STRIKING A BALANCE: NAVIGATING THE INTERSECTION OF NATIONAL SECURITY INTERESTS' AND THE RIGHT TO PRIVACY IN SURVEILLANCE PRACTICES

Submitted in partial fulfilment of the requirements of the Bachelor of Laws Degree,

Strathmore University Law School

By:

Lindsay Leslie Nyabonyi O

133582

Submitted on this …15th**…. Day of …**June……**. 2024**

Word Count: 14,578 (excluding footnotes and table of contents).

Table of Contents

ACKNOWLEDGEMENT

I would like to extend my heartfelt gratitude to my dissertation supervisor for her unwavering guidance, support and constructive feedback throughout this journey. Her expertise has been instrumental in shaping the trajectory of this dissertation. I am extremely grateful to my family for their unconditional love, encouragement, and unwavering support. Their belief in me has been a constant source of strength and motivation, and I am forever indebted to them for their sacrifices. I am also grateful to my friends, who were always available for a chat when I found myself uncertain about certain aspects of my research. Their willingness to share their thoughts and provide insights served as a constant eye-opener, helping me navigate through challenges and refine my ideas.

DECLARATION

I, LINDSAY LESLIE NYABONYI, 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 or diploma. Other works cited or referred to are accordingly acknowledged.

Signed: LINDSAY LESLIE N 

Date: 15th JUNE 2024

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

Signed:

MS. JANET MACHARIA

ABSTRACT

This research examines the balance between national interests and individual privacy rights in surveillance practices within Kenya's legal framework. The study uses the theory of proportionality to examine when fundamental rights are constrained in pursuit of state objectives. It explores Kenya's Constitution, specifically Article 31, which guarantees the right to privacy while permitting lawful limitations under certain circumstances, such as national interest. The paper exposes the gaps in Kenya's legal framework, particularly under Section 6(1) of the Official Secrets Act, which grants discretionary surveillance powers to the Cabinet Secretary for Internal Security to access data without a court order. Its major claim is that the access to data without a high court order is prone to abuse and infringes on citizens' right to privacy. The paper therefore advocates for the introduction of essential checks and balances to prevent potential abuses and ensure accountability in surveillance initiatives. The benefits and harms of surveillance measures are also examined, emphasizing the need for a principled approach to surveillance that prioritizes individual rights and democratic principles while safeguarding national interests' effectively. The paper further analyzes the existing legal, institutional, and policy frameworks governing data surveillance in Kenya. A comparative study is conducted between the United Kingdom and Kenya. The paper scrutinizes the UK's Investigatory Powers Act, and further advocates for the incorporation of an Investigatory Powers Commissioner's Office (I.P.C.O) and Investigatory Powers Tribunal (I.P.T) to enhance oversight mechanisms. This according to the paper, when adopted in the Kenyan dimension would help prevent abuse of investigatory powers by public authorities. The paper draws critical findings which are directed towards enlightening policy makers, lawyers, adjudicators, and scholars, enriching the ongoing discourse surrounding safeguarding privacy rights amidst increasing state surveillance.

KEY WORDS: Surveillance, Privacy, National Interest, Official Secrets Act.

LIST OF CASES

1. Liberty and Privacy International v. Security Service and Secretary of State for the Home Department [2023], The United Kingdom Investigatory Powers Tribunal.
2. Kenya Human Rights Commission v Communications Authority of Kenya & 4 others (2018) eKLR
3. Klass & Others v Germany (1978) ECtHR.
4. Ahamad Abolfathi Mohammed & another v Republic [2018] eKLR
5. Szabó and Vissy v Hungary (2016) ECtHR.
6. Okiya Omtatah Okoiti vs. Communication Authority of Kenya & 8 Others (2018) eKLR

LIST OF LEGAL INSTRUMENTS

1. Constitution of Kenya (2010).
2. Data Protection Act, Act No. 24 of 2019.
3. Official Secrets Act, Act No. 11 of 1968.
4. National Intelligence Service Act, Act No.28 of 2012.
5. Kenya Information Communication Act, Act No. 2 of 1998.
6. Kenya Information and Communication (Consumer Protection) Regulations, Act No. 54 of 2010.
7. Regulation of Investigatory Powers Act UK (2000).
8. Investigatory Powers Act UK (2016).
9. European Convention on Human Rights (ECHR).
10. International Convention on Civil and Political Rights (ICCPR).
11. Universal Declaration of Human Rights (UDHR)
12. European Union General Data Protection Regulation (1995).

LIST OF ABBREVIATIONS

COK – Constitution of Kenya (2010)

CS - Cabinet Secretary for Internal Security in Kenya, head of Ministry of Interior and National Administration.

NIS - National Intelligence Service

IPT - Investigatory Powers Tribunal

OECD - Organization for Economic Co-operation and Development

EU - European Union

UN - United Nations

UK - United Kingdom

ECHR- European Convention on Human Rights

ECtHR - European Court on Human Rights

CAK - Communication Authority of Kenya

ICT - Information and Communication Technology

OSA - Official Secrets Act

GDPR - General Data Protection Regulation

CHAPTER 1: INTRODUCTION

1.0 Background to The Study

Privacy is a fundamental human right enshrined in various legal instruments both at national and international levels. The right to privacy is expressly guaranteed under Article 31 of the Constitution of Kenya (2010) which provides that every person has the right to privacy, which includes the right not to have their person, home or property searched, their possessions seized, information relating to their family or private affairs unnecessarily required or revealed and the privacy of their communications infringed.[1] The Constitution of Kenya, under Article 2(5) integrates international law into its national legal framework.[2] Kenya, through its ratification of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), affirms the rights of all citizens to privacy. Article 12 of the UDHR and Article 17 of the ICCPR both protect individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence.[3]

Privacy is not merely a standalone right, it serves as a crucial cornerstone for other fundamental rights and freedoms such as equal participation in political and public affairs, and the freedoms of opinion, expression, religion, peaceful assembly, and association[4]. Daniel Solove's notes in his work 'Conceptualizing Privacy' that the six essential components of privacy which are solitude, restricted access to oneself, secrecy, personal information control, personhood, and intimacy

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

[2] Article 2 (5) Constitution of Kenya (2010).

[3] Article 12, Universal Declaration of Human Rights, 10 December 1948, GA Res 217A (III).

Article 17, International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171.

[4] Sheinin M, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 2009,13.

control, individually contribute to maintaining this crucial role.[5] Solitude provides space for contemplation and decision-making, limited access to oneself fosters autonomy, secrecy safeguards personal affairs, control of personal information ensures self-determination, personhood reinforces dignity, and control over intimacy preserves individual autonomy.[6] Strengthening privacy safeguards empowers individuals to make well-informed choices and engage fully in societal activities, fostering a more inclusive and participatory community. [7]

The Data Protection Act, enacted in Kenya in 2019 to regulate the processing of personal data, protect the privacy of individuals, and establish the legal and institutional mechanism to protect personal data,[8] represents a significant step forward in safeguarding citizens' privacy rights in this digital age.

National interest encompasses a broad range of goals and priorities that a country seeks to achieve for its overall well-being, including economic prosperity, cultural values, and political stability.[9] National security specifically focuses on the protection and defense of the nation against threats, ensuring the safety and sovereignty of the state, and is a critical component of the broader national interest.[10] Surveillance is the systematic monitoring of people, activities, places and behaviors'.[11] In Kenya, state agencies often conduct surveillance activities under the banner of national security.[12] The National Intelligence Service (NIS), Directorate of Criminal Investigations (DCI), and Communications Authority of Kenya (CAK) are key players in this arena. These agencies

[5] Solove D, 'Conceptualizing Privacy' Vol. 90(4) California Law Review,2002,1092.

[6]Solove D, Conceptualizing Privacy, 1106.

[7] Solove D, Conceptualizing Privacy, 1107.

[8] Data Protection Act, (Act No 24 of 2019)

[9] Rajan, M. S. "The Idea of National Interest." The Indian Journal of Political Science 14 (3),1953,199.

[10] Rajan, M. S. "The Idea of National Interest,199.

[11] Kenya's Balancing Act: Securing Citizens While Protecting Privacy <https://www.kictanet.or.ke/kenyas-balancing-act-securing-citizens-while-protecting-privacy/> on 27th May 2024.

[12] Kenya's Balancing Act: Securing Citizens While Protecting Privacy <https://www.kictanet.or.ke/kenyas-balancing-act-securing-citizens-while-protecting-privacy/> on 27th May 2024.

engage in various surveillance activities, including monitoring communications, tracking individuals' movements, and intercepting electronic data.[13]

While these measures are intended to prevent threats such as terrorism and crime and ensure public safety, they can lead to significant infringements on individual privacy and civil liberties.[14] Excessive surveillance can create a climate of fear and mistrust, where people feel constantly watched and hesitant to express themselves freely, hindering the freedom of expression.[15] Furthermore, without robust oversight and accountability mechanisms , state agencies may abuse their surveillance powers to target political adversaries or individuals based on personal agendas rather than legitimate security concerns.[16]

Governments must endeavor to strike a balance between national interest and privacy so as to uphold fundamental human rights.[17] While the government may assert the need to infringe individuals' privacy for national security purposes, the infringement must be lawful, reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom[18] Judicial oversight is imperative to ensure accountability and adherence to the rule of law. Courts serve as guardians of civil liberties, scrutinizing the legality and necessity of surveillance measures, and providing a crucial check on state power.[19]

[13] Privacy International 'State of Privacy Kenya' 29 January 2019 https://privacyinternational.org/state-privacy/1005/state-privacy-kenya> on 29 May 2024,

[14] Kinyanjui A, Data Protection as a Human Right; Balancing the Right to Privacy and National Security in Kenya, University of Nairobi,2017, 12.

[15] Murray D and Fussey P, Bulk Surveillance in The Digital Age 'Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data, 43.

[16] Murray D and Fussey P, Bulk Surveillance in The Digital Age 'Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data, 43.

[17] Davis R, 'Striking the Balance: National Security s Civil Liberties', 12.

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

[19] Reinhard S, The Judicial Role in National Security, 86 Boston University Law Review, 2006, 1309.

The International Principles on the Application of Human Rights to Communications Surveillance[20] mandate that before conducting surveillance, a state must convince a competent judicial authority of the likelihood of a serious crime or specific threat. Access to protected information must be justified by its relevance to the crime or threat and only after less invasive methods have been exhausted. Collected data should be limited to relevant information, with any excess promptly destroyed or returned and access should be restricted to designated authorities for the intended purpose and duration, without compromising privacy or fundamental freedoms.[21]

The Constitution of Kenya provides vital safeguards to ensure that infringements on fundamental rights, such as the right to privacy, are transparent, accountable, and subject to review. Article 47 grants individuals the right to receive written reasons for administrative actions that negatively impact their rights and mandates the review of such actions by courts or impartial tribunals.[22] This allows individuals to challenge decisions they believe are unfair or unlawful.

1.2 Problem Statement

Ideally, the government should balance national interests' with the right to privacy in surveillance, however, Kenya's current legal framework, particularly under Section 6(1) of the Official Secrets Act, inadequately protects citizens' rights amid communication interception.[23] Section 6(1) of the Official Secrets Act grants the Cabinet Secretary for Internal Security discretionary powers to access data from any telecommunication apparatus without obtaining a High Court Order when it is deemed in national interest.[24] The use of the term 'may' in the wording of the section implies that obtaining a court order is optional, thereby granting the Cabinet Secretary the leeway to bypass

[20] International Principles on the Application of Human Rights to Communications Surveillance May 2014 - <Necessary and Proportionate> on 1st March 2023

[21] International Principles on the Application of Human Rights to Communications Surveillance May 2014 - <Necessary and Proportionate> on 1st March 2023

[22] Article 47 Constitution of Kenya (2010).

[23] Section 6(1) Official Secrets Act (Act no 20 of 2020)

[24] Section 6(1) Official Secrets Act (Act no 20 of 2020).

the court's approval.[25] The lack of oversight can potentially lead to abuses of power by the Cabinet Secretary thus violating the right to privacy. Infringements to fundamental rights, such as privacy must be lawful, reasonable, and justifiable.[26] Even when conducted for national interest, surveillance initiatives ought to be subject to prior judicial authorization before accessing personal data to ensure adherence to legal standards.

The purpose of this study is to determine whether Section 6(1) of the Official Secrets Act, in granting the Cabinet Secretary discretionary powers to examine any data without mandatorily having to obtain a court order, violates the right to privacy as envisioned under article 31 of the Constitution of Kenya. The research aims to contribute to the on-going discourse on balancing national interests' and the right to privacy in surveillance practices.

1.3 Research Objectives

1. To examine the extent to which surveillance for national interest aligns with the right to privacy.
2. To assess the existing safeguards and oversight mechanisms in place regarding surveillance of data in Kenya.
3. To investigate, by conducting a comparative analysis, the extent to which surveillance and privacy laws in the United Kingdom are sufficient for the enactment of similar laws in Kenya.

1.4 Research Questions

1. What is the extent to which surveillance for national interest aligns with the right to privacy?
2. What safeguards and oversight mechanisms are in place regarding surveillance of data in Kenya?
3. Can conducting a comparative analysis on surveillance and privacy laws in the United

[25] Section 6(1) Official Secrets Act (Act no 20 of 2020).

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

Kingdom influence the enactment of similar laws in Kenya?

1.5 Hypothesis

The Cabinet Secretary's ability to scrutinize data without a court order, as granted in Section 6(1) of the Official Secrets Act, violates an individual's right to privacy as provided for in Article 31(d) of the Constitution of Kenya. This provision grants the cabinet secretary discretionary powers which allows him to bypass authorization from the judiciary, creating a risk of potential abuses of power without adequate safeguards. The official secrets act must include checks and balances to hold the Cabinet Secretary accountable when exercising such powers. This can only be achieved by amending the act to make it mandatory for the Cabinet Secretary to seek a court order before accessing data.

1.6 Justification

This study conducts a comprehensive analysis of Kenya's current surveillance laws, as well as situations where surveillance initiatives for national interests intersect with privacy rights. It proposes an amendment to the Official Secrets Act to make it mandatory for the Cabinet Secretary to seek a court order before accessing personal data. The envisioned amendment to the Official Secrets Act holds the potential to wield significant influence on adjudicators by conferring upon them the authority to scrutinize executive power and prevent infringements on privacy. The main aim is to introduce a system of checks and balances that curtails the risk of abuse of authority by the Cabinet Secretary. Furthermore, the outcomes of this research are anticipated to play a pivotal role in guiding lawmakers during the process of amending the Official Secrets Act to ensure alignment with the constitutional vision of safeguarding individual privacy rights under article 31.[27] By doing so, the research seeks to contribute to the establishment of a legal framework that ensures the protection of citizens' rights and prevents unwarranted infringements on privacy. Lastly, the study is beneficial to the society by educating the public on privacy rights, thus empowering them to advocate for necessary changes in the law.

[27] Article 31, Constitution of Kenya 2010.

1.7 Theoretical Framework

1.7.1 Theory of Proportionality

This study utilizes the theory of proportionality to analyze whether surveillance activities conducted by government agencies in pursuit of state interests are proportional to individuals' right to privacy they potentially infringe upon. Proportionality, central to global legal frameworks, navigates competing interests, especially when fundamental rights are restricted in pursuit of state objectives.[28].

At its core, the theory of proportionality requires that any encroachment on a right, such as privacy, must be commensurate with the benefits obtained.[29] This theory encompasses three sub-principles: suitability, necessity, and proportionality in a narrow sense.[30] Suitability assesses whether a specific action or measure is appropriate for achieving a legitimate aim, ensuring alignment with the intended purpose. The necessity sub-principle evaluates whether there are less intrusive alternatives to achieve the same objective, urging decision-makers to opt for the least restrictive option while still achieving their goals. Proportionality in its narrower sense ensures that the advantages gained from an action do not excessively outweigh the harm caused, aiming to maintain a balance and prevent disproportionate burdens on individuals.[31]

Proportionality is grounded in Article 24(1) of the Constitution of Kenya which outlines the necessity for limitations to fundamental rights to be lawful, reasonable and justifiable, taking into account whether there are less restrictive means available to achieve the purpose sought.[32]

---

[28] Moller, K., Proportionality: Challenging the critics. Oxford University Press and New York University School of Law, 2012,710.

[29] Moller K, 'Proportionality: Challenging the critics' 711.

[30] Alexy R, 'Constitutional Rights and Proportionality' Open Edition Journals, 2014, https://journals.openedition.org/revus/2783 on 3rd March 2023.

[31] Alexy R, 'Constitutional Rights and Proportionality' Open Edition Journals, 2014, https://journals.openedition.org/revus/2783 on 3rd March 2023.

Moller K, 'Proportionality: Challenging the critics' 713.

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

How should the proportionality test apply in practice, when making decisions regarding communication surveillance?

Applying proportionality to communication surveillance necessitates a careful balancing act.[33] The potential benefits of intercepting communications must be weighed against the potential harm to individual privacy and human rights. The sensitivity of information accessed, and the extent of privacy intrusion warrant meticulous consideration, urging careful decision-making with minimal infringement on fundamental rights.[34]

The International Principles on the Application of Human Rights to Communications Surveillance[35] mandate that before conducting surveillance, a state must convince a competent judicial authority of the likelihood of a serious crime or specific threat. Access to protected information must be justified by its relevance to the crime or threat and only after less invasive methods have been exhausted. Collected data should be limited to relevant information, with any excess promptly destroyed or returned. Access should be restricted to designated authorities for the intended purpose and duration, without compromising privacy or fundamental freedoms.[36]

Landmark cases like ***Klass & others v Germany (1978)***[37] demonstrate the global application of proportionality. The case involved the surveillance of journalist Hans Klass by the German Federal Intelligence Service (BND) during the 1960s and 1970s. Klass, known for his critical reporting on the BND, became the subject of surveillance in an attempt to uncover his sources. The European Court of Human Rights ruled that a state's interference with an individual's rights must align proportionately with the legitimate aim pursued. It found that the BND's surveillance exceeded

---

[33] Mavedzenge A, 'Necessity, Proportionality and Accountability in Law Enforcement Use of Personal Data' 8 https://rm.coe.int/council-of-europe-presentation-justice-alfred-mavedzenge-2754-8385-792/1680a1a50d on 3rd March 2023.

[34] International Principles on the Application of Human Rights to Communications Surveillance May 2014 - <Necessary and Proportionate> on 1st March 2023.

[35] International Principles on the Application of Human Rights to Communications Surveillance May 2014 - <Necessary and Proportionate> on 1st March 2023

[36] International Principles on the Application of Human Rights to Communications Surveillance May 2014 - <Necessary and Proportionate> on 1st March 2023

[37] *Klass & others v Germany* ECtHR Judgement on 6 September 1978.

what was necessary for national security, constituting an unjustifiable infringement of Klass's right.[38]

Judicial oversight is crucial for ensuring accountability and upholding fundamental rights during surveillance initiatives. Prior judicial authorization serves as a vital safeguard against potential abuses by providing independent scrutiny of the necessity and proportionality of such measures. The case of ***Szabó and Vissy v. Hungary***[39] exemplifies this significance. Brought before the European Court of Human Rights (ECtHR) by two Hungarian nationals, the case challenged the compatibility of Hungary's 2011 anti-terrorism legislation with the right to privacy.

This legislation granted broad surveillance powers to the Anti-Terrorism Task Force (TEK), allowing secret recording of conversations, opening of letters, and monitoring of electronic communications without individuals' knowledge or consent. The applicants raised concerns about the lack of judicial control and oversight in Hungary's surveillance framework, particularly regarding national security-related measures. They argued that the absence of prior judicial scrutiny left individuals vulnerable to arbitrary interference with their privacy rights, thus violating Article 8 of the European Convention on Human Rights (ECHR). Privacy International intervened in the case, advocating for surveillance measures to be subject to judicial control or require a judicial warrant. The ECtHR ruled in favor of the claimants, finding that the surveillance practices under the Hungarian Law violated Article 8 of the ECHR due to their overbroad nature, lack of necessity assessments, and absence of judicial supervision. Despite the legitimate aim of national security, the court emphasized the need for safeguards to prevent abuse of executive power. [40]This case highlighted the importance of ensuring that surveillance measures are proportional, necessary, and subject to judicial scrutiny.

[38] *Klass & others v Germany* ECtHR Judgement on 6 September 1978.

[39] *Szabó and Vissy v Hungary*, ECtHR Judgement of 12 January 2016.

[40]*Szabó and Vissy v Hungary*, ECtHR Judgement of 12 January 2016.

Existing surveillance legislation often prioritizes state power over robust privacy protections.[41] Arguments suggesting that individuals with 'nothing to hide' should not object to surveillance overlook the fundamental purpose of privacy—not merely as a shield for wrongdoing, but as a cornerstone of individual dignity and autonomy.[42] While some may argue that requiring judicial authorization every time the Cabinet Secretary seeks to intercept data for national security may hinder the government's ability to promptly address imminent dangers, it is crucial to note that in secret surveillance individuals' are not informed neither is their consent sought,[43] therefore they are unaware that their privacy rights are being infringed. This limits their ability to seek redress through judicial review when they feel aggrieved. It is thus essential to subject such surveillance powers to independent scrutiny by the courts to ensure adherence to the law, necessity and proportionality. This prevents arbitrary interference with individuals' right to privacy and abuse of surveillance powers.

Using the theory of proportionality, this study critically evaluates whether the data surveillance carried out by the Cabinet Secretary to safeguard national interests is proportional to the potential infringement on the right to privacy. This analysis aims to ensure a balanced and accountable approach to surveillance in Kenya, protecting individual rights while promoting national interests.

1.8 Literature Review

So far, the literature on privacy and national interest in surveillance practices has mostly focused on introducing the general issues, examining the current limitations on the right to privacy and assessing their constitutionality,[44] assessing the role of social media on national security with reference to Kenya,[45] analyzing the state's justification on the use of digital surveillance and its

---

41 Mavedzenge, A, The right to privacy v national security in Africa: Towards a legislative framework which guarantees proportionality in communications surveillance. African Journal of Legal Studies, 12(3), 13-25,2020.

42 Solove, D. J., Nothing to hide: The false trade-off between privacy and security. Yale University Press,2011.

43 Iphofen R, Ethical issues in surveillance and privacy, 18.

44 See For Example: Kinyanjui A, 'Data Protection as A Human Right: Balancing the Right to Privacy and National Security in Kenya' Published, University of Nairobi, Nairobi, 2017, 14.

45 See For Example: Olasya P, 'Assessing the Impacts of Social Media on National Security in Kenya' Published, University of Nairobi, Nairobi, 2018, 12.

impact on the right to privacy of citizens,[46] and examining the balance between counterterrorism and privacy in the digital age.[47] Although some blogs have touched on my research problem in their discussions, the claims made there are too assumptive and general in nature as they did not extensively analyze the problem in the lens of privacy vis-a-vee national security.[48] I therefore expect that my study will be a unique contribution through examining national security versus privacy concerns in surveillance practices with a particular focus on whether the Cabinet secretary should have the powers to obtain and scrutinize personal data without the mandatory requirement of obtaining a court order.

1.8.1. To examine the extent to which surveillance for national interest aligns with the right to privacy.

Pushya Chabria and Hiya Gandhi, in their article on the grey area between national interest and the right to privacy in India, conclude that this ambiguity stems from unclear statutory frameworks in their jurisdiction,[49]specifically, the National Security Act which does not define 'national security,' creating potential for government abuse and infringement on citizens' privacy rights. [50]They suggest that the legislature should take measures to clearly define laws so as to eliminate the grey area thus ensuring surveillance is confined to specific purposes and scopes, mitigating potential abuses.[51] This scenario mirrors the findings of my dissertation, which similarly reveals

---

[46] See For Example: Badurdeen F, 'Digital Surveillance and Privacy Concerns in The Counter Terrorism Discourse in Kenya: Policy Implications' ,2017, 2.

[47] See For Example: Torrorey LK, 'Trust and Concern: The Balance Between Privacy in A Digital Age and Counter Terrorism in Kenyan Law', Strathmore University, 2016, 6.

[48] See For Example: Andere B, 'Kenya's Sneak Attack On Privacy: Changes To The Law Allow Government Access To Phone And Computer Data,' < Kenya's Sneak Attack On The Right To Privacy - Access Now>, On 23rd December 2023; < Kenya: Official Secrets Act incompatible with freedom of expression standards - ARTICLE 19>, on 23rd December 2023.

[49] Hiya G, Pushya C, National Security vs. Right to Privacy: A Conflict of Interests', International Journal of Law and Management studies, 5(4), 1107-1111.

[50] Hiya G, et al, National Security vs. Right to Privacy: A Conflict of Interests', 1107-1111.

[51] Hiya G, et al, National Security vs. Right to Privacy: A Conflict of Interests', 1107-1111.

that in Kenya, legal frameworks governing surveillance fail to define what 'national interest,' constitutes leading to potential abuses of power.

Christopher Reddick arrives at the conclusion that public perception is an important factor when it comes to government surveillance. He conducts investigations of NSA surveillance programs highlighting the need for the societal acceptance or rejection of such initiatives. His research explored the importance of public sentiment in shaping surveillance policies and calls for the need for government to be more efficacious in communicating about surveillance programs more transparently to garner greater citizens' approval for its surveillance programs.[52]

Kiptoo Torrorey in his thesis on the balance between privacy in a digital age and counter terrorism in Kenyan law, argued that Kenya lacks legislation to appropriately regulate the powers of public bodies to carry out surveillance. His analysis of Article 35 of the Prevention of Terrorism Act 2012 concluded that it grants extensive powers to state authorities to limit fundamental freedoms and encroach on the right to privacy through surveillance.[53] Torrorey's examination of the Prevention of Terrorism Act 2012 and its implications for privacy rights lays groundwork for discussing the balance between privacy rights and national interests' concerns. His conclusion that the Prevention of Terrorism Act grants excessive powers for surveillance without sufficient checks and balances is in line with my paper's proposition that the Official Secrets Act in Section 6(1) has gaps that may potentially lead to infringement of privacy rights of Kenyan citizens.

Melissa De Zwart and Sal Humphreys in their article, investigate the data gathering and surveillance practices by businesses and government, and the implications for individual privacy in the face of widespread collection and use of big data. Their focus is on the United Kingdom and the USA.[54] They have examined the opinion by the EU Data Protection Working Party on Surveillance of Electronic Communications for Intelligence and National Security Purposes. In

---

[52] Roderick C, Akemi T and Jaramillo P, 'Public opinion on National Security Agency surveillance programs: A multi-method approach', Government Information Quarterly, 32(2), 2015, 129-131.

[53] Torrorey LK, 'Trust and Concern: The Balance Between Privacy in A Digital Age and Counter Terrorism in Kenyan Law', Strathmore University, 2016, 6.

[54] Zwart M & Humphrey S, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK,' University of New South Wales Law Journal, 37(2)2, 2014, 713.

that opinion the group concluded that secret, massive and indiscriminate surveillance programs are incompatible with their fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. They further called for effective oversight of intelligence services and enforcing compliance with protections and freedoms under the ECHR.[55] This discourse holds significance as it establishes a crucial context for a fundamental assertion that this research advances. Consequently, it will be pivotal in our examination of the debates surrounding national security versus privacy.

1.8.2. To assess the existing safeguards and oversight mechanisms in place regarding surveillance of data in Kenya.

Cynthia Laberge discusses the potential invasion of privacy in the pursuit of national security in a post 9/11 world,[56] which is a global issue affecting many countries. She provides examples of security measures taken by various countries, including the United States, the United Kingdom, Australia, [57]and New Zealand[58], as well as international institutions such as the United Nations, the OECD, the Council of Europe, and the European Union. [59] She argues that while laws and technologies have their place in keeping us safe, they cannot succeed on their own, thus stressing on the need for robust, independent oversight to ensure that national security measures do not unduly sacrifice privacy.[60] The discussion in her paper lays strong foundation for what my dissertation advances as there needs to be strong safeguards against abuse of powers in furtherance of national interest goals.

[55]Zwart M & Humphrey S, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK',740-741.

[56] Laberge C, 'To What Extent Should National Security Interests Override Privacy in a Post 9/11 World,' 3 Victoria University of Wellington Working Paper Series, 2010, 9.

[57] Laberge C, 'To What Extent Should National Security Interests Override Privacy in a Post 9/11 World,' 46.

[58] Laberge C, 'To What Extent Should National Security Interests Override Privacy in a Post 9/11 World,' 42.

[59] Laberge, C, 'To What Extent Should National Security Interests Override Privacy in a Post 9/11 World,' 22.

[60] Laberge, C, 'To What Extent Should National Security Interests Override Privacy in a Post 9/11 World,'132.

Arun Chinmayi has examined India's surveillance system and calls for the need for appropriate safeguards as this presents new threats to the right to privacy.[61] He evaluates the landscape of privacy rights and surveillance in India, dissecting the jurisprudence surrounding privacy rights and the underlying concerns arising from unchecked mass surveillance.[62] Arun identifies a structural flaw in that India does not even have external oversight in the form of an independent regulatory body to ensure that no abuse of surveillance systems takes place.[63] This bears some resemblance to and simultaneously differs from the present issue that this paper aims to pinpoint, which revolves around privacy concerns related to the unrestrained authority of the Cabinet Secretary in intercepting data for national security interests.

Malik Ayesha and Anwar Oves dissect Pakistan's Legal framework amid the mass surveillance and collection of data that has resulted in heightened concerns regarding the sanctity of data rights and privacy.[64] In their paper they consider the legislation which provides cover for these measures and the potential legal issues raised by their use.[65] They propose the establishment of an authority which can provide oversight and monitor the implementation of Punjab and Khyber Pakhtunkhwa's laws which relate to safeguarding personal data. Further they push for the need that there be laws in place which provide a right to a remedy in case of breaches of data privacy to promote accountability and transparency.[66] Ayesha and Oves' proposals for oversight mechanisms and legal remedies align with the objectives of this research, which aims to evaluate Kenya's surveillance practices and propose reforms to ensure transparency, accountability, and protection of privacy rights.

---

[61] Chinmayi A, 'Paper-Thin Safeguards and Mass Surveillance in India', National Law School of India Review 26(2), 2014, 105.

[62] Chinmayi A, 'Paper-Thin Safeguards and Mass Surveillance in India', 106.

[63] Chinmayi A, 'Paper-Thin Safeguards and Mass Surveillance in India', 113.

[64] Oves A, Ayesha M, 'Cyber Surveillance and Big Data - Pakistan's Legal Framework and the Need for Safeguards', RSIL Law Review 2020, 35.

[65] Oves A et al, 'Cyber Surveillance and Big Data - Pakistan's Legal Framework and the Need for Safeguards', 35.

[66] Oves A et al, 'Cyber Surveillance and Big Data - Pakistan's Legal Framework and the Need for Safeguards', 35.

Overall, the literature review underscores the significance of robust oversight mechanisms and up to date legal frameworks aimed at protecting privacy rights in the face of surveillance initiatives. The insights gained from these scholarly works will inform the analysis and recommendations proposed in this dissertation, contributing to the ongoing discourse on balancing national security imperatives with individual privacy rights.

1.9 Research Methodology

This study's research methodology involves two major parts. The first will entail a doctrinal analysis which will involve an in-depth examination of secondary sources such as journal articles and books as well as primary sources such as cases and statutes to determine measures that can be taken to ensure that government surveillance is conducted in a way that respects citizens' right to privacy while also safeguarding national interests.

The second part of the study will be a comparative analysis of surveillance laws in Kenya and the United Kingdom (UK). The UK has robust surveillance laws such as the Investigatory Powers Act (2016)[67] which have proved effective in adequately protecting individuals' rights amidst surveillance as will be discussed further in chapter four, thus it will be prudent, for Kenya to adopt some of their mechanisms to fit its local context. Secondly, both Kenya and the UK share a common law legal system, which means that legal principles and precedents from the UK often influence legal developments in Kenya. Lastly, since Kenya is a former British colony, majority of the country's social, legal, and economic systems have been borrowed from its colonial masters, therefore it will be easier for Kenya to adopt laws from the UK. This analysis aims to provide insights into strategies that can be implemented in Kenya's surveillance laws to better protect the right to privacy amidst increasing surveillance.

1.10 Limitations of the Study

The study relies on publicly available court cases and legal documents. Some relevant cases or documents may not be publicly accessible due to confidentiality or national security concerns. The

[67] Long Title, Investigatory Powers Act UK, 2016.

interpretation of legal texts and court rulings involves a degree of subjectivity, which may lead to different conclusions. Laws and regulations related to privacy and national security are subject to change, which could render some findings of the study outdated.

1.11 Chapter Breakdown

Chapter 1 serves as an introduction to the paper. It provides the background to the study, problem statement, identifies the research objectives and questions, hypothesis, justification to the study, theoretical framework, literature review, research methodology and outlines the limitations to the study.

Chapter 2 examines the benefits of enhanced surveillance measures against their potential harms, provides an analysis to the 'Nothing to Hide' argument, and proposes a way forward with regards to government surveillance.

Chapter 3 examines current laws and institutions governing surveillance of data in Kenya. The main aim is to assess the effectiveness of these measures and identify potential areas for improvement.

Chapter 4 conducts a comparative analysis on surveillance laws in the United Kingdom and Kenya. The aim is to ascertain the feasibility of Kenya adopting analogous laws that robustly protect citizens' privacy rights. This analysis critically considers the effectiveness of the UK's legal framework, exploring challenges and opportunities for replication in Kenya.

Chapter 5 serves as the culmination of the paper, offering a comprehensive summary of findings, recommendations, and the conclusion. It proposes actionable strategies to address identified challenges and enhance the protection of privacy rights under data surveillance in Kenya, with a focus on implications for Section 6(1) of the Official Secrets Act.

CHAPTER 2: THE EXTENT TO WHICH DATA SURVEILLANCE FOR NATIONAL SECURITY ALIGNS WITH THE RIGHT TO PRIVACY?

INTRODUCTION

This chapter delves into the analysis of data surveillance in the context of national security, examining both the benefits of enhanced government surveillance measures against their potential harms. The 'nothing to hide' argument, which posits that only individuals with something to conceal should fear surveillance, is examined. The paper sides with the critiques to the argument, highlighting the broader implications for privacy and civil liberties. Lastly the chapter provides insights on how best surveillance can be conducted to ensure protection of individuals rights while safeguarding national interests' effectively.

i. Benefits of Enhanced National Security Measures

While government surveillance for national security purposes often faces criticism for potentially violating individuals' privacy rights, when conducted with proper oversight and adherence to established procedures, it can yield significant benefits such as crime prevention, thus enhancing overall security.[68] This approach aligns with the Utilitarian school of thought, which argues that an action is justified if it produces the greatest good for the greatest number of people.[69]

In a counter-terrorism operation named Tripartite Spider coordinated by INTERPOL with the support of AFRIPOL, 14 terror suspects were arrested in Central and Eastern Africa.[70] The operation, conducted from 27th March to 23rd April 2023, aimed at assisting national Counter-Terrorism investigation teams in identifying suspected terrorists and disrupting their financial

---

[68] Mavedzenge A, 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance,' African Journal of Legal Studies, Volume 12(3), 2020, pp 364.

[69] <Jeremy Bentham: 'It is the greatest good to the greatest number of people which is the measure of right and wrong.' — The Socratic Method (socratic-method.com)>, on 13th February 2024.

[70] <https://www.interpol.int/en/News-and-Events/News/2023/14-terror-suspects-arrested-in-African-operation>, on 13th February 2024.

networks.[71] The suspects, linked to terror groups ADF, Al-Shabaab, and ISIS, were apprehended in countries including the Democratic Republic of Congo, Kenya, Somalia, Tanzania, and Uganda. The arrests were made with the collaboration of various intelligence agencies and experts, including INTERPOL's Regional Counter-Terrorism Node in Africa.[72] The outcomes yielded by this operation underscore the efficacy of robust surveillance mechanisms in combating criminal activities, thereby underscoring one of the positive outcomes of heightened surveillance measures.

Another notable success story involves the apprehension of two Iranian citizens Ahamad Abolfathi and Sayed Mansour in Kenya in 2014 by the Anti-Terrorism Police Unit under suspicion of involvement in a terrorist mission.[73] The two who had entered Kenya on tourist visas, were intercepted by the Anti-Terrorism Police Unit before departing the country and were found in possession of explosives leading to charges including unlawful possession of explosives and participation in a terrorist mission. Intelligence gathered through surveillance efforts, including monitoring of suspicious communications and movements, enabled their capture. The prosecution's case against the appellants centered on their visit to a golf course in Mombasa, where they unlawfully concealed Cyclotrimethylene Trinitramine (RDX), an explosive substance, with the intent to cause grievous harm or commit the felony of grievous harm against golfers. [74]

These examples demonstrate how strategic surveillance measures, when conducted within proper legal and ethical frameworks, contribute to the greater good of society by enhancing national security and preventing criminal activities.

ii. Potential Risks of Unchecked Government Surveillance.

As discussed above, government surveillance holds the potential for numerous advantages in the fight against crime, thereby strengthening national security. Nonetheless, its execution often falls

---

[71] <https://www.interpol.int/en/News-and-Events/News/2023/14-terror-suspects-arrested-in-African-operation>, on 13th February 2024.

[72] <https://www.interpol.int/en/News-and-Events/News/2023/14-terror-suspects-arrested-in-African-operation>, on 13th February 2024.

[73] Ahamad Abolfathi Mohammed & another v Republic [2018] eKLR

[74] Ahamad Abolfathi Mohammed & another v Republic [2018] eKLR

short of ideal standards, presenting a host of legal and ethical dilemmas that warrant careful consideration.[75] The 'chilling effect' is a term used to describe a situation where individuals alter their behavior due to the fear of surveillance.[76] This fear can result in self-censorship, where individuals hold back from expressing dissenting opinions or participating in certain activities because they are afraid of being monitored.[77] This hinders the freedom of expression and political participation, leading to a more restricted and less free society.[78] This underscores the need to balance security imperatives with the protection of individual rights and civil liberties.

Gathering personal data from individuals who are not suspected of any wrongdoing is unethical.[79] Traditional surveillance practices often require initiating surveillance based on reasonable suspicion that an individual is engaged in criminal activity. However, in bulk monitoring of communications data, suspicion is not a prerequisite for data collection. Instead, surveillance is initiated based on the analysis of the data itself leading to profiling and the categorization of people based on their communication patterns rather than reasonable suspicion.[80] This raises questions about the role of probable cause, reasonable suspicion, due process, and the presumption of innocence in such surveillance practices.[81] In recognition of these issues, the African Commission in its 2023 *Resolution on the deployment of mass and unlawful targeted communication*

---

[75] Murray D and Fussey P, Bulk Surveillance in The Digital Age 'Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data,'52 Israel Law Review 1, 2019, 32.

[76] Murray D and Fussey P, Bulk Surveillance in The Digital Age 'Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data, 43.

[77] Richards N ' The Dangers of Surveillance' *Havard Law Review* , 2019, <https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/#:~:text=First%2C%20surveillance%20is%20harmful%20because,about%20political%20and%20social%20issues.> on 14th February 2024.

[78] Murray D and Fussey P, Bulk Surveillance in The Digital Age 'Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data, 45.

[79] Iphofen R, Ethical issues in surveillance and privacy, 18.

[80] Murray D and Fussey P, Bulk Surveillance in The Digital Age 'Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data,47.

[81] Murray D and Fussey P, Bulk Surveillance in The Digital Age 'Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data,47.

surveillance and its impact on human rights in Africa, calls on state parties to only engage in targeted communication surveillance that is authorized by law, conforms with international human rights law and standards, and is premised on reasonable suspicion that a serious crime has been or is being carried out. [82]

Secret surveillance programs conducted for national security by state agencies often lack prior judicial authorization, making it challenging to hold these agencies accountable and address potential abuses of power by government entities engaged in surveillance. The case of ***Szabó and Vissy v Hungary,***[83] brought before the European Court of Human Rights (ECtHR) by two Hungarian lawyers, challenged the compatibility of surveillance measures under Hungary's 2011 anti-terrorism legislation with the right to privacy. The legislation granted broad surveillance powers to the Anti-Terrorism Task Force (TEK), allowing secret recording of conversations, opening of letters, and monitoring electronic communications without individuals' knowledge or consent. Privacy International intervened in the case, arguing that surveillance measures should be subject to judicial control or require a judicial warrant. The ECtHR ruled in favor of the claimants, finding that the surveillance practices under the Hungarian Law violated Article 8 of the European Convention on Human Rights, which provides for the right to privacy, due to their overbroad nature, lack of necessity assessments, and absence of judicial supervision. Despite the legitimate aim of national security, the court emphasized the need for minimum safeguards to prevent abuse of executive power.[84] This case highlighted the importance of ensuring that surveillance measures are proportional, necessary and subject to appropriate safeguards and oversight mechanisms to protect individual privacy rights.

In the case of ***Okiya Omtatah Okoiti vs. Communication Authority of Kenya & 8 Others***[85]**,** the High Court of Kenya assessed the constitutionality of the Device Management System (DMS),

---

[82]Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa - ACHPR/Res.573 (LXXVII) 2023 https://achpr.au.int/en/adopted-resolutions/573-resolution-deployment-mass-and-unlawful-targeted-communication> on 29th May 2024

[83] *Szabó and Vissy v Hungary*, ECtHR Judgement of 12 January 2016.

[84] *Szabó and Vissy v Hungary*, ECtHR Judgement of 12 January 2016.

[85] *Okiya Omtatah Okoiti vs. Communication Authority of Kenya & 8 Others* (2018)) eKLR.

which was a communication surveillance tool implemented by the Kenyan Government through the Communication Authority of Kenya (CAK). The DMS used mobile phone networks operated by Mobile Network Operators (MNOs) to identify counterfeit, stolen and unapproved mobile devices. Concerns were raised about potential privacy invasions due to the DMS's access to subscribers' personal information without sufficient safeguards. This was through features like the home location register. The petitioner argued that the DMS enabled unwarranted surveillance and infringed upon privacy rights. Relying on constitutional provisions particularly Article 24 and 31, the Court found the DMS to be inconsistent with the law, lacking proper safeguards, and failing to meet the criteria for justifiable privacy limitations in a democratic society. Consequently, the Court deemed the DMS unconstitutional, stressing the importance of safeguarding individuals' autonomy and dignity, particularly in this digital era.[86]

In conclusion, while government surveillance enhances national security and aids in crime prevention, it also presents numerous ethical and legal challenges that cannot be overlooked. The chilling effect, where fear of being monitored leads to self-censorship and restricted freedom of expression emphasizes the delicate balance that needs to be achieved between national security imperatives and civil liberties. The practice of gathering personal data without reasonable suspicion undermines fundamental legal principles such as probable cause and due process, shifting surveillance from targeted investigations to indiscriminate profiling. Therefore, it is necessary to establish robust safeguards and oversight mechanisms that ensure surveillance measures are both effective in achieving security objectives and respectful of individual rights and freedoms.

iii. Nothing to Hide Argument in Government Surveillance

This paper dissects the Nothing to hide argument with an aim to show its flawed nature. The notion that 'if you have nothing to hide, you have nothing to fear' concerning surveillance is not a recent concept; it has been present since the 19th century, predating the internet age.[87] This argument is founded upon the aspect that if the government conducts surveillance, privacy is only at risk if the

---

[86] *Okiya Omtatah Okoiti vs. Communication Authority of Kenya & 8 Others* (2018) eKLR

[87] < Why the "nothing to hide" argument is privacy's biggest battle (ipvanish.com)>, on 2nd January 2024.

government discovers illicit conduct, therefore, if an individual engages only in legal activity, they have nothing to worry about[88]

The basic rationale of the nothing-to-hide view is that objecting to surveillance is admitting some sort of guilt.[89] This perspective assumes that government surveillance will consistently adhere to its intended purpose and procedures. However, this paper challenges this notion, highlighting the difficulty in achieving perfect alignment between surveillance practices and goals, thus leading to potential misuse of surveillance tools beyond intended national security objectives.

Richard Posner contends that the desire for privacy stems from individuals' seeking power to conceal information that could be used against them.[90] However, critics argue that Posner oversimplifies privacy, associating it primarily with concealing wrongdoing or negative aspects of one's life.[91] This paper sides with the critics, diverging from Posner's argument. Posner's stance places the burden on individuals to prove their innocence by accepting government surveillance thus essentially reversing the presumption of innocence until proven guilty. Everyone has the right to privacy and thus should not in any instance be compelled to give self-incriminating evidence.

Charles Fried, on the other hand, posits that privacy is a basic right for every individual simply because they are individuals.[92] His viewpoint echoes Immanuel Kant's philosophy which emphasizes that individuals should be regarded as ends in themselves, preventing the subjugation of their essential interests to the pursuit of collective happiness or welfare.[93] This perspective underscores the primacy of individual privacy rights, challenging the notion of prioritizing national security over privacy for the greater public well-being.

---

88 Solove J, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, *Washington University Law School*, 2007, 747.

89 Ignacio N, 'Nothing to Hide, But Something to Lose', The University of Toronto Law Journal, 2020, 70(1), 67.

90 Ignacio N, 'Nothing to Hide, But Something to Lose', 70.

91 Solove J, Nothing to Hide, 'The False Trade-off Between Privacy and Security', 26.

92 Solove J, Nothing to Hide, 'The False trade-off Between Privacy and Security', Yale University Press, 2011, 48.

93 Solove J, Nothing to Hide, 'The False trade-off Between Privacy and Security', 48.

iv. Way Forward with Regards to Government Surveillance

In the modern era of rapid technological advancement, the protection of privacy amidst national security concerns presents a significant challenge.[94] Stephen Reinhardt in his work 'The judicial role in national security' notes that courts play a crucial role in this dynamic landscape, serving as guardians of legal boundaries and checks on executive power. Through judicial oversight, surveillance activities are meticulously scrutinized to ensure adherence to legal procedures, warrant requirements, and constitutional principles.[95] Judicial oversight serves to assess the necessity and proportionality of surveillance, preventing overreach by law enforcement agencies and safeguarding citizens' rights. By utilizing their adjudicatory powers, courts provide avenues for citizens to challenge the lawfulness of surveillance activities, thereby upholding privacy rights and promoting accountability.[96] This oversight mechanism contributes to a nuanced balance between national security imperatives and individual liberties, ensuring that surveillance activities are conducted within legal boundaries and respect fundamental rights.

Establishing clear legal frameworks is an important step towards achieving a balance between national security surveillance and individual privacy. Such frameworks can provide guidance on the scope, purpose, and limitations of surveillance activities, as well as the procedural and substantive standards that must be met to ensure that surveillance programs comply with privacy requirements. This fosters trust and confidence among citizens. [97]

Adherence to data minimization principles is crucial. These principles as provided in Article 5(1) of the EU General Data Protection Regulation (GDPR), provide that governments should only collect the minimum amount of information necessary for the specified surveillance purpose,

---

[94] Reinhard S, The Judicial Role in National Security, 86 Boston University Law Review, 2006, 1309.

[95] Reinhard S, The Judicial Role in National Security, 86 Boston University Law Review, 2006, 1309.

[96] A Justice Report the State We're in: Addressing Threats & Challenges to the Rule of Law September 2023 https://files.justice.org.uk/wp-content/uploads/2023/08/31123029/JUSTICE-The-State-Were-In-Addressing-Threats-Challenges-to-the-Rule-of-Law-September-2023.pdf on 24th January 2024.

[97] Resta G and Bignami F, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance (2018), 10.

avoiding the indiscriminate gathering of extensive and unnecessary data.[98] Additionally, strict protocols for data retention should be adhered to, preventing the prolonged and unwarranted storage of sensitive information.[99] These not only align with the principle of proportionality but also serve as fundamental safeguards against the misuse of collected data.[100]

Lastly, sensitization of citizens is imperative. Governments should develop strategies for regularly conducting public awareness campaigns to educate citizens on their rights and the implications of unchecked government surveillance.[101] This empowers individuals to understand the recourse mechanisms available if their constitutional rights are infringed by surveillance.[102]

CONCLUSION

This chapter has analyzed data surveillance in the context of national security, examining both the benefits of enhanced government surveillance measures such as crime prevention against their potential harms. The nothing to hide argument is examined with the paper siding with the critiques to the argument emphasizing the need to respect individual rights irrespective of surveillance objectives. The chapter highlights the importance of establishing clear legal frameworks, enhancing judicial oversight, adherence to data minimization principles and increasing public awareness on their rights. Only through such measures can we achieve a balanced and accountable approach to surveillance in Kenya, protecting individual rights while promoting national interests.

[98] Article 5 (1) European Union General Data Protection Regulation (1995).

[99] Mitsilegas V, Elspeth Guld E, Kuskonmaz & Vavoula N 'Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks, 29 (1-2) European Law Journal, 2023 86.

[100] Mitsilegas V, Elspeth Guld E, Kuskonmaz & Vavoula N 'Data retention and the future of large-scale surveillance,86.

[101] Carothers T & Brechenmacher S, Accountability, Transparency, Participation, And Inclusion:'' A New Development Consensus?' October 20, 2014 https://carnegieendowment.org/2014/10/20/accountability-transparency-participation-and-inclusion-new-development-consensus-pub-56968 on 25t January 2024

[102] Increasing Resilience in Surveillance Societies, Final Report Summary - IRISS (Increasing Resilience in Surveillance Societies) https://cordis.europa.eu/project/id/290492/reporting/fr on 25th January 2024.

CHAPTER 3: EXISTING SAFEGUARDS AND OVERSIGHT MECHANISMS IN PLACE REGARDING DATA SURVEILLANCE IN KENYA

INTRODUCTION

This chapter critically examines the current frameworks governing data surveillance in Kenya. It starts by analyzing the constitution of Kenya 2010 which enshrines the right to privacy. Key legislations like the National Intelligence Service (NIS) Act, the Official Secrets Act, the Data Protection Act, the Kenya Information and Communication Act (KICA) and the Kenya Information and Communication (Consumer Protection) Regulations are scrutinized, as well as international treaties such as the International Convention on Civil and Political Rights (ICCPR). The institutional framework, encompassing bodies such as the Office of the Data Protection Commissioner (ODPC) and Communication Authority of Kenya (CAK), is discussed. The chapter's extensive assessment aims to highlight the various strategies taken in navigating data surveillance in Kenya.

LEGISLATIVE FRAMEWORK

I. Constitution of Kenya 2010-Right to Privacy

In 2010, Kenya embraced a transformative Constitution inspired by the South African model but uniquely tailored to address the specific circumstances of the country.[103] This Constitution goes beyond the conventional objective of ensuring constitutionalism in a traditional sense.[104]

In the case ***Speaker of the Senate & Another v Attorney-General & Another & 3 Others***[105], the Supreme Court of Kenya acknowledged the transformative nature of the constitution. It emphasized that unlike the traditional 'liberal' constitutions from previous decades, which primarily focused on controlling and legitimizing public power, the present constitution is

[103] Kibet E, 'Transformative constitutionalism and the adjudication of constitutional rights in Africa', African Human Rights Law Journal,2017, 352.

[104] Kibet E, 'Transformative constitutionalism and the adjudication of constitutional rights in Africa', African Human Rights Law Journal,2017, 352.

[105] Speaker of the Senate & Another v Attorney-General & Another & 3 Others [2013] eKLR.

explicitly oriented towards fostering social change and reform. This transformation is driven by principles such as social justice, equality, devolution, human rights, and the rule of law.[106]

The constitution has a robust bill of rights which under article 31 provides for the Right to Privacy. It just reiterates the aspect that an individual has the right not to have the privacy of their communications infringed upon.[107]The constitutional guarantee of the Right to Privacy acts as a legal restraint on government surveillance practices. It establishes a clear boundary, requiring any intrusion into private communications to be justified within the parameters stipulated by the law. This legal constraint ensures that surveillance is conducted in accordance with defined procedures, preventing arbitrary actions.

Hans Kelsen in his conception of the *grundnorm* envisions it as a norm presupposed in juristic thinking and is at the top of the pyramid of the norms of each legal order. The *grundnorm* of a legal system is the postulated ultimate rule. He argues that it can only be changed through a revolution.[108] Drawing from this one can deduce that the 2010 constitution is a *grundnorm* because it's the ultimate law in the hierarchy of laws. It came into place as a result of the 2007 post-election violence that necessitated the need for a new constitution and through a referendum held on 4th August, 2010.[109] That being the case therefore, the right to privacy accorded to an individual as per article 31 is superior to all other protections which are afforded to an individual under the law and cannot be limited except as otherwise provided under article 24 which requires limitation to be reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.[110] Therefore, it is essential for a surveillance agency to follow the proper procedures before engaging in the monitoring of public communications.

---

[106] Speaker of the Senate & Another v Attorney-General & Another & 3 Others [2013] eKLR.

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

[108] Hopton T, 'Grundnorm and Constitution: The Legitimacy of Politics, 1978, 81-83.

[109]Ombaka D, 'Christians and the 2010 constitution referendum in Kenya: A search for explanations from a retrospective study', *International Journal of Arts and Commerce*, 146.

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

II. National Intelligence Service (NIS) Act (2012)

This is an act of parliament to provide for the functions, organization, and administration of the National Intelligence Service pursuant to Article 239(6) of the Constitution; to give effect to Article 242(2) and other relevant provisions of the Constitution; to provide for the establishment of oversight bodies and for connected purposes.[111]

Section 36 of the Act provides for the limitation to the right to privacy in that, it may be limited in respect of a person who is subject to investigation by the Service or suspected to have committed an offence. The privacy of the said person's communications may be investigated, monitored, or otherwise interfered with.[112] The Service is however required, prior to taking any action under this section, obtain authorization from the Director General which shall be specific and accompanied by a warrant from the High Court, and shall be valid for a period of one hundred and eighty days unless otherwise extended.[113] The use of the term 'shall' explicitly signifies that obtaining a warrant from the High court is an obligatory prerequisite. Nevertheless, notwithstanding this stipulation, there are allegations suggesting that the National Intelligence Service (NIS) functions as a rogue agency without adequate oversight, consequently infringing upon several rights and freedoms protected by the constitution.[114]

III. Official Secrets Act (1968)

This is an Act of Parliament to provide for the preservation of State secrets and State security.[115] This legislation was enacted prior to independence and has undergone multiple amendments in its provisions to align with evolving societal dynamics. The recent amendment introduced through

[111] Long Title, *National Intelligence Service Act*, Act No.28 of 2012.

[112] Section 36, *National Intelligence Service Act*, Act No.28 of 2012.

[113] Section 42, *National Intelligence Service Act*, Act No.28 of 2012.

[114] Privacy International (PI), 'The Right to Privacy in Kenya', Joint Stakeholder Report, 2019, 5.

[115] Long Title, *Official Secrets Act*, Act No. 11 of 1968.

the Statute of Miscellaneous Amendment Act 2020 modifies Section 6(1) particularly relevant to surveillance.[116]

Section 2 of the Act defines 'telecommunication apparatus' as apparatus constructed or adapted for use in transmitting or conveying anything transmissible by a telecommunication system.[117] This definition encompasses modern electronic devices such as phones or computers and various forms of data transmitted through them, including internet activity, messages, location data, stored documents, and transactions.[118]

This paper places emphasis upon Section 6(1) of the act which enables the surveillance of individuals by the Cabinet Secretary for Internal Security, when deemed in national interest. It obliges owners or controllers of telecommunications apparatus used for sending or receiving data to or from outside Kenya to provide the original or transcripts of all such data and related documents to the Cabinet Secretary.[119] The requirement of a judicial warrant is bypassed, as the term 'may' implies that it is discretionary for the Cabinet Secretary to seek a high court order before requesting data.[120] Therefore, the Cabinet Secretary is legally authorized to request and obtain personal data without a court order, leading to potential abuses of power and violations of privacy rights. Limitation to fundamental rights must be lawful, reasonable and justifiable.[121] The paper has identified this as a gap which needs to be redressed immediately to avoid posing threat to the fundamental rights envisioned in the 2010 Constitution. The discretionary powers given to the cabinet secretary may lead to state whereby intelligence agencies operate above the law. In more advanced democracies like the United Kingdom, intelligence agencies subscribe to a stringent

---

116 Statute of Miscellaneous Amendment Act 2020.

117 Section 2, *Official Secrets Act*, Act No. 11 of 1968.

118 Article 19, 'Legal Analysis Kenya: Official Secrets Act 1970, Revised 2012) And Amendment (2020)' <https://www.article19.org/wp-content/uploads/2020/09/KenyaOfficialSecretsAct-analysis-August-2020-Protect-format.pdf> on 23rd December 2023.

119 Section 6(1), *Official Secrets Act*, Act No. 11 of 1968.

120 Section 6(1), *Official Secrets Act*, Act No. 11 of 1968.

121 Article 24, Constitution of Kenya (2010).

legal framework that ensures accountability in relation to their operations such that warrants at any point will require ultimate authorization of a judicial commissioner.[122] This will become more elaborate in chapter 4 of the paper.

In addition the act provides a broad definition of what amounts to data, this being information recorded in a format in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium.[123] This is problematic as it opens up intrusion of a citizen's personal data which is sensitive and ought to be protected by the law. It is thus equivalent to equipping the cabinet secretary with the powers to break and enter a person's house without a court order in the pretext of public interest.[124]

This paper calls for the amendment of section 6(1) of the Official Secrets Act to make it mandatory for the Cabinet Secretary to obtain a court order before accessing personal data. The amendment will help prevent potential abuses of powers by the Cabinet Secretary and ensure privacy rights protection.

IV. Data Protection Act (2019)

This is an Act of Parliament which was established in the year 2019 to give effect to Article 31(c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner, to make provision for the regulation of the processing of personal data , and to provide for the rights of data subjects and obligations of data controllers and processors.[125] Despite being enacted by the legislature nearly a decade subsequent to the promulgation of the 2010 Constitution, we acknowledge and commend the safeguards which have been put in place aimed at protecting the fundamental right to privacy of individuals.

---

[122] Investigatory Powers Act.

[123] Section 2, Official Secrets Act, Act No.11 of 1968.

[124] Article 19, 'Legal Analysis Kenya: Official Secrets Act 1970, Revised 2012) And Amendment (2020)' <https://www.article19.org/wp-content/uploads/2020/09/KenyaOfficialSecretsAct-analysis-August-2020-Protect-format.pdf> on 23rd December 2023.

[125] Long Title, *Data Protection Act*, Act No. 24 of 2019.

The paper draws particular attention to Section 2, which defines data as information which is, processed by means of equipment operating automatically in response to instructions given for that purpose, recorded with intention that it should be processed by means of such equipment, is recorded as part of a relevant filing system, forms part of an accessible record, and is recorded information which is held by a public entity.[126]

Further to this it defines a data controller as a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.[127] Government agencies and Authorities that gather data for surveillance purposes are thereby governed by the Act.[128]

Section 25 of the act outlines essential principles for data processors and controllers when handling personal data.[129] It emphasizes the need for data processing to be conducted in accordance with the right to privacy, within the law, transparently and confined to legitimate purposes. Moreover, collected information should be limited to what is strictly required and not stored for longer than necessary.[130] These principles are vital for safeguarding individuals' privacy and ensuring responsible data management in this digital age. The above initiatives undertaken by the Data Protection Act to protect the right to privacy are commendable as it shows the commitment undertaken by parliament towards ensuring protection of personal data of Kenyans.

V. Office of Data Protection Commissioner

This office is established by virtue of Section 5 of the Data Protection Act.[131] Of the functions stipulated under Section 8, their mandated with the role of exercising oversight on data processing operations, either of own motion or at the request of a data subject and verify whether the

[126] Section 2, *Data Protection Act,* Act No. 24 of 2019.

[127] Section 2, *Data Protection Act,* Act No. 24 of 2019.

[128] Section 2, *Data Protection Act,* Act No. 24 of 2019.

[129] Section 25, *Data Protection Act,* Act No. 24 of 2019

[130] Section 25, *Data Protection Act,* Act No. 24 of 2019

[131] Section 5, *Data Protection Act,* Act No. 24 of 2019.

processing of data is vital.[132] This is important as they are entrusted to ensure that data is safeguarded, and privacy rights of individuals are not violated.

Section 9 allows for the Data Commissioner to enter association with other bodies or organizations within and outside Kenya as appropriate in furtherance of the object of the Data Protection Act.[133] He is tasked with ensuring uniformity in laws and regulation in the data privacy sphere at both national and international levels. Despite there being clear stipulations under the Data Protection Act on what the Commissioner is set to perform, there is no provision which provides for his role in supervising the exercise of investigatory powers by public authorities. This is a gap that needs to be addressed and given that his office is well equipped to deal with such supervisory functions, this paper proposes for the expansion of the Data Protection Commissioners' role to include oversight of investigatory agencies' use of their powers, to ensure compliance with the law.

VI. Kenya Information and Communication Act (K.I.C.A.)

This is an Act of Parliament to provide for the establishment of the Communications Commission of Kenya, also known as the Communications Authority of Kenya, and to facilitate the development of the information and communications sector. It encompasses various areas such as broadcasting, multimedia, telecommunications, postal services, and electronic commerce.[134] Under Section 2 of the Act it defines 'intercept' as listening to, or recording a function of a computer, or acquiring the substance, its meaning or purport of such function.[135]

Section 31 of the law outlines specific actions that, when taken by a licensed telecommunication operator outside the normal course of their business, constitute offenses and are liable on conviction to a fine as provided for in the act, imprisonment or both.[136] This includes the interception of a message transmitted through a licensed telecommunication system and the

[132] Section8, *Data Protection Act,* Act No. 24 of 2019.

[133] Section 9, *Data Protection Act,* Act No. 24 of 2019.

[134] Long Title, *Kenya Information Communication Act*, Act No. 2 of 1998.

[135] Section 2, *Kenya Information Communication Act*, Act No. 2 of 1998.

[136] Section 31, *Kenya Information Communication Act*, Act No. 2 of 1998.

disclosure of its contents.[137] This section is important as it provides safeguards against potential abuses of interception powers by outlining clear limitations. Telecommunication operators playing a critical role in providing access to intelligence agencies on their customers communication, this paper saw the need to examine KICA as it is crucial, being that it guides intelligence agencies and other persons intercepting communication.

VII. Kenya Information and Communications (Consumer Protection) Regulations (2010)

Section 15(1) in relation to Confidentiality provides that a licensee shall not monitor, disclose, or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data.[138] This, by itself, underscores the principle that telecommunication operators should not permit the interception of their customers' communications even by third parties such as government agencies without their awareness.

VIII. Communication Authority of Kenya

This authority is established under Section 3 of the Kenya Information and Communication Act.[139] It is mandated to license and regulate postal, information and communication services in accordance with the provisions of the Act. Section 5 stipulates that the Authority shall be independent and free of control by government, political or commercial interests in the exercise of its powers and in the performance of its functions.[140] This however may prove to be problematic due the fact that it could be susceptible to political influence as the President is the appointing authority of the Chairperson of the Authority. This may undermine the Authority's ability to act impartially and in the public interest.

[137] Section 31, *Kenya Information Communication Act*, Act No. 2 of 1998.

[138]Section 15(1), Kenya *Information and Communications (Consumer Protection) Regulations*, Legal Notice No.54 of 2010.

[139] Section 3, *Kenya Information Communication Act*, Act No. 2 of 1998.

[140] Section 5, *Kenya Information Communication Act*, Act No. 2 of 1998.

IX. International Legal Framework

To understand how international laws apply in domestic cases, we must first understand the concept of Monism. In a monist state, once the government ratifies an international law, it seamlessly integrates into the domestic legal framework and can be directly invoked and applied by state courts.[141] Citizens can rely on it as part of their legal rights without the need for further domestication by the courts.[142] Kenya is a monist state as per Article 2(6) of the Constitution, which provides that any treaty or convention ratified by Kenya shall form part of its law.[143] Article 17 of the International Convention on Civil and Political Rights (ICCPR), to which Kenya is a party to, provides that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.[144] Therefore, intelligence agencies in Kenya are obligated to adhere to Article 17 in their operations. Failure to which would constitute a violation of the Convention.

CONCLUSION

In this chapter the paper has examined the major statutes and regulations that relate to data surveillance in Kenya. These are the 2010 Constitution, the N.I.S Act, the Official Secrets Act, the Data Protection Act, the Kenya Information and Communications Act and the Kenya Information and Communications (Consumer Protection) Regulations. In the examination it identified current gaps in Kenya's legislations that are prone to abuse and called for the need to address these gaps for a better legislative framework. International laws, particularly the ICCPR, are highlighted as crucial benchmarks, emphasizing Kenya's monist approach in incorporating international principles into domestic law.

---

[141] Zartner D, 'Internalization of International Law', International Studies Department, University of San Francisco, 2020, 10.

[142] Zartner D, 'Internalization of International Law', 10

[143] Article 2(6), *Constitution of Kenya* (2010).

[144] Article 17 of the International Convention on Civil and Political Rights (ICCPR).

CHAPTER 4: COMPARATIVE ANALYSIS BETWEEN THE UNITED KINGDOM AND KENYA

INTRODUCTION

The paper in this chapter will conduct a comparative analysis between Kenya and the United Kingdom in relation to surveillance systems. The justification for choosing the United Kingdom is because its approach to surveillance powers has proven effective in adequately protecting individuals' rights as will be discussed in the chapter, and thus it would be prudent for Kenya to adapt some of their mechanisms to fit its local context. This chapter will also examine both legal and institutional frameworks present in the United Kingdom in relation to surveillance. The paper further aims to assess the Investigatory Powers Act which provides for the office of the Investigatory Powers Commissioner whose task is to oversee the use of investigatory powers by security agencies. Lastly, it will examine the Investigatory Powers Tribunal which proves to be an effective recourse mechanism for persons aggrieved by misuse of investigatory powers. The analysis aims to offer insights into potential amendments to Kenya's data surveillance laws to better protect the right to privacy.

LEGAL FRAMEWORK

The paper has identified the UK's Investigatory Powers Act[145] as a crucial framework governing surveillance, noted for its effective implementation and unique approach to regulating investigatory agencies. The following section will provide a thorough analysis of the Act, emphasizing its role in ensuring the accountability of these agencies.

i. Investigatory Powers Act

The Investigatory Powers Act (I.P.A) is an act of parliament that regulates the conducting of interception activities, equipment interference and data acquisition by the UK intelligence agencies.[146]

---

[145] Investigatory Powers Act UK, 2016.

[146] Long Title, Investigatory Powers Act UK, 2016.

Some of the proponents of this act argue that the IPA makes the system arguably more transparent and reduces the risk of gaps between regimes, thus potentially improving oversight. To underscore the IPA's commitment to curbing misuse of investigatory powers, it emphasizes the consideration of whether objectives could be reasonably accomplished through less invasive methods.[147] Under article 2, the act mandates the public authority when deciding whether or not to give a warrant, to determine whether the objective which the warrant ought to serve can be achieved in a less intrusive manner.[148] This provision aligns with Article 24 of the Constitution of Kenya which mandates that fundamental rights such as privacy should only be limited when there are no other less intrusive means that can achieve the purpose.[149] By imposing a requirement to consider less intrusive alternatives, the provision helps prevent the abuse of surveillance powers, emphasizing on the need for law enforcement to consider interception as the last option in relation to combating crime.

One of the significant innovations in the Act is the introduction of the 'double lock' system for the issuing of warrants. When a warrant is issued, it is signed by the Secretary of State and then subject to review by a 'judicial commissioner'. General oversight of the operation of the regime falls to the Investigatory Powers Commissioner.[150] This is a very nuanced approach that is particularly keen on ensuring judicial oversight which should be a case that the Kenyan counterparts can learn from. Such a system when incorporated into the Kenyan dimension can prove to be effective in preventing abuse of investigatory powers granted to members of the executive more so the cabinet secretary in this context.

From the above analysis of the Investigatory Powers Act one can deduce that it possesses numerous safeguards meant to ensure that surveillance activities are conducted lawfully, proportionately, and with respect for privacy rights. Contrasting this to the Kenyan dimension we lack an express legislation that is designed to monitor activities of investigatory authorities keeping

---

147 Article 2 (2), Investigatory Powers Act UK, 2016.

148 Article 2(2), Investigatory Powers Act UK, 2016.

149 Article 24 (1) (e), Constitution of Kenya (2010).

150 <Safeguards governing investigatory powers come into effect - GOV.UK (www.gov.uk)>, on 9th January 2024.

them in check. The enduring necessity of judicial oversight in warrant issuance is self-evident, underscoring Kenya's need to embrace such checks and balances to enhance privacy rights protection.

INSTITUTIONAL FRAMEWORK

i. Investigatory Powers Commissioner

The Investigatory Powers Act establishes a system of independent oversight to scrutinize the use of surveillance powers. This includes the creation of the Investigatory Powers Commissioner's Office (I.P.C.O), which oversees the use of these powers and ensures compliance with the law. Article 227 grants power to the Prime Minister to Appoint the Investigatory Powers Commissioner. This is subject to recommendation by the Lord Chancellor, the Lord Chief Justice of England and Wales, the Lord President of the Court of Session, and the Lord Chief Justice of Northern Ireland.[151] He is mandated under article 229 to keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to the interception of communications, the acquisition or retention of communications data and the acquisition of secondary data.[152]

Currently in the Kenyan framework there is no office mandated to independently exercise oversight of surveillance powers. This paper therefore advocates for the establishment of an Investigatory Powers Commissioner in Kenya to supervise the use of investigatory powers, thereby preventing potential abuses. Given the risks outlined in the preceding chapter arising from the discretionary powers granted to the Cabinet Secretary under Section 6(1) of Official Secrets Act, if these powers are exercised in a way that contravenes laws such as the right to privacy, the Cabinet Secretary will be held accountable by the Investigatory Powers Commissioner, ensuring that he gives justification for his actions. Establishing this oversight office is the first step in ensuring accountability of Investigatory Agencies.

---

[151] Article 227, Investigatory Powers Act UK, 2016.

[152] Article 229, Investigatory Powers Act UK, 2016.

An alternative would be the expansion of the powers granted to the Data Protection Commissioner(DPC) under the Data Protection Act to include oversight of use of investigatory powers.[153] The office of the DPC is well equipped to undertake such a role since it already oversees the processing of data by public and private entities as guided by data protection principles under section 25.[154] There is dire need for there to be an office entrusted with supervision of investigatory powers by intelligence agencies in Kenya due to the threat of abuse of this powers in the name of 'national interest'. An accountability mechanism that can keep these powers in check is the way forward if we are to protect citizens' right to privacy as enshrined in article 31.

ii. Investigatory Powers Tribunal

The Investigatory Powers Tribunal is an independent court, established under Section 65 of the Regulation of Investigatory Powers Act 2000 (RIPA).[155] This is an act dedicated towards making provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed and to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters.[156]

The Tribunal considers complaints under RIPA and claims under the Human Rights Act 1998 (HRA). It considers allegations of unlawful intrusion by public bodies, including the UK intelligence services, the Police and local authorities and investigates alleged conduct by or on behalf of the UK intelligence services whether it involves investigatory powers or not.[157] This is a positive step as it provides an accountability mechanism through which persons can seek redress in the case that the privacy of their communications' are interfered with without lawful reasons.

---

153 Section 5 Data Protection Act, Act No. 24 of 2019.

154 Section 8 Data Protection Act, Act No. 24 of 2019. See also, Section 25 Data Protection Act, Act No. 24 of 2019.

155 Section 65, Regulation of Investigatory Powers Act UK, 2000.

156 Long Title, Regulation of Investigatory Powers Act UK, 2000.

157 Section 65(5), Regulation of Investigatory Powers Act UK, 2000.

The Tribunal ensures the United Kingdom meets its obligations under Article 13 of the European Convention on Human Rights (ECHR) which provides for citizen's right to effective remedy before a national authority for violations of their rights and freedoms under the ECHR through administrative actions.[158]

Further to this the tribunal has been given powers under section 67 that allows them to give orders relating to quashing or cancelling any warrant or authorization, a notice under Part 3 of the Investigatory Powers Act 2016 or a retention notice.[159] This is a positive step as one can move to the tribunal if at all he or she gets wind of their privacy being infringed by any government body without proper authorization and pray for an order quashing the warrant. Appeals on the decisions of the tribunals are disallowed except on a point of law.[160]

In Kenya currently, there is no quasi-judicial/ judicial body mandated to hearing cases relating to abuse of investigatory powers. This paper therefore posits that establishing an Investigatory Powers Tribunal in Kenya would be instrumental in addressing challenges within the criminal justice system, such as case backlog, which often leads to slow and prolonged litigation processes.[161] The tribunal will provide an avenue which is quasi-judicial and expeditious in nature, through which the aggrieved parties can launch their claims against public authorities who exercise intrusive investigatory powers. Tribunals are known to work within strict timelines and have lesser evidentiary rules as opposed to courts and thus purpose to serve the ends of Justice.[162] Article 169 of the 2010 constitution grants powers to the parliament to establish tribunals as part of the subordinate courts.[163] This has led to the establishment of tribunals by parliament such as Business

158 <About the Tribunal - The Investigatory Powers Tribunal>, on 7th January 2024.

159 Section 67, Regulation of Investigatory Powers Act UK, 2000.

160 Section 67, Regulation of Investigatory Powers Act UK, 2000.

161 Kipyator I, 'How to help courts to beat challenges' Daily Nation, 27 April 2023 <https://nation.africa/kenya/blogs-opinion/blogs/how-to-help-courts-to-beat-challenges-4215306> on 30th May 2024.

162 Muigua K, 'Tribunals within the Justice System in Kenya: Integrating Alternative Dispute Resolution in Conflict Management', 2019, 2. See also Section 13, Tax Appeals Tribunal Act.

163 Article 169, Constitution of Kenya 2010.

Premises Rent Tribunal, Competition Tribunal, Copyright Tribunal, and many others[164] which oversee specific sectors of government and have proved efficient in resolution of grievances. If established, the Investigatory Powers Tribunal would hold a status similar to that of other subordinate courts, such as Magistrate Courts, Kadhis' Courts etc.[165] Any challenge to the decisions made by the Investigatory Powers Tribunal would be appealed to the High Court.[166]

Currently, Kenya lacks a tribunal specifically tasked with investigating complaints related to surveillance activities. By filling this gap, such a tribunal would enhance accountability within the government and further give effect to Article 47 of the Constitution of Kenya which grants individuals the right to challenge unfair administrative actions that infringe on their rights,[167] and mandates the law to provide avenues for review of such actions by courts or independent and impartial tribunals.[168] Enabling individuals to challenge and seek redress for unauthorized or improper surveillance would foster accountability among government agencies, thus mitigating the risk of abuse of investigatory powers.

CASE STUDY - UK PERSPECTIVE

This part provides an in-depth discussion into a landmark judgment which was issued by the Investigatory Powers Tribunal (IPT) in relation to violation of the right to privacy of individuals. This case is important as it shows the practical benefits of establishing an independent tribunal dedicated to addressing abuses of investigatory powers. It is a classic example of how investigatory agencies can be held accountable for actions done in contravention of the law.

Liberty and Privacy International v. Security Service and Secretary of State for the Home Department [2023] UKIP Trib

164 < Judiciary Tribunals – The Judiciary>, on 12th June 2024.

165 Article 169, Constitution of Kenya 2010.

166 Article 165(3)(c), Constitution of Kenya 2010.

167 Article 47Constitution of Kenya (2010).

168 Article 47(3) Constitution of Kenya (2010).

Facts

This case concerns the failure by the Security Service (MI5) over a considerable period to comply with the statutory safeguards required by the Regulation of Investigatory Powers Act 2000 (R.I.P.A), and the Investigatory Powers Act 2016 (I.P.A) concerning the acquisition and holding of personal data. The relevant safeguards were the retention, review, and disposal (RRD) of personal data within MI5's technology environments. The Relevant datasets fall into two categories, bulk personal datasets (BPD), and bulk communications data (BCD).[169]

The Claimants are non-governmental organizations concerned with the protection of privacy rights. Their major claim was the systemic and systematic non-compliance with the relevant statutory safeguards and related non-statutory arrangements, over a prolonged period, despite considerable knowledge within MI5 of the compliance issues. The relevant period straddles the statutory regimes under RIPA from 2010 and IPA from 2018.[170]

Issues

The issues for determination were:

i. **Whether the warrants and authorizations were issued unlawfully by the Secretary of State (SoS).**
ii. **Whether MI5 breached its duty of full and frank disclosure when applying to the SoS for warrants and directions.**
iii. **Whether there is a systemic failure in the statutory scheme and oversight process under both RIPA and IPA, leading to a systemic breach of Articles 8 and 10?**

[169] *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

[170] *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

iv. Whether the warrants/authorizations should be quashed, and whether the IPT should order data be destroyed.[171]

Tribunal's Analysis

The Tribunal found that there were serious failings in compliance with the statutory obligations of M.I.5 from late 2014 onwards, and those failings ought to have been addressed urgently by the Management Board. It noted that in a MI5 committee paper dated 4 October 2018 it was reported that there were legal compliance risks marked as RED which could lead to legal challenges. The Tribunal found that it had no evidential basis to find that any officers of MI5 did seek to hide any information, but the failure of the Management Board to disclose the compliance failings to the Investigatory Powers Commissioner (IPC) until February 2019 was a serious misjudgment on their part.[172]The Tribunal arrived at the conclusion that the Secretary of State (S.o.S) did breach the Tameside duty in not making adequate enquiries as to whether the statutory safeguards were or were not being met.[173] Given the reports of longstanding non-compliance risks, it was irrational of the S.o.S to not make enquiries as to the scale and nature of the non-compliance. Based on the factual findings, it declared warrants which were issued after late 2014 through to 5 April 2019 to be unlawful in that they did not meet the safeguarding requirements imposed under RIPA or IPA. It further stated that applications for warrants are made without notice to individuals affected by a warrant who may never be aware that their privacy rights have been interfered with. In those circumstances it is of particular importance that the person granting the warrant, namely the SoS, is given full information about any significant non-compliance issues.[174] Moreover, the tribunal added that since MI5 was aware of serious and longstanding issues of non-compliance with

171 *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

172 *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

173 *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

174 *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

statutory safeguards, they had a duty to bring that to the attention of the SoS when seeking a warrant, which they failed to do.[175]

In relation to the Claimants' argument that the safeguards under the UK regime were not adequate and effective due to the failings of the IPC to detect serious and systemic compliance failures which had not been disclosed by MI5 before 27 February 2019.[176] The tribunal stated that robust steps were taken by the IPC once his office had been alerted to the seriousness of the issues and investigations had been carried out, which demonstrates the effectiveness of the safeguard's regime and the adequacy of the measures available to IPCO. It further held that the failure by MIS to report or correct its incompliance in accordance with its statutory duties did not demonstrate that the legal regime was not in accordance with the law.[177]

The Tribunal rejected the plea by the applicants to hold that the product of all warrants be destroyed stating that it would be disproportionate to the unlawfulness. This according to it does not minimize the seriousness of that unlawfulness.

That being the case, this landmark judgement just shows the important role that the Tribunal has played in so far as ensuring the safety of privacy of individuals. It has dissected the national security vis-a-vee privacy arguments and arrived at the conclusion that although there was need to protect national interests in acquisition of the data, proper mechanisms ought to have been followed by the M.I.5 in relation to application for warrants.[178] Setting up robust safeguards and oversight mechanisms, akin to those present in the UK, would help prevent the misuse or abuse of investigatory powers by government agencies in Kenya. By subjecting surveillance activities to independent review, the risk of overreach or unauthorized surveillance would be mitigated.

---

[175] *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

[176] *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

[177] *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

[178] *Liberty and Privacy International v. Security Service and Secretary of State for the Home Department* [2023], The United Kingdom Investigatory Powers Tribunal.

CONCLUSION

The paper in this chapter has done a comparative analysis between Kenya and the United Kingdom in relation to surveillance systems. It has examined both legal and institutional framework. It has looked at the Investigatory Powers Act which provides for Investigatory Powers Commissioner whose task is to oversee the use of investigatory powers by security agencies. It has also looked at the Investigatory Powers Tribunal which provides an avenue for individuals to challenge unauthorized surveillance and seek redress for privacy violations, thereby promoting accountability. The landmark judgment in the ***Liberty and Privacy International v. Security Service*** case highlights the tribunal's role in scrutinizing compliance with statutory safeguards and holding authorities accountable for breaches of privacy rights. Kenya can learn from the UK perspective and adopt requisite changes in legislation to suit its local circumstances.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

INTRODUCTION

This chapter serves as the conclusion of the whole paper. Its discussion is based on three major components. First, it begins by giving a summary of the findings showing whether the research hypothesis has been confirmed or disproved, then provides practical recommendations on the way forward regarding the amendment of section 6(1) of the official secrets Act. Lastly a conclusion is drawn and some recommendations on possible ways of solving the research problems are made.

SUMMARY OF FINDINGS

This study has carried out an extensive analysis on the discourse on surveillance mechanisms and legal and institutional frameworks resulting in several key findings which will be discussed below.

The study utilized the theory of proportionality to emphasize the need for a balanced approach to communication surveillance that weighs the potential benefits of surveillance against their potential harm to individual privacy and human rights. This approach ensures infringements to fundamental rights are conducted lawfully, only when necessary and justifiable. The paper found that judicial oversight is extremely necessary during surveillance, even when conducted for national interests as it promotes accountability, preventing arbitrary interference with privacy rights and abuse of powers.

In the analysis of the first research objective the paper outlined the effectiveness of surveillance in preventing criminal activities and enhancing overall security, citing successful operations such as Tripartite Spider. By apprehending terror suspects and disrupting criminal networks, surveillance measures contribute significantly to public safety and the greater good of society. Despite the benefits, the research sheds light on potential harms that may arise from surveillance such as the erosion of individuals' privacy, increased self-censorship, unlawful profiling, and the risk of abuses of power due to lack of adequate oversight and accountability mechanisms. The paper has examined the '**Nothing to Hide'** argument, which suggests that individuals need not worry about

surveillance if they have nothing to hide. It challenges this perspective by emphasizing the importance of individual privacy rights and autonomy, regardless of innocence or guilt.

In exploring the existing safeguards and oversight frameworks governing data surveillance, the paper identified gaps and areas for improvement. It scrutinized legislative frameworks such as the Constitution of Kenya 2010 and specific statutes governing surveillance activities such as the NIS Act, Official Secrets Act, Data Protection Act, Kenya Information and Communication Act and the Kenya Information and Communication (Consumer Protection Regulations). Despite the constitutional guarantee of the right to privacy and exceptional conditions for its limitations, it found that statutes such as the NIS Act have vague provisions which may lead to the potential misuse of investigatory powers by security agencies. After examining the Official Secrets Act, the paper found that the discretionary powers granted to the Cabinet Secretary to scrutinize personal data without obtaining a court order violate the right to privacy as guaranteed in article 31 of the Constitution of Kenya.

The role of the Communication Authority of Kenya is evaluated, highlighting concerns about political influence and impartiality in oversight mechanisms. The role of the Office of the Data Protection Commissioner (ODPC) is examined, and the paper makes a crucial finding that in Kenya's legal framework there is no established independent body which deals with the scrutiny of investigatory powers of various government agencies which proves to be wanting.

Finally, in the paper's extensive examination of UK surveillance laws in contrast to Kenya, it made an interesting finding in that the UK has an Investigatory Powers Commissioner tasked solely with scrutinizing warrant issuance for government investigations. This Commissioner plays a crucial role in keeping agencies in check. Additionally, their exists an Investigatory Powers Tribunal (IPT) that handles complaints and legal challenges regarding surveillance, ensuring accountability and legal compliance. These oversight mechanisms are absent in Kenya's current legal framework.

RECCOMENDATIONS

Based on the findings, the following recommendations are proposed. To begin with, the paper recommends for the amendment of section 6(1) of the Official Secrets Act to make it mandatory

for the Cabinet Secretary to seek a high court order before accessing personal data. The incorporation of judicial oversight will prevent abuse of powers and foster accountability.

This paper when examining the existing legal frameworks on surveillance in Kenya identified need for strengthening the Communication Authority to enhance its independence from political interference. Clear mechanisms should therefore be established to ensure that regulatory decisions are made impartially and in the public interest, without interference from government or commercial interests.

While legislations such as the Data Protection Act and the National Intelligence Service Act contain provisions aimed at enhancing privacy protections, concerns persist regarding allegations of security agencies such as the National Intelligence Service operating unseemly without adequate oversight, potentially infringing upon constitutional rights and freedoms, necessitating enhanced oversight mechanisms to monitor and ensure compliance.

Upon conducting a comparative analysis with the UK's surveillance framework, this paper identified the need for institutional Reforms in Kenya. Kenya can thus establish independent oversight bodies, akin to the Investigatory Powers Commissioner's Office (IPCO) in the UK, to monitor and regulate surveillance activities. This office should have the authority to conduct investigations, review surveillance warrants, and ensure compliance with legal standards, keeping the security agencies in check. Alternatively, the role of the Data Protection Commissioner's office can be expanded to include oversight of use of investigatory powers by law enforcement and Investigatory agencies. The office of the ODPC is well equipped to take up this role.

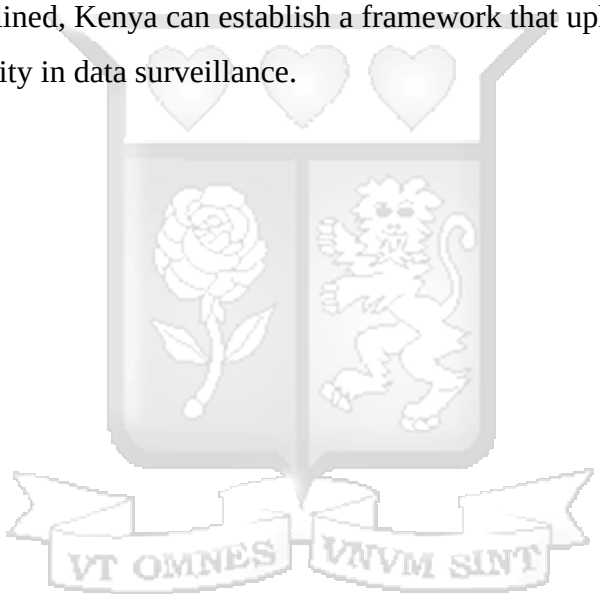
The paper advocates for the establishment of an Investigatory Powers Tribunal (IPT) in Kenya to enable individuals to challenge unauthorized surveillance and seek redress for privacy violations. Judicial oversight through the IPT will ensure surveillance activities are lawful and proportionate thus adequately safeguard privacy rights. Modeled after the UK's framework, this mechanism will promote accountability and transparency, subjecting government surveillance to stringent legal scrutiny.

Lastly, sensitization of citizens is imperative. Kenya should develop a strategy for regularly conducting public awareness campaigns to educate citizens on their rights and the implications of

unchecked government surveillance. This empowers individuals to understand the recourse mechanisms available if their constitutional rights are infringed by surveillance.

CONCLUSION

In conclusion, the dissertation calls for a balance between national interest and the right to privacy in Kenya's legal framework. While surveillance is necessary for safeguarding against emerging threats, unchecked powers pose significant risks to privacy and other civil liberties. The paper recommends for the amendment of section 6(1) of the Official Secrets Act to make it mandatory for the Cabinet Secretary to seek a high court order before accessing personal data. The incorporation of judicial oversight will prevent abuse of investigatory powers. By implementing the recommendations outlined, Kenya can establish a framework that upholds fundamental rights and promotes accountability in data surveillance.



Bibliography

Books:

Resta, G., & Bignami, F, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance.' Oxford University Press, 2018.

Solove, D, 'Conceptualizing Privacy, 'California Law Review, 90(4), 2002.

Solove, D, 'Nothing to Hide: The False Trade-off Between Privacy and Security.' Yale University Press, 2011.

Internet Sources

A Justice Report the State We're in: Addressing Threats & Challenges to the Rule of Law, September 2023 https://files.justice.org.uk/wp-content/uploads/2023/08/31123029/JUSTICE-The-State-Were-In-Addressing-Threats-Challenges-to-the-Rule-of-Law-September-2023.pdf on 24th January 2024.

Alexy R, 'Constitutional Rights and Proportionality' Open Edition Journals, 2014, https://journals.openedition.org/revus/2783 on 3rd March 2023.

Andere B, 'Kenya's Sneak Attack On Privacy: Changes To The Law Allow Government Access To Phone And Computer Data,' < Kenya's Sneak Attack On The Right To Privacy - Access Now>, on 23rd December 2023;

Carothers T & Brechenmacher S, Accountability, Transparency, Participation, And Inclusion:'' A New Development Consensus?' <https://carnegieendowment.org/2014/10/20/accountability-transparency-participation-and-inclusion-new-development-consensus-pub-56968> on 25th January 2024.

Increasing Resilience in Surveillance Societies, Final Report Summary - IRISS (Increasing Resilience in Surveillance Societies) https://cordis.europa.eu/project/id/290492/reporting/fr on 25th January 2024.

International Principles on the Application of Human Rights to Communications Surveillance May 2014 - <Necessary and Proportionate> on 1st March 2023.

Muigua K, 'Tribunals within the Justice System in Kenya: Integrating Alternative Dispute Resolution in Conflict Management', 2019 < https://kmco.co.ke/wp-content/uploads/2019/04/Tribunals-within-the-Justice-System-in-Kenya-Integrating-Alternative-Dispute-Resolution-in-Conflict-Management-Kariuki-Muigua-30th-April-2019.pdf> on 5th June 2024

Kenya's Balancing Act: Securing Citizens While Protecting Privacy <https://www.kictanet.or.ke/kenyas-balancing-act-securing-citizens-while-protecting-privacy/> on 27th May 2024.

Mavedzenge A, 'Necessity, Proportionality and Accountability in Law Enforcement Use of Personal Data' 8 https://rm.coe.int/council-of-europe-presentation-justice-alfred-mavedzenge-2754-8385-792/1680a1a50d on 3rd March 2023.

Privacy International 'State of Privacy Kenya' 29 January 2019 https://privacyinternational.org/state-privacy/1005/state-privacy-kenya> on 29 May 2024.

Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa - ACHPR/Res.573 (LXXVII) 2023 https://achpr.au.int/en/adopted-resolutions/573-resolution-deployment-mass-and-unlawful-targeted-communication> on 29th May 2024.

Welekwe A, Comparitech 'What is a Privacy Impact Assessment (PIA)?' on 27th June 2021, < What is a Privacy Impact Assessment? When & How to Undertake it (comparitech.com)>, on 1st January 2024.

<https://www.interpol.int/en/News-and-Events/News/2023/14-terror-suspects-arrested-in-African-operation>, on 13th February 2024.

Jeremy Bentham: 'It is the greatest good to the greatest number of people which is the measure of right and wrong.' — The Socratic Method (socratic-method.com)>, on 13th February 2024.

< Why the "nothing to hide" argument is privacy's biggest battle (ipvanish.com)>, on 2nd January 2024.

< Kenya: Official Secrets Act incompatible with freedom of expression standards - ARTICLE 19>, on 23rd December 2023.

<Safeguards governing investigatory powers come into effect - GOV.UK (www.gov.uk)>, on 9th January 2024.

<About the Tribunal - The Investigatory Powers Tribunal>, on 7th January 2024.

Journal Articles:

Badurdeen F, 'Digital Surveillance and Privacy Concerns in The Counter Terrorism Discourse in Kenya: Policy Implications' 2017.

Christopher Parsons and Adam Molnar, "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports" 16 Canadian Journal of Law and Technology 16(1), 2018.

Chinmayi A, 'Paper-Thin Safeguards and Mass Surveillance in India.' National Law School of India Review, 26(2), 2014.

Davis R, 'Striking the Balance: National Security vs Civil Liberties' Brooklyn Journal of International Law 29(1, 2003.

Hiya G, Pushya C, National Security vs. Right to Privacy: A Conflict of Interests', International Journal of Law and Management studies, 5(4), 2021.

Ignacio N, 'Nothing to Hide, But Something to Lose.' The University of Toronto Law Journal, 70(1), 2020.

Iphofen R, Ethical issues in surveillance and privacy: Human Factors Theory and Application, Open University,2014.

Kibet E, 'Transformative constitutionalism and the adjudication of constitutional rights in Africa', African Human Rights Law Journal,2017.

Laberge C, 'To What Extent Should National Security Interests Override Privacy in a Post 9/11 World. 'Victoria University of Wellington Working Paper Series, 2010

Moller K, Proportionality: Challenging the critics. Oxford University Press and New York University School of Law, 2012,710.

Mavedzenge A, The right to privacy v national security in Africa: Towards a legislative framework which guarantees proportionality in communications surveillance. African Journal of Legal Studies,2020.

Murray D & Fussey P,'Bulk Surveillance in The Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data.' Israel Law Review, 52(1), 2019.

Mitsilegas V, Elspeth Guld E, Kuskonmaz & Vavoula N, 'Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks, European Law Journal 29 (1), 2023.

Ombaka D, 'Christians and the 2010 constitution referendum in Kenya: A search for explanations from a retrospective study', International Journal of Arts and Commerce, 2(5),2013.

Oves A & Ayesha M, 'Cyber Surveillance and Big Data - Pakistan's Legal Framework and the Need for Safeguards', RSIL Law Review 2020.

Roderick C, Akemi T and Jaramillo P, 'Public opinion on National Security Agency surveillance programs: A multi-method approach', Government Information Quarterly, 32(2), 2015.

Resta G and Bignami F, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance, Oxford University Press, 2018.

Rajan M, "The Idea of National Interest." The Indian Journal of Political Science 14 (3),1953.

Reinhard S, The Judicial Role in National Security, 86 Boston University Law Review, 2006, 1309.

Solove J, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, Washington University Law School, 2007, 747.

Torrorey K, 'Trust and Concern: The Balance Between Privacy in A Digital Age and Counter Terrorism in Kenyan Law,' Strathmore University, 2016.

Zartner D, 'Internalization of International Law', International Studies Department, University of San Francisco, 2020, 10.

Zwart M & Humphrey S, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK,' University of New South Wales Law Journal, 37(2)2, 2014.

Thesis

Kinyanjui A, Data Protection as a Human Right; Balancing the Right to Privacy and National Security in Kenya, University of Nairobi,2017, 12.

Olasya P, 'Assessing the Impacts of Social Media on National Security in Kenya' Published, University of Nairobi, Nairobi, 2018.

Torrorey K, 'Trust and Concern: The Balance Between Privacy in A Digital Age and Counter Terrorism in Kenyan Law', Strathmore University, 2016, 6.

Reports:

Privacy International (PI), 'The Right to Privacy in Kenya', Joint Stakeholder Report, 2019.

Sheinin M, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 2009,13.