tools. [231] They can also pressure the government when there is doubt that the information collected through mass surveillance is mishandled.[232]

There are instances where states misuse secrecy in the name of national security. National security secrets are often used to hide mismanagement, corruption or poor prioritization.[233] This shows a concern on potential abuse of power regarding surveillance. This is through using state-owned surveillance tools to spy on the opposition or citizens even where a national security

---

[224] Watt E, 'The right to privacy and the future of mass surveillance,'781.

[225] Parsons C, 'Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance,' 5.

[226] Leffler M, 'National Security,' 77 The Journal of American History 1, 1990, 143.

[227] Wolfers A, " National Security" as an ambiguous symbol,' 67 Political Science Quarterly 4, 1952, 490.

[228] Akin H, 'Politics of Digital Surveillance, National Security and Privacy,' 14.

[229] Moore A, 'Privacy, Security and Government Surveillance: Wikileaks and the new accountability,' 25 Public Affairs Quarterly 2, 2011, 141.

[230] Cayford M, 'The effectiveness of surveillance technology: what intelligence officials are saying,' 88.

[231] Akin H, 'Politics of Digital Surveillance, National Security and Privacy,' 15.

[232] Akin H, 'Politics of Digital Surveillance, National Security and Privacy,' 4.

[233] Akin H, 'Politics of Digital Surveillance, National Security and Privacy,' 4.

threat is absent.[234] Surveillance in this case is used to hide actions that are not related to security concerns. Daniel Solove opines that giving governments too much power undermines the objective of providing security as the government itself becomes a threat to security.[235] When the government has too much power in surveillance matters, a threat to the very security it aims to protect may arise.

The 'Nothing to hide' argument opines that the potential harm of data mining and the security interests of detecting and preventing terrorist attacks are to be balanced.[236] This argument implies that if individuals have nothing to hide then they should willingly accept a certain level of their privacy to be intruded for the sake of security. It also shows that there is a trade-off between security and privacy. It is of the idea that the security interest often carries more weight than the minimal costs of surveillance.[237] This means that privacy intrusions are a nuisance and are easily traded for an increase in security.[238] The benefits of increased security may at times outweigh the cost of privacy intrusions.

Oversight mechanisms are important as they act as a bridge of public consent for surveillance and establish and monitor safeguards with the government.[239] These mechanisms could play a crucial role in ensuring that surveillance activities in a state align with the interests of the public. They can hold the government accountable for the surveillance activities within a state.

Conclusion.

To sum it all up, some principles are necessary for surveillance to qualify as lawful. They are required to be present while carrying out surveillance activities so that they can be deemed as lawful. Kenyan law lacks provisions that show these principles clearly. Therefore, it is difficult to determine whether surveillance activities are lawful. The installation of the Device Management System should only be allowed where it is proportionate, reasonable, and lawful in order to ensure that the privacy of individuals is protected.

---

[234] Akin H, 'Politics of Digital Surveillance, National Security and Privacy,' 4.

[235] Moore A, 'Privacy, Security and Government Surveillance: Wikileaks and the new accountability,' 146.

[236] Moore A, 'Privacy, Security and Government Surveillance: Wikileaks and the new accountability,' 145.

[237] Moore A, 'Privacy, Security and Government Surveillance: Wikileaks and the new accountability,' 146.

[238] Moore A, 'Privacy, Security and Government Surveillance: Wikileaks and the new accountability,' 146.

[239] Akin H, 'Politics of Digital Surveillance, National Security and Privacy,' 15.

National security is a justifiable limit to the right to privacy concerning mass surveillance. However, there are instances where the government has too much power leading to abuse of surveillance powers. They can use surveillance to hide corruption and mismanagement. The 'nothing to hide argument' presents the view that security interests may require intrusion of individuals' privacy hence if there is nothing they are hiding they should willingly allow a certain level of intrusion of their privacy. This is to achieve the objective of national interest or social order.

Kenya requires an oversight mechanism that will establish safeguards to protect the fundamental rights and freedoms of the public and monitor the surveillance activities of the government. The mechanism will also determine when surveillance is necessary so as to avoid unnecessary privacy intrusion. It will ensure that public interest is upheld and public consent is given to surveillance activities, especially through the electronic media.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS.

Conclusion.

The right to privacy is guaranteed in the Constitution of Kenya (2010) and other domestic and international legal provisions. However, with mass surveillance this right is threatened and undermined. Failure to protect this right will lead to a violation of individuals' fundamental rights and freedoms as provided for in the Bill of Rights.

Serious concerns have been raised relating to mass surveillance in Kenya. The installation of device management systems in mobile phone networks poses the risk of mass surveillance. The interception of communication is an intrusion of an individual's privacy. The people of Kenya are concerned that this may give the government too much power leading to an abuse of this power. Other countries have made and implemented laws that govern the surveillance of communications. Kenya's laws such as the Kenya Information and Communications Act are lacking in protecting and providing measures to protect the communication between persons. The existing laws are not well implemented in Kenya.

It is difficult to balance privacy and other government interests such as national security, public order and counterterrorism among others. There is an inevitable trade-off between privacy and security. Mass surveillance through interception of communication brings about some potential privacy concerns such as profiling. However, there are justifiable limits to the right to privacy hence allowing mass surveillance to occur. This includes situations where there is a threat to national security such as a terror attack. Kenyan law prohibits surveillance but does not provide for instances where mass surveillance may be justified and allowed at the cost of privacy. Generally, there is a lack of urgency in the Kenyan legal regime in developing proper legislation concerning the right to privacy and surveillance.

The first chapter begins by introducing the study, chapter two discusses the trade-off between privacy and other government objectives, chapter three has given potential privacy concerns that may arise when communication is intercepted, chapter four has given the justifiable limits of privacy to allow mass surveillance and chapter five will give the conclusion and recommendation on the way forward.

Recommendations.

The study above proposes the following recommendations:

1. The legislative body of the government of Kenya ought to create laws and regulations concerning surveillance activities especially communication surveillance and the protection of fundamental rights and freedoms so as to avoid any legal problems, confusion or threats and to prevent any situations where the law does not address matters that are of public concern.
2. The Communications Authority of Kenya should apply the laws governing communication surveillance in Kenya while installing the Device Management Systems and keep the government and other surveillance agencies accountable while carrying out surveillance. The rollout of the Device Management Systems should put in place specific safeguards such as collecting data necessary for the intended purpose, applying strong encryption methods, obtaining consent from users before collecting their personal data and implementing comprehensive security measures so as to protect the privacy of individuals.
3. The recommended legislation and regulations to be created should consider the scholarly approaches and international human rights law and principles while creating the law on surveillance.
4. The judiciary should be given the mandate to determine whether the intrusion of privacy of the population's or one's communication is necessary and to give or deny warrants in that regard.
5. The Kenya Information and Communications Act should include measures to ensure that mobile phone users give their consent to be subjected to surveillance knowingly and willingly.

BIBLIOGRAPHY.

Journal articles

1. E Braten, 'Autonomous IoT Device Management Systems: Structure Review and Generalized Cognitive Model,' Internet of Things Journal, 2021.
2. Miller R, Miller J, 'Jeremy Bentham's Panoptic Device,' 41 The MIT press, 1987.
3. Neil M, 'The dangers of surveillance,' 126 Harvard Law Review 7, 2013.
4. Dragu T, 'Is there a trade-off between security and liberty? Executive Bias, Privacy Protections and Terrorism Prevention,' 105 American Political Science Review 1, 2011.
5. Pozen D, 'Privacy-Privacy Trade-offs,' 83 The University of Chicago Law Review 1, 2015.
6. Skaug H, 'The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security,' 68 Technology in Society, 2022.
7. Parsons C, 'Beyond Privacy: Articulating the broader harms of pervasive mass surveillance,' 3 University of Toronto 3, 2015.
8. Kampmark B, 'Restraining the surveillance state: A Global Right to Privacy,' 2 The Journal of Faultlines 1,2014.
9. Haggen J,' Protecting the digitized society- the challenge of balancing surveillance and privacy,' 1 The Cyber Defense Review 1, 2016.
10. Hadjimatheou K, 'The Relative Moral Risks of Untargeted and Targeted Surveillance,' 17 Ethical Theory and Moral Practice, 2014.
11. Hayes D, ' An effective approach to mobile device management: security and privacy issues associated with mobile applications,' 1 Digital Business 1, 2020.
12. Leffler M, 'National Security,' 77 The Journal of American History 1, 1990.
13. Wolfers A, " National Security" as an ambiguous symbol,' 67 Political Science Quarterly 4, 1952
14. Moore A, 'Privacy, Security and Government Surveillance: Wikileaks and the new accountability,' 25 Public Affairs Quarterly 2, 201

Online journals

1. Galic M, ' Bentham, Deleuze and beyond: an overview of surveillance theories from the panopticon to participation,' 2016 https://link.springer.com/article/10.1007/s13347-016-0219-1#Sec2
2. Stahl T, 'Indiscriminate mass surveillance and the public sphere,' 18 Ethics Inf Technol, 2016 https://link.springer.com/article/10.1007/s10676-016-9392-2
3. Kamau J, 'Is Counterterrorism Counterproductive? A case study of Kenya's response to terrorism, 1998-2020,' 28 South African Journal of International Affairs 2, 2021 https://www.tandfonline.com/doi/full/10.1080/10220461.2021.1924252
4. Watt E, 'The right to privacy and the future of mass surveillance,' 21 The International Journal on Human Rights 7, 2017, 778 https://doi.org/10.1080/13642987.2017.1298091
5. Froomkin M, 'Government data breaches,' University of Miami Legal Studies, Research paper Number 20, 2009, 1026 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427964
6. Cayford M, 'The effectiveness of surveillance technology: what intelligence officials are saying,' 34 The Information Society 2, 2018, 89 https://doi.org/10.1080/01972243.2017.1414721

Book Chapters

1. Halborg S, 'Panopticon: a critique,' in Foo F (ed) *UCL Jurisprudence Review*, 28 Law Journal library, 1995.
2. Cohen J, 'Surveillance vs Privacy: Effects and Implications,' in Gray D and Henderson S (eds) *Cambridge Handbook of Surveillance,* Cambridge University Press, New York, 2017.
3. Raab C, 'Surveillance: Effects on privacy, autonomy and dignity,' in Wright D and Kreissl R (eds) *Surveillance in Europe*, Routledge, London, 2014.
4. S Stefan, 'A game of hide and seek? Unscrambling the trade-off between security and privacy,' in Friedewald M(ed), *Surveillance, privacy and Security*, 1ed, Routledge, London, 2017.

Books.

1. Foucault M, ' Discipline and punish: The birth of the prison, Knopf Doubleday Publishing Group, 1995.
2. Busser E, ' Big Data: The conflict between protecting privacy and securing nations,' A twenty-first century arms race,' Atlantic Council, 2017.

Theses.

1. Bonello R, 'Mass surveillance and the right to privacy,' published LLM thesis, Universiteit Leiden, Leiden 2016.
2. Schermer B, 'Software agents, surveillance and the right to privacy: a legislative framework for agent enabled surveillance,' published doctoral thesis, Leiden University Leiden, 2007.

Reports.

1. Universal Periodic Review, The Right to Privacy in Kenya, 2019.
2. Feldstein S, 'Distinguishing between legitimate and unlawful surveillance,' The Global Expansion on AI Surveillance, 2019.
3. Akin H, 'Politics of Digital Surveillance, National Security and Privacy,' Centre for Economics and Foreign Policy Studies, 2018.

UN documents.

1. UNGA, The right to privacy in the digital age, UN A/Res/75/176 (16th December 2020).

International instruments.

1. International Covenant on Civil and Political Rights, 16 December 1966, 2200A (XXI).

Online Sources.

1. https://www.privacyinternational.org/learn/mass-surveillance
2. https://privacyinternational.org/learn/mass-surveillance#:~:text=Mass%20surveillance%20is%20indiscriminate%20surveillance,is%20reasonable%20suspicion%20of%20wrongdoing

3. https://www.businessdailyafrica.com/bd/economy/state-linked-to-mass-mobile-phone-surveillance-plot-3992454
4. https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management
5. https://www.counterextremism.com/countries/kenya-extremism-and-terrorism
6. https://restofworld.org/2023/kenya-device-management-system-digital-rights-activists/
7. https://gadgets-africa.com/2023/12/04/ca-phones-kenya/#:~:text=The%20Communication%20Authority%20of%20Kenya%20%28CA%29%20intends%20to,end%20the%20proliferation%20of%20counterfeit%20devices%20and%20theft