Strathmore University
Law School

LOOKING AHEAD: STRIKING A BALANCE BETWEEN PRIVACY AND NATIONAL SECURITY AND PUBLIC INTEREST IN THE USE OF DIGITAL INTERMEDIARY PLATFORMS

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

By

MOGAKA SANDRA GESARE

146090

Prepared under the supervision of

DR LYNETTE OSIEMO

MARCH 2025

Word count: 12250 words (excluding footnotes)

TABLE OF CONTENTS

ACKNOWLEDGEMENTS iv
DECLARATION v
LIST OF CASES vi
LIST OF LEGAL INSTRUMENTS vi
LIST OF ABBREVIATIONS vi
ABSTRACT vii
CHAPTER 1 1
1.0. BACKGROUND 1
1.1. PROBLEM STATEMENT 4
1.2. RESEARCH OBJECTIVES 5
1.3. RESEARCH QUESTION 5
1.4. HYPOTHESIS 6
1.5. JUSTIFICATION OF THE STUDY 6
1.6. LITERATURE REVIEW 7
1.6.1. On the Potential Risks and Benefits of Surveillance 7
1.6.2. On the Principles or Essential Elements of Surveillance Law 9
1.7. LIMITATIONS OF THE STUDY 11
1.8. THEORETICAL FRAMEWORK 11
1.8.1. Legal Realism 11
1.9. METHODOLOGY 12
1.10. CHAPTER BREAKDOWN 13
CHAPTER 2 14
2.0. LEGAL FRAMEWORK 14
2.1 INTRODUCTION 14
2.2. NATIONAL LEGISLATION 15
2.2.1 The 2010 Constitution of Kenya 15
2.2.2. Data Protection Act 15
2.2.3. Computer Misuse and Cybercrimes Act 18
2.2.4. Access to Information Act 18
2.3. INTERNATIONAL LAW 19
2.3.1. International Instruments 19
2.3.1.1. Universal Declaration of Human Rights 19

2.3.2. International Treaties and Conventions 20
2.3.2.1. International Covenant on Civil and Political Rights 20
2.3.2.2. African Union Convention on Cyber Security and Personal Data Protection 20
2.4. REGULATION FRAMEWORK 21
2.4.1. National Transport and Safety Authority (Transport Network Companies, Owners, Drivers, and Passengers) Regulations 21
2.5. CONCLUSION 22
CHAPTER 3 23
3.0. MEASURES TAKEN BY DIGITAL INTERMEDIARY PLATFORMS IN PROTECTING THEIR CONSUMERS PRIVACY AND ABIDING BY PUBLIC INTEREST AND NATIONAL SECURITY CONCERNS 23
3.1. INTRODUCTION 23
3.2. MEASURES TAKEN BY DIGITAL INTERMEDIARY PLATFORMS 23
3.2.1. Measures taken by digital intermediary platforms in protecting their consumers' privacy 23
3.2.2. Measures taken by digital intermediary platforms in abiding by public interests and national security concerns. 25
3.3. CONCLUSION 27
CHAPTER 4 29
4.0. PRINCIPLES AND ESSENTIAL ELEMENTS OF LAW NEEDED TO ENSURE A BALANCE OF PRIVACY RIGHTS, PUBLIC INTEREST, AND NATIONAL SECURITY 29
4.1. INTRODUCTION 29
4.2. PRINCIPLES AND ESSENTIAL ELEMENTS OF SURVEILLANCE LAWS 29
4.3. CONCLUSION. 33
CHAPTER 5 34
5.0. CONCLUSION AND RECOMMENDATIONS. 34
5.1. CONCLUSION 34
5.2. RECOMMENDATIONS 35
BIBLIOGRAPHY 36

ACKNOWLEDGEMENTS

I would first like to thank the Almighty God for giving me the strength to work and finish on this dissertation. Secondly, I would like to acknowledge and express my deepest appreciation to my supervisor, Dr Lynette Osiemo, for her guidance and patience throughout the process of drafting this dissertation. Lastly, I would like to thank my parents, Mr. William Mogaka, and Ms. Josephine Makori for providing me with moral support while I was drafting this dissertation.

DECLARATION

I, [MOGAKA SANDRA GESARE], 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: .....

Date: .....13th March 2025.....

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

Signed: ..... 18 March 2025

Dr. Lynette Osiemo

LIST OF CASES

Aukot & 2 others v National Security Council & 5 others (2024).

John Muriithi & 8 others vs. Registered Trustees of Sisters of Mercy (Kenya)t/a "The Mater Misericordiae Hospital & another [2018].

Okiya Omtatah Okoiti v Communications Authority of Kenya & 21 others (2017).

Republic v Diana Suleiman Said & Mahadi Swaleh Mahadi Alias Jesus (2014).

LIST OF LEGAL INSTRUMENTS

Access to Information Act (Act No. 107 of 2016)

Constitution of Kenya (2010)

Computer Misuse and Cybercrimes Act (Act No. 58 of 2018)

Data Protection Act of Kenya (Act No. 24 of 2019).

The Universal Declaration of Human Rights

The International Covenant on Civil and Political Rights

The African Union Convention on Cyber Security and Personal Data Protection.

National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012)

LIST OF ABBREVIATIONS

Digital Intermediary Platforms - DIPs

ABSTRACT

Individual Privacy rights are the basis of most privacy protection laws but with increased development and societal interests, the need to limit the rights has increased. Society at large has had a growing reliance on the different technologies being developed, especially on Digital Intermediary Platforms. This study recognizes this reliance especially on Digital Intermediary Platforms that function as intermediaries between different service providers and potential customers. These platforms have lately been threatened and are used to facilitate criminal activities threatening internal security in the country. Due to this reliance, there is a need to balance privacy rights with national security concerns and public interest concerns which leads to a limitation on privacy rights.

The study examines the legal and regulatory framework challenges that arise when balancing privacy, security, and public interest concerns. It also examines the risks and benefits of privacy threatening practices such as surveillance and their implications to give practical recommendations to be implemented that balance the different concerns. The study is grounded in the understanding that to be able to manage modern situations, such as the Digital Intermediary Platforms, and address modern concerns, the law should constantly evolve to cater for such situations and concerns. The study identifies the gaps in the legal framework and seeks to provide ways to balance privacy, security, and public interest concerns in relation to Digital Intermediary Platforms

CHAPTER 1

1.0. BACKGROUND

Before the nineteenth century, privacy was not considered to be an issue to be protected.[1] It is considered a recent invention leading to different states forming specific laws to protect it.[2] In the Kenyan context, the right to privacy is provided for under the 2010 Constitution of Kenya as fundamental human right and it includes the right to not have one's information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed.[3] One may ask then what is privacy and what does the right to privacy entail? Privacy can be defined as the ability a person has to control attainment or release of information about themselves.[4] Hence the right to privacy entails that a person has the right to have control over one's personal information and to conduct one's affairs without unwanted intrusions.[5]

As a fundamental right, the state has a mandate to protect the right from various threats. Threats to privacy mainly involve obtaining and use of personal information without owners consent or threats to privacy can manifest itself during either collection , processing or dissemination of one's information.[6] Both government and private organisations have relied on individual personal information to provide different services.[7] They can access this information through surveillance which generally means keeping a close watch over someone or something,[8] or aggregation involves combining different information on a person to create a new piece of information.[9] Neil Richards gives a deeper understanding of the term surveillance terming it as the focused, systematic and routine attention to personal details for the purpose of management, protection or direction.[10] This definition is noteworthy as the terms focused, systematic, routine and for the purpose expand our understanding on what surveillance is and its purposes.[11] The term focused

[1] Froomkin M, *'The Death of Privacy?'*,52 Stanford Law Review 5, 2000, 1467.
[2] Froomkin M, *'The Death of Privacy?'*, 1467.
[3] Article 31, *Constitution of Kenya* (2010).
[4] Froomkin M, *'The Death of Privacy?*' 1463.
[5] Okiya Omtatah Okoiti v Communications Authority of Kenya & 21 others (2017) eKLR
[6] Solove D, 'I've got nothing to hide and other misunderstandings of privacy,' GWU Law School Public Law Research Paper Number 289, 2007, 758-<https://ssrn.com/abstract=998565>- on 31 December 2024.
[7] Froomkin M, *'The Death of Privacy?*',1472.
[8] Merriam Webster Dictionary, 11 ed.
[9] Solove D, *'I've got nothing to hide and other misunderstandings of privacy*', 766.
[10] Richards N, *'The Dangers of Surveillance'* 126 Harvard Law Review 7, 2013, 1937.
[11] Richards N, *'The Dangers of Surveillance,'* 1937.

means that the practice of surveillance directs its attention and interest in learning information on individuals while the term systematic means that surveillance actions are intentional and not random.[12] The other terms of routine and for the purpose generally indicate that it is part of the ordinary administrative apparatus for the state and private organisations in society to influence or control their ends.[13]

The state uses information it has obtained from surveillance or aggregation to provide services such as issuing of national identity cards, birth certificates, passports, conducting census, collect taxes, promote security and many other functions and services.[14] Private organisations on the other hand mainly conduct surveillance to analyse data on their consumers in order to profit and conduct marketing and advertising.[15] The information obtained however is required under law to be collected with the knowledge and consent of the data subject without prejudicing their interests.[16] Though privacy as discussed above is always required to be protected, recent developments have shown the need to limit privacy rights in order to achieve the benefits that arise from doing so. This can be observed by the provision of Article 24 of the Constitution which provides for the ability of Parliament to create laws to limit rights to the extent that is reasonably justifiable.[17] The law recognizes the changing circumstances of society which is due to either the evolving societal interests or technological advancements that have occurred through time constantly expanding the scope of privacy.

With the use and development of technology, different government and private individuals have increased their surveillance practices and have invented new ways of conducting surveillance.[18] Different digital services and platforms have emerged that require personal data to operate hence are burdened with the mandate of protecting the privacy of the users.[19] Digital Intermediary

[12] Richards N, *'The Dangers of Surveillance*,' 1937.
[13] Richards N, *'The Dangers of Surveillance,'* 1937.
[14] Froomkin M, *'The Death of Privacy?*' 1472.
[15] Richards N, *'The Dangers of Surveillance,'* 1938.
[16] Section 28, Data Protection Act (Act No. 24 of 2019).
[17] Article 24, *Constitution of Kenya* (2010).
[18] ECNL Learning Centre, 'Technology and Artificial Intelligence: Surveillance technology' ECNL Learning Centre, 10 December 2024-< https://learningcenter.ecnl.org/learning-package/surveillance-technology >- on 10 December 2024
[19] Owano J, 'Data Privacy And Protection In Kenya: The New Corporate Risk', 8 October 2024 -< https://www.businessdailyafrica.com/bd/opinion-analysis/columnists/data-privacy-and-protection-in-kenya-the-new-corporate-risk-4788892 >- on 10 December 2024

Platforms, here henceforth referred to as DIPs such as Uber or Bolt which are online platforms that connect drivers and riders for various types of rides and Airbnb or Booking.com which are online platforms that are used to connect property owners and potential tenants for booking a place to stay or for renting out your property in different places in the world for a specific timeframe. These platforms provide a basis where a service provider is connected to different potential consumers. These platforms involve different parties that are not tied to the owners of the platform, raising questions on the risk of third-party usage of personal information.

The nature of these platforms has brought about new dangers to society as it has increased the level of crimes occurring. Recently different news reports have brought to light different security concerns on the use of these platforms. At the beginning of 2024 alone, it was recorded that a woman was brutally murdered in an Airbnb in South B, Nairobi.[20] South B is a division within the subcounty of Starehe Constituency in Nairobi County in Kenya.[21] After less than two weeks another woman was also brutally murdered in an Airbnb in Nairobi County.[23]Airbnb however put out a public statement that the events were not connected to them as the girls were not registered under the system.[24] Airbnb in this sense means the property listed under the platform, that is the property that the owners list in the platform as available for booking and the potential customer books a stay in.[25] These murders in the Airbnb's contributed to the rise of femicide cases in Kenya. Femicide is killing of a woman or a girl because of her gender.[26]

[20] Kiage N and Ngigi E,' Police open probe after Nairobi socialite Starlet Wahu is stabbed to death in South B AirBNB' Daily Nation, 7 January 2024 -<https://nation.africa/kenya/counties/nairobi/puzzle-hiv-test-kit-dead-socialite-starlet-wahu-south-b-airbnb--4483656>- on 26 November 2024

[21] Hauzisha, 'South B', Hauzisha,24 February 2024-<https://hauzisha.co.ke/blog/about-south-b/>-on 24 February 2024

[23] Kupemba D, 'Kenya Femicide: A woman's murder exposes the country's toxic online misogyny', on 15 January 2024, BBC-<https://www.bbc.com/news/world-africa-67987347>- on 26 November 2024.

[24] Airbnb, 'A statement fromAirbnb on Kenya' Airbnb Newsroom, 15 January 2024 -<https://news.airbnb.com/a-statement-from-airbnb-on-kenya/>- on 26 November 2024.

[25] Folger J, 'How Airbnb works- for hosts, guests and the company itself', Investopedia, 13 December 2024 -<https://www.investopedia.com/articles/personal-finance/032814/pros-and-cons-using-airbnb.asp>- on 24 February 2024.

[26] European Institute of Gender Equality, *Femicide: a classification system*, 2021, 9.

In 2020 Kenya saw a rise of what was termed as 'Uber attacks'.[27] Uber attacks are where criminals attack uber drivers while posing as customers or uber drivers attacking their customers.[28] These attacks and crimes occurring through the use of the platforms are threats to the users of the platform which is why concerns on national security and public interest are raised. These events raise the question, if limitations were placed on privacy rights regarding such platforms will it enable prevention of such crimes?

Digital intermediaries have different functions which are mainly to provide infrastructure, to collect, organise and evaluate dispersed information, to facilitate social communication and information exchange, to aggregate supply and demand, to facilitate market process, to provide trust and to take into account the needs of the users.[29] They generally do not have a general monitoring and surveillance obligation.[30] Threats to society and the security of the state are the main reasons to the limitation of privacy rights as greater risks may be suffered if the right to privacy is upheld disregarding security and public interest concerns.[31] Surveillance can be used to monitor individuals when they are using DIPs to ensure security and public interest concerns are addressed although limiting the right to privacy.

1.1. PROBLEM STATEMENT

Article 31 of the Constitution of Kenya provides for the right to privacy. This right is among those limited by Article 24 to the extent that is reasonably justifiable. With recent expeditious technological developments in the use of DIPs, various security concerns have arisen. These DIPs involve strict privacy protection regulations that need to be limited to promote public interest and to help address security risks.[32] A lack of limitation of such regulations exposes vulnerable consumers to various exploitations.

[27]BBC News, 'Kenya investigates 'barbaric' uber attacks in Nairobi', BBC News, 2 February 2016 -<https://www.bbc.com/news/world-africa-35476405>- on 26 November 2024

[28] BBC News, 'Kenya investigates 'barbaric' uber attacks in Nairobi', BBC News, 2 February 2016 -<https://www.bbc.com/news/world-africa-35476405>- on 26 November 2024.

[29] OECD, 'The Role of Intermediaries in Advancing Public Policy Objectives', OECD Publishing, 2011, 13

[30] OECD, 'The Role of Intermediaries in Advancing Public Policy Objectives', OECD Publishing, 2011, 13

[31] Manes J, 'Online service providers and surveillance law transparency' 125 Yale Law Journal Forum, 2016, 356.

[32] Generis Global Legal Services, 'Understanding data protection and privacy laws in Kenya', Generis Global Legal Services, 20 November 2024, -<https://generisonline.com/understanding-data-protection-and-privacy-laws-in-kenya/>- on 9 December 2024.

Intermediary platforms often involve many parties such as users of the platforms or the buyers who seek the service, the advertisers or sellers who provide the service and the platform company which provides the system that connects the buyers and sellers.[33] The platforms only act as an intermediary hence, if a crime were to be committed through its use, it would be hard to access all requisite information required by the government to hold the party responsible for the crime liable due to stringent privacy protection guidelines. As such, an increase in criminal activities continues to be inevitable hence threatening the security of the other parties who are primary consumers of the intermediary services and products. Therefore, this study will examine privacy limitation laws that exist which can be updated or adjusted to be relevant to the use of DIPs to help prevent security risks.

1.2. RESEARCH OBJECTIVES

1. To examine the legal framework governing privacy protection and limitation in Digital Intermediary Platforms in Kenya.
2. To analyse measures taken by Digital Intermediary Platforms to protect privacy of their users while adhering to public interest and national security concerns.
3. To examine the principles and essential elements of law needed to ensure a balance of privacy rights, public interest, and national security.
4. To propose recommendations and conclusions.

1.3. RESEARCH QUESTION

1. What is the legal framework governing privacy protection and limitation in Digital Intermediary Platforms in Kenya?
2. What are the measures taken by Digital Intermediary Platforms to protect the privacy of their users while adhering to public interest and national security concerns?
3. What are the principles and essential elements of law needed to ensure a balance of privacy rights, public interest, and national security?
4. What recommendations and conclusions should be made?

[33] IMF, OECD, UNCTAD and WTO, *Handbook on measuring digital trade*,28 July 2023, 93.

1.4. HYPOTHESIS

The right to privacy is recognized as a fundamental right in the constitution and in international laws and treaties.[34] However, this right is limited in the Constitution, which recognizes that fundamental rights can be limited by law.[35] This is seen for example in the Computer Misuse and Cybercrimes Act of 2018 grants police officers' power during criminal investigations to among others search and seize computer data.[36] This is a justifiable limitation of the right to privacy by law as it addresses security concerns in the use of computers. DIPs require a law that gives them a general duty and obligation to monitor and surveil activities conducted through their platforms to ensure national security concerns are addressed. The study argues that a law limiting privacy rights of DIPs similar to how the Computer Misuse and Cybercrimes Act does is important in the use of DIPs to address public interest and national security concerns.

1.5. JUSTIFICATION OF THE STUDY

The government has highlighted the need for Airbnb's to register with the Tourism Regulatory Authority after the femicide cases as they have recognized the need for them to be regulated in order to guarantee that such properties meet strict standards of security.[37] Despite the numerous laws on security and data protection in Kenya, no law has been formulated to regulate DIPs to ensure they promote security and public interest . Due to this, the study is important as it is a unique contribution to the scope of law as it proposes a new angle of limiting privacy laws and using surveillance laws to help hold service providers to strict standards and ensure safety and security. This study will benefit users of different service platforms if considered as it pushes for their safety and for their data protection. It will also benefit law and policy makers by giving them a fresh view to design sound and logical law and policies to ensure service platforms are held to strict standards to ensure security of their customers and service providers without undermining privacy rights.

[34] Article 31, *Constitution of Kenya* (2010).
[35] Article 24, *Constitution of Kenya* (2010).
[36] Section 53, *Computer Misuse and Cybercrimes Act* (Act No. 5 of 2018
[37] Nairobi County Assembly, 'Regulation of Airbnb services within the county', Nairobi County Assembly, 10 September 2024-<https://nairobiassembly.go.ke/motion/regulation-of-airbnb-services-within-the-county/>- on 9 December 2024

1.6. LITERATURE REVIEW

Different literature based on surveillance and its risk to individual rights are available as the topic has been written upon with the rise of technology and the use of artificial intelligence. Surveillance being a core source to obtain data on individuals, many authors write with the fear that individuals' rights, especially privacy and data protection, may be infringed.

1.6.1. On the Potential Risks and Benefits of Surveillance

This section highlights the potential risks and benefits of surveillance actions as determined by different authors. As surveillance actions involve monitoring an individual to collect data it poses a major risk to the individuals' privacy, especially since the individual might not be aware of such actions being conducted against them. Neil Richards speaks greatly on this topic in his article *'The Dangers of Surveillance'* where he tries to explain the harms present in surveillance.[38] He discussed this by focusing on the broader topic that the society lacks an understanding of the dangers related to surveillance due to its large scope as it is mainly conducted in the form of government surveillance and private surveillance with or without the society's knowledge.[39] The lack of knowledge on surveillance actions or the ignorance towards such practices can greatly detriment one's privacy hence the need to be fully aware of any way their information may be collected and used. Neil Richards discusses how surveillance causes dangers such as creation of a power imbalance between the watcher and the person being watched which can lead to blackmail, discrimination, undue persuasion and have a chilling effect on free speech.[40] He also recognizes that surveillance poses benefits such as better security in the state from crime and terrorism, improved quality of life and convenience of modern technology and communications which are important for the peace and development of a country.[41]

Michael Froomkin in his Article, '*The Death Of Privacy?',* he recognizes that surveillance collects data and organises it into centralised or distributed databases that have consequences beyond the simple loss of privacy.[42] According to him, various forms of discrimination such as price

[38] Richards N, *'The Dangers of Surveillance,'* 1936.
[39] Richards N, *'The Dangers of Surveillance,'* 1939.
[40] Richards N, *'The Dangers of Surveillance,'* 1953.
[41] Richards N, *'The Dangers of Surveillance,'* 1944.
[42] Froomkin M, *'The Death of Privacy?*' 1469.

discrimination occurs as data accumulation enables construction of personal profiles for individuals grouping them into various sorts of categories which facilitate targeted marketing.[43] Once such information is made public it may lead to discrimination and may cause a chilling effect on the speech, conduct and reading of individuals as they have a fear that someone is watching them.[44]

Michael Froomklin highlights the danger and benefit of government surveillance and classifies the dangers to how it affects individuals and society. According to him, once the government obtains access to data it gains a powerful investigative tool to map movement actions and financial activities of suspects and gains new methods for identifying suspects and detecting crimes.[45] He highlights that surveillance practices like obtaining everyone's location and transactions will make it possible to achieve a perfect law enforcement and create a society where no crimes go unnoticed or unpunished.[46] Even though he highlights this as a benefit he recognizes a further danger that such access to this information will cause the government to construct personal profiles to predict possible crimes before they happen.[47] This is a danger as people meeting the criteria will be profiled and flagged as dangerous which can lead them to being discriminated against or subject them to increased surveillance and searches.

Fathima Badurdeen wrote an article titled *'Digital Surveillance and Privacy Concerns in the Counter Terrorism Discourse in Kenya: Policy Implications'.*[48] According to her, there is great importance in balancing national security and privacy laws when forming surveillance laws due to the issues that it requires the people to sacrifice their privacy rights to some degree in order for the government to perform its national security functions effectively.[49] She does this by emphasising the roles of surveillance in counter-terrorism and the importance of surveillance laws in ensuring national security. The article's main argument was on the need to balance individual rights to

[43] Froomkin M, *'The Death of Privacy?*' 1469.
[44] Froomkin M, *'The Death of Privacy?*' 1470.
[45] Froomkin M, *'The Death of Privacy?*' 1470.
[46] Froomkin M, *'The Death of Privacy?*' 1470.
[47] Froomkin M, *'The Death of Privacy?*' 1471.
[48] Badurdeen F, '*Digital Surveillance and Privacy Concerns in the Counter Terrorism Discourse in Kenya: Policy Implications'* SSRN, 2017, 11, -<https://ssrn.com/abstract=3058666>-on 8 March 2024.
[49] Badurdeen F, '*Digital Surveillance and Privacy Concerns in the Counter Terrorism Discourse in Kenya: Policy Implications'* SSRN, 2017, 11, -<https://ssrn.com/abstract=3058666>-on 8 March 2024.

matters of the common good such as National Security while focusing on the contextual analysis of terrorism in Kenya and surveillance practices. This article is important to this work as it highlights the importance of the balance between surveillance and individual rights that laws are required to provide to effectively govern surveillance practices.

Contribution to the study

Due to the dangers and risks highlighted above, many academics believe that in the age of surveillance, maintaining privacy is becoming impossible. Hence there is a need for Surveillance Laws to ensure that the risks that surveillance practices cause are minimised, and the benefits are maximised. This is as the world can no longer operate without surveillance practices as they are needed for different developments to occur. A balance should hence be struck to ensure that surveillance practices risks should not be greater than the benefits they accrue. This study advocates for surveillance practices due to the benefits it accrues and aims to find a way in which surveillance laws can be used to mitigate the risks surveillance practices pose.

1.6.2. On the Principles or Essential Elements of Surveillance Law

According to Neil Richards, principles must be developed to guide in the formation of surveillance laws while aiming to strike the balance between the benefits and risks of surveillance. He provides four principles to guide on shaping the law on surveillance. The principles he advocates for are that there needs to be a recognition that surveillance transcends the public/private divide,[50] secret surveillance is illegitimate,[51] total surveillance is illegitimate,[52] and that surveillance is harmful.[53] The strength of Neil Richards article is that it proposes principles to guide evolution of the law of surveillance and identifies values that they ought to protect which can be considered as a threshold to help analyse the legitimacy of surveillance actions. However, Richards's article poses a weakness as it mainly focuses on surveillance in the western world without considering how other government systems or other countries have tackled the issue.

[50] Richards N, *'The Dangers of Surveillance'*, 1959.
[51] Richards N, *'The Dangers of Surveillance,'* 1960.
[52] Richards N, *'The Dangers of Surveillance,'* 1962.
[53] Richards N, *'The Dangers of Surveillance,'* 1963.

Steven Feldstein authored a report on '*The Global expansion of AI Surveillance'* where he gives his findings on the rapid use of AI surveillance.[54] Though his report mainly focused on the statistics on the use and distribution of AI surveillance worldwide, part of his report distinguished between legitimate and illegitimate surveillance. He focused mainly on state surveillance providing that there are legitimate reasons to support state surveillance that should be distinguished from unlawful surveillance.[55]

Feldstein distinguishes lawful and unlawful surveillance by recognizing that one needs to consider the three principles raised in international human rights law to assess whether a surveillance action is lawful. The principles are first whether domestic law allows for surveillance.[56] Second is if the surveillance action meets the international standards of necessity and proportionality.[57] The third principle is whether the interests justifying the action are legitimate.[58] The strength of this report is that it does advocate for surveillance stating its benefits in the society and government and also recognizes the illegitimacy that may arise from the use of surveillance. The only weakness that can be pointed out is that the index he uses does not provide for the legitimate or illegitimate use of surveillance by different companies, hence cannot project the risks and benefits of surveillance to the companies or to the people. He also does not demonstrate whether the laws provided after considering the principles still pose a legal problem. The report though is greatly beneficial in this work as it provides a criterion on analysing the different laws provided to determine the legal problem and provide remedies for the same.

Contribution to the study

This study recognizes that there are certain elements or principles that are important to the creation and formalisation of privacy laws in order to achieve the balance needed to ensure that surveillance practices regardless of whether practiced by the government or private entities do not pose dangers

[54] Feldstein S, Carnegie Endowment for International Peace, *Distinguishing Between Legitimate and Unlawful Surveillance*, 2019, 11-12.
[55] Feldstein S, Carnegie Endowment for International Peace, *Distinguishing Between Legitimate and Unlawful Surveillance*, 2019, 11.
[56] Feldstein S, Carnegie Endowment for International Peace, *Distinguishing Between Legitimate and Unlawful Surveillance*, 2019, 12.
[57] Feldstein S, Carnegie Endowment for International Peace, *Distinguishing Between Legitimate and Unlawful Surveillance*, 2019, 12.
[58] Feldstein S, Carnegie Endowment for International Peace, *Distinguishing Between Legitimate and Unlawful Surveillance*, 2019, 12.

to the civil society of the state. Literature referred to have provided for different principles and elements that can be used to achieve the said balance hence important to the study.

1.7. LIMITATIONS OF THE STUDY

An increase in new surveillance technologies and DIPs are continuously being developed that many people do not understand the scope in which such technologies surveil or monitor them.[59] This is a limitation to the study as different technologies may require a different way of regulating and using them in order to balance the right to privacy with public interest with national security concerns. As they have not yet been fully understood as to how they may pose a risk amounting to a public interest or national security concern they cannot be incorporated in the study. In order to mitigate this there is need for one formal consolidated law on DIPs that can be formulated in a manner that caters for the new or yet to be developed technologies of DIPs to facilitate regulation on their use.

1.8. THEORETICAL FRAMEWORK

1.8.1. Legal Realism

The legal realism theory, founded by Oliver Wendell Holmes Jr and further discussed by Alf Ross, is a theory that looks at how law in practice differs from written laws putting emphasis on the facts and that law should be used to serve social needs.[60] It is classified into American Legal Realism and Scandinavian Legal Realism.[61] Oliver was the main proponent for American realism stating that "*Life of law has not been logic but experience"*.[62] This means that the law evolve with the needs of society taking into consideration the process resulting in the need and not just logical deductions.[63] Alf Ross on the other hand supported Scandinavian realism which involved the law being purely in terms of observable facts and the study of such facts emphasising the need to base legal notions on hard empirically verifiable facts.[64] He also emphasises the concept of validity of

[59] Oluwatosin R, Nkechi E, Ehimuan B, Anyanwu A, Olorunsogo T and Temitayo O, 'Privacy law challenges in the digital age: A global review of legislation and enforcement' 6(1) *International Journal of Applied Research in Social Sciences,* 2024, 79.
[60] Gilmore G, 'Legal realism: Its cause and cure' 70(7) The Yale Law Journal, 1961, 1038.
[61] Alexander G, 'Comparing the two legal realisms: American and Scandinavian' 50(1) *The American Journal of Comparative Law,*2002,131.
[62] Jones H, 'Law and morality in the perspective of legal realism,'61(5) *Columbia Law Review*, 1961, 799.
[63] Jones H, 'Law and morality in the perspective of legal realism,' 801.
[64] Hart A, 'Scandinavian Realism,'17(2) The Cambridge Law Journal, 1959, 236.

rules by determining the effectiveness of the rule as established by observation of the facts and the extent to which the rules are regarded as binding.[65]

American Legal realism mainly arises from the skepticism on the uncertainty that is in rules as they can be interpreted in different ways and it advocates that courts are to mainly engage with the facts of the cases when deciding a matter.[66] It perceives law as dynamic and evolving with the aim of regulating and managing social interactions heavily relying on societal impact of the rules in assessing its efficiency.[67] It is mainly relevant in discussions on data privacy.[68] Scandinavian Legal Realism on the other hand takes an approach that calls for observation and experimentation rather than relying on theories when forming laws and it considers the role of the social context in shaping the law or legal norms.[69]

Relevance of the theory to this Study

The study in relation to this theory takes the view that for the law to be effective and valid, there should be a clear observation of the facts surrounding the law to determine whether it has served its purpose. It is premised on the fact that the law should be constantly evolving in order for it to reflect the current circumstances and experience of its subjects, ensuring its relevance and effective implementation. This study critiques the various laws regulating privacy and security concerns on DIPs through the legal realism framework holding that laws involving regulating these concerns should serve the current needs of society.

1.9. METHODOLOGY

This study will adopt the doctrinal research method relying on both primary and secondary sources. It will primarily rely on secondary sources such as journal articles, reports and news outlets while

[65] Holtermann J, 'Naturalizing Alf Ross's Legal Realism: A Philosophical Reconstruction' 24 *Revus - Journal for Constitutional Theory and Philosophy of Law*, 2014,172.
[66] Ramisetty R, 'A critical analysis on American legal realism and Scandinavian legal realism: Similarities and differences' 2(2) International Journal of Legal Studies and Social Sciences, 2024, 30
[67] Ramisetty R, 'A critical analysis on American legal realism and Scandinavian legal realism: Similarities and differences,' 32
[68] Ramisetty R, 'A critical analysis on American legal realism and Scandinavian legal realism: Similarities and differences', 34
[69] Ramisetty R, 'A critical analysis on American legal realism and Scandinavian legal realism: Similarities and differences', 36

also relying on some primary sources such as the Constitution, case legislation and various regional and international instruments.

1.10. CHAPTER BREAKDOWN

Chapter 1: This chapter comprises the introductory part of the study. It introduces the concept of privacy. It highlights the different ways in which privacy rights can be limited in favour of national security and public interest.

Chapter 2: The second chapter presents the legal framework governing privacy protection and limitation in DIPs in Kenya.

Chapter 3: The third chapter will discuss the measures taken by DIPs to protect privacy and abide by public interest and national security concerns.

Chapter 4: This chapter will discuss the fundamental elements and principles required when forming privacy limitation laws.

Chapter 5: This chapter will be the concluding chapter providing for a summary of the conclusions of the study and recommendations based on the study's findings.

CHAPTER 2

2.0. LEGAL FRAMEWORK

2.1 INTRODUCTION

This chapter seeks to review the legal framework governing DIPs in both the Kenyan and International Context. It aims to illustrate that the existing framework does not consider DIPs by itself and is otherwise scattered in different legislations according to some of the functions it conducts such as collection of data which is regulated by the Data Protection Act. The chapter analyses in depth the Constitutional and legal framework including also different regulations. The legal framework will focus on the Data Protection Act, Computer Misuse and Cybercrimes Act, Access to Information Act, international instruments, treaties, and conventions such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the African Union Convention on Cyber Security and Personal Data Protection. These legislations provide for different principles and elements related to practices that involve information of individuals aiming to protect individual privacy.

DIPs are widely used in any economy as they are businesses operating online that facilitate direct interaction between buyers and sellers for a fee without taking any ownership of the goods or services being sold.[70] They can include platforms facilitating short-term accommodation, ride hailing services and intermediate any electronic content without taking economic ownership over it such as phone application stores.[71] Due to the fact DIPs have an intermediary nature, Kenya has taken different legislative approaches to ensure privacy of the different parties is upheld and ensure their security.[72] DIPs generally do not have a duty to monitor but the data they collect can be used to assist government officials in addressing security concerns and public interest concerns such as when a person is murdered while staying in an Airbnb, just as in the cases reported and discussed in the chapter 1, the platform may provide any details they have on the Airbnb property on the day the crime happened to assist the police in finding the killer.

[70] IMF, OECD, UNCTAD and WTO, *Handbook on measuring digital trade*,28 July 2023, 92.
[71]IMF, OECD, UNCTAD and WTO, *Handbook on measuring digital trade*,28 July 2023, 92.
[72]The Kenya Institute for Public Policy Research and Analysis, 'Strengthening data protection in Kenya: Opportunities and the way forward' KIPPRA, 30 June 2024 -<https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/>- on 31st December 2024.

2.2. NATIONAL LEGISLATION

2.2.1 The 2010 Constitution of Kenya

Article 31 of the Constitution provides for the right to privacy. The right includes the right to not have the privacy of a person's communication infringed or information on their private affairs or family unnecessarily required or revealed.[73] Article 24 provides for limitation to specific rights by law as long as it is reasonably justifiable. For the limitation to be justifiable there are different factors it should consider,

> "(a) the nature of the right or fundamental freedom; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and (e) the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose."[74]

2.2.2. Data Protection Act

The data protection act was enacted by the Kenyan Parliament in 2019 to give effect to Article 31 (c) and (d) of the Constitution. Data Protection Act defines data,

> ""Data" means information which; (a) is processed by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with intention that it should be processed by means of such equipment; (c) is recorded as part of a relevant filing system; (d) where it does not fall under paragraphs (a), (b) or (c), forms part of an accessible record; or (e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d)."[75]

The purpose of the Data Protection Act is to regulate the processing of data in order to protect individuals' right to privacy.[76] The Data Protection Act provides for principles of data protection emphasizing the need of data controllers to ensure that personal data is processed in a manner in line with right to privacy of the data owner, it is accurate, adequate, relevant and limited to what is necessary to the purpose which it is processed for and many other principles.[77] Under the Act,

[73] Article 31, *Constitution of Kenya* (2010).
[74] Article 24, *Constitution of Kenya* (2010).
[75]Section 2, Data Protection Act (Act No. 24 of 2019).
[76]Section 3, Data Protection Act (Act No. 24 of 2019).
[77] Section 25, Data Protection Act (Act No. 24 of 2019).

collection of data has to be directly from the data subject but it also provides scenarios where the data can be collected indirectly.[78] The scenarios where data can be collected indirectly are:

> "(2) Despite subsection (1), personal data may be collected indirectly where— (a) the data is contained in a public record; (b) the data subject has deliberately made the data public; (c) the data subject has consented to the collection from another source; (d) the data subject has an incapacity, the guardian appointed has consented to the collection from another source; (e) the collection from another source would not prejudice the interests of the data subject; (f) collection of data from another source is necessary— (i) for the prevention, detection, investigation, prosecution and punishment of crime; (ii) for the enforcement of a law which imposes a pecuniary penalty; or (iii) for the protection of the interests of the data subject or another person."[79]

The Act provides that for processing of data to be lawful it should have been consented to by the data subject or if processing the data is necessary for compliance with any legal obligation which controller of the data is subject, to perform a task that is carried out in public interest or by a public authority, or for the exercise by any person in public interest.[80] The Data Protection Act also provides that data obtained should not be used for commercial purposes unless the data collector has sought and obtained consent from data subject or it is authorized by law and data subject is notified.[81] The Act provide that retaining of data should only be as long as required for the purpose it was collected and it gives circumstances where it can be retained longer. The Act states that:

> "(1) A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is— (a) required or authorised by law; (b) reasonably necessary for a lawful purpose; (c) authorised or consented by the data subject; or (d) for historical, statistical, journalistic literature and art or research purposes. (2) A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under subsection (1) in a manner as may be specified at the expiry of the retention period.".[82]

The Act also provides for exemptions from complying with the principles of data protection which are whether it is necessary for national security or public interest or if it is required to be disclosed

[78] Section 28, Data Protection Act (Act No. 24 of 2019).
[79] Section 28, Data Protection Act (Act No. 24 of 2019).
[80]Section 30, Data Protection Act (Act No. 24 of 2019).
[81]Section 37, Data Protection Act (Act No. 24 of 2019).
[82]Section 39, Data Protection Act (Act No. 24 of 2019).

by any written law or by an order of the court.[83] The Data protection Act also provides for responsibilities of data controllers which include DIPs as they control data of their customers. Their responsibilities include appointing a data protection officer who shall advise the data controller on data processing requirements under law and ensure that the Act is complied with by the data controller.[84] Data processors should also ensure the rights of their data subjects are upheld which includes the right to allow correction or deletion of false or misleading data, right to object processing of their data in part or whole, the right to be informed of the use of their data and the right to access their data.[85] DIPs and any other data controller are expected to notify the data subject that their data is being collected,[86] carry out a data protection impact test prior to processing of data to determine whether the processing poses high risks,[87] abide by the restrictions on cross-border transfers,[88] and notify the Office of the Data Protection Commissioner in case of a breach to privacy.[89] Data possessors are also required to register with the Data Commissioner under the Act.[90]

The Act is extensive in ensuring individual privacy and providing for privacy violations. It provides for the rights and duties of both the data subject and the data controllers keeping in mind the need to consider public interest and national security matters. A gap in the law is noted in the matter of DIPs as they involve different customers using the platforms, each requiring protection of their privacy. The gap is that the Act does not understand the complex nature of DIPs where the customers can be both data controllers and subjects and can be at risk if proper measures are not implemented to ensure both their privacy and security are protected. This is as the Act provides for the platforms as data controllers to adhere to their provisions, but the platforms involve giving information about service providers to customers and giving information of service providers to customers as an intermediary. The Act gives no obligation to the service providers and their customers through the platforms as they cannot be recognized as data controllers as they do not

[83] Section 51, Data Protection Act (Act No. 24 of 2019).
[84] Section 24, Data Protection Act (Act No. 24 of 2019).
[85] Section 26, Data Protection Act (Act No. 24 of 2019).
[86] Section 29, Data Protection Act (Act No. 24 of 2019).
[87] Section 31, Data Protection Act (Act No. 24 of 2019).
[88]Section 49, Data Protection Act (Act No. 24 of 2019).
[89] Section 43, Data Protection Act (Act No. 24 of 2019).
[90] Section 18, Data Protection Act (Act No. 24 of 2019).

process the data, but they still have access to others personal data. This may raise security and privacy concerns of any party involved.

2.2.3. Computer Misuse and Cybercrimes Act

The object of this act is to protect confidentiality and integrity of computer systems by preventing their unlawful use and facilitate punishment of cybercrimes while also protecting the right to privacy granted under the constitution.[91] Under the Act a service provider is not subjected to neither criminal nor civil liability for disclosure of data to the extent required by law and only assumes liability if the server has knowledge or aided and abetted use by any computer system managed by them in connection with any contravention in law.[92] The act allows for interception of data by a police officer if they have reasonable grounds to believe that specific electronic communications are important to investigate an offence as they may apply to the court for an order permitting them to access the information.[93] A police officer can also search and seize stored computer data if reasonably required for criminal investigations through issuance of a search warrant.[94]

The Act mainly addresses matters in relation to computer use. Though DIPs are not computers the Act is relevant as it provides for liability of service providers who are the main consumers of the platforms and allows for interception of data by the police for investigations of criminal matters. This act can be relevant to DIPs as they involve service providers and electronic content but can also fail to be relevant as in interpreting the Act its scope is limited to the use of computer programs and software.

2.2.4. Access to Information Act

The Act provides for the right to access information,[95] and its purpose is to provide a framework to facilitate access of information of both private and public bodies.[96] The Act also provides for limitations to the right to access information in that if the disclosure of the information may

[91] Section 3, Computer Misuse and Cybercrimes Act (Act No 58 of 2018)
[92]Section 56, Computer Misuse and Cybercrimes Act (Act No 58 of 2018)
[93] Section 53, Computer Misuse and Cybercrimes Act (Act No 58 of 2018)
[94] Section 48, Computer Misuse and Cybercrimes Act (Act No 58 of 2018)
[95] Section 4, Access to Information Act (Act No. 107 of 2016).
[96] Section 3, Access to Information Act (Act No. 107 of 2016).

undermine national security, endanger safety or health of a person or involve unwarranted invasion of an individual's privacy.[97] The Act states that:

> "(1) Pursuant to Article 24 of the Constitution, the right of access to information under Article 35 of the Constitution shall be limited in respect of information whose disclosure is likely to— (a) undermine the national security of Kenya; (b) impede the due process of law; (c) endanger the safety, health or life of any person; (d) involve the unwarranted invasion of the privacy of an individual, other than the applicant or the person on whose behalf an application has, with proper authority, been made."

The Act provides for access of information which is a limitation of the right to privacy. This is relevant to intermediary platforms as being managed by private bodies some information needed may not be accessible. When security and public interest concerns are raised in relation to these platforms the Act allows and facilitates for access of necessary information to solve such concerns.

2.3. INTERNATIONAL LAW

The Constitution recognizes that the general rules of International Law and any treaty or convention ratified by Kenya forms part of the law of Kenya.[98] These are the instruments, treaties and conventions Kenya has ratified or signed that are relevant to this study.

2.3.1. International Instruments

2.3.1.1. Universal Declaration of Human Rights

Article 12 of the UDHR provides for the right to privacy, stating that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[99]

This provision is emulated under Article 31 of the constitution which as discussed earlier provides for the right to privacy.

[97] Section 6, Access to Information Act (Act No. 107 of 2016).
[98] Article 2, *Constitution of Kenya* (2010).
[99] Article 12, *Universal Declaration of Human Rights,* 10 December 1948, General Assembly Resolution 217A.

2.3.2. International Treaties and Conventions

2.3.2.1. International Covenant on Civil and Political Rights

Article 17 of the ICCPR provides for the right to protection against actions or interferences with one's privacy. This is adopted in Kenya through Article 31 of the Constitution just as the UDHR Article. The Treaty states that:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks."[100]

The data protection act enforces this provision as it gives protection to data subjects to any interference or attack to their privacy.

2.3.2.2. African Union Convention on Cyber Security and Personal Data Protection

Chapter II of the convention deals with personal data protection. Its objective is to commit states into developing legal frameworks that protect data and punish any violation of privacy.[101] The convention provides for principles governing processing of personal data which are the principle of consent and legitimacy, principle of lawfulness and fairness, principle of accuracy, principle of transparency, principle of confidentiality and security, and the principle of purpose relevance and storage.[102] It also provides for specific provisions of sensitive data which involves prohibiting data collection and processing of states that reveal specific details of data subject.[103] The convention states that:

> "State Parties shall undertake to prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject."[104]

The convention also notes circumstances where the prohibition does not apply which includes when a judicial proceeding or criminal investigation has been instituted, when processing is

[100] Article 17, *International Covenant on Civil and Political Rights*, 16 December 1966, General Assembly resolution 2200A (XXI).
[101] Article 8, *African Union Convention on Cyber Security and Personal Data Protection,* 27 June 2014, Treaty Series No. 0048.
[102] Article 13, *African Union Convention on Cyber Security and Personal Data Protection*.
[103]Article 14, *African Union Convention on Cyber Security and Personal Data Protection.*
[104] Article 14, *African Union Convention on Cyber Security and Personal Data Protection*.

necessary in public interest or for compliance with a legal obligation.[105] The convention has different principles that have been incorporated in the Data protection Act. Even though Kenya has not ratified it, the convention is beneficial to the study as it provides different principles on the law regarding privacy which is to be discussed in the next chapter.

2.4. REGULATION FRAMEWORK

2.4.1. National Transport and Safety Authority (Transport Network Companies, Owners, Drivers, and Passengers) Regulations

These regulations explain one version of the DIPs. It describes a Transport network platform as a digital platform or any other similar system that is offered or operated by a transport network company and used by persons for the transportation of passengers for compensation by a transport network driver.[106] These regulations were formed to regulate transport networks services and drivers through the platforms.

The regulation provides for conditions for one to offer transport network services.[107] A transport network company is required to maintain and retain records for 3 years.[108] The records they are meant to maintain and retain are:

> "(1) A transport network company shall maintain the following data for each transport network service offered through a network platform for a period of three years— (a) the motor vehicle registration number used to offer the transport network service; (b) the name, driving license number and Public Service Vehicle registration number of the transport network driver who provided the transport network service; (c) the name and relevant identification details of the transport network passenger who was provided with the transport network service; (d) the date, time and location of pick-up and drop-off relating to the transport network service; (e) the method

[105] Article, *African Union Convention on Cyber Security and Personal Data Protection*.
[106] Section 2, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012)
[107] Section 3, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012).
[108] Section 17, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012).

of payment made by the transport network passenger for the transport network service; and (f) the details relating to the pricing of transport network service."[109]

The regulations confer duties to transport network drivers,[110] and passengers to ensure their safety[111] It also provides for operations of transport network companies requiring them to provide information on the transport drivers name, photo, motor vehicle make and model and estimated fare to the passenger and also put a system to verify identity of passengers when they enroll to the platform identity.[112] Platform companies are also required to report and deactivate drivers that Rise public safety concerns.[113] They also have different duties such as providing a panic button with appropriate response on the digital platform which is to be manned at all times.[114]

These regulations limit privacy rights due to different requirements of disclosing of information to ensure public safety and security concerns are addressed. Such regulations are necessary in balancing of privacy rights with public interest and national security though no other regulation governing the other different DIPs have been enforced.

2.5. CONCLUSION

The legal framework does not provide for extensive provisions on matters relating to DIPs which require strict regulations to ensure privacy rights are upheld without undermining public interest and national security concerns. The Kenyan legal framework provides for the right to privacy and the various limitations that affect it, which is also supplemented with International Law. It however does not provide for any general monitoring function of the platforms in order to impose these laws and maintain public interest and security concerns.

[109] Section 17, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012).
[110] Section 21, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012).
[111] Section 22, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012).
[112] Section 14, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012).
[113] Section 18, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012).
[114] Section 11, National Transport and Safety Authority (Transport Network Companies, Owners, Drivers and Passengers) Regulations (Act No 33 of 2012).

CHAPTER 3

3.0. MEASURES TAKEN BY DIGITAL INTERMEDIARY PLATFORMS IN PROTECTING THEIR CONSUMERS PRIVACY AND ABIDING BY PUBLIC INTEREST AND NATIONAL SECURITY CONCERNS

3.1. INTRODUCTION

DIPs have developed internal policies and mechanisms they use to ensure the consumers' data is protected.[115] This chapter aims to examine how the existing DIPs have adhered to the different laws that relate to some of the functions they perform and determine the risks and benefits of the measures they have taken. It will also dwell on the risks and benefits that are posed by private or government actions that undermine privacy such as surveillance.

3.2. MEASURES TAKEN BY DIGITAL INTERMEDIARY PLATFORMS

3.2.1. Measures taken by digital intermediary platforms in protecting their consumers' privacy

DIPs have adhered to the provisions of the Data Protection Act by having systems and technologies that secure data storage and transmission[116] They have also provided privacy policies to all their customers to read and understand before agreeing to use the platforms.[117] The policies are clear and detailed on how the data is collected, shared and used by platforms.[118] They also have consent mechanisms for the users of the platform where one may opt in or out of different features or updates giving them control over their data.[119] The platforms are also transparent in their data practices as they inform their users about any updates on their terms and conditions or any new

---

[115] Office of the Australian Information Commissioner, 'What is a privacy policy?', Office of the Australian Information Commissioner, 31 December 2024-<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-a-privacy-policy >- on 31 December 2024

[116] Uber Developers, 'SFTP Data Automation', Uber, 31 December 2024,-<https://developer.uber.com/docs/health/data-automation/introduction>- on 31 December 2024.

[117] Bolt, 'Privacy notice for passengers and riders', Bolt, Bolt, 31 December 2024-< https://bolt.eu/en-sa/privacy/privacy-for-riders/>- on 31st December 2024.

[118] Office of the Australian Information Commissioner, 'What is a privacy policy?', Office of the Australian Information Commissioner, 31 December 2024-<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-a-privacy-policy >- on 31 December 2024

[119]Usercentrics, 'How important is consent management under the Digital Markets Act (DMA)?', Usercentrics, 30 October 2023-<https://usercentrics.com/knowledge-hub/consent-management-digital-markets-act-dma/>- on 31 December 2024

practice that may affect their user's data.[120] DIPs collect data on their customers which may create a sort of power imbalance between the platforms and their customers.[121] Though the laws provide for protection of the data subjects but the power imbalance cannot be ignored as it is the cause of greater dangers such as discrimination and undue persuasion.[122] Though, due to their intermediary nature recognizing such dangers may be hard. This is because determining when and how a service provider or customer has been discriminated or if they have been subjected to undue persuasion is different in each case.

The danger of power disparities is mainly on information gathered by platforms as the platforms have knowledge on how data is used, processed and disclosed, while the users of the platform can only view or access the information available to them.[123] This is especially since they are few alternatives to the platforms and the consumers preference for the ease it provides creates a greater power imbalance on the parties involved.[124] The platforms collect some information on its users in order to conduct their functions and adhere to the Data Protection Act to the extent to which the data collected is useful to the function it is required for. They explain to their customers through notices and privacy policies on any update or change in terms and conditions of using the platform. Though with the development of the technology, different updates are made by increasing the complexity of data processing, putting the user at a disadvantage.

Due to the information gathered by the platform, in exercising its management purposes it may use the information provided to provide certain benefits to its users. For example, a platform user let's say in the case of Uber, a passenger, as it is a ride hailing platform, may be provided for certain discounts allowing them to pay less than the required price. This benefit by the platform does not affect the driver who is the service provider as the discounts are covered by the platform

[120]Airbnb, 'Airbnb law enforcement and transparency reports', Airbnb Newsroom, 31 December 2024 - <https://news.airbnb.com/transparency/>- on 31 December 2024.
[121] Richards N, *'The Dangers of Surveillance,'* 1953.
[122] Richards N, *'The Dangers of Surveillance,'* 1953
[123] Office of the Australian Information Commissioner, *Global scan of privacy regulation of digital platforms*, June 2020, 11.
[124] Office of the Australian Information Commissioner, *Global scan of privacy regulation of digital platforms* June 2020, 11.

and do not affect the earnings of the driver.[125] Regardless of this some drivers still subject their passengers to incidents where they harass them by requesting more money even though the discount does not affect their earnings.[126] Some platforms users have claimed to be assaulted by their drivers who lock them inside the cars for failing to pay an additional price they request on top of the fare provided by the platforms.[127] Here a benefit to the passenger or passengers whose data is processed in a certain way to accord such benefits may lead to them being subjected to insecurity concerns.

DIPs normally do not collect much data on the users hence cannot effectively perform surveillance or monitoring functions. They adhere to the Data Protection Act in relation to the few data they collect but an obligation should be imposed on them to surveil the users of the platform as necessary to help prevent crimes that are committed through the use of the platform but the surveillance practice must be proportional to the reason it is conducted.

3.2.2. Measures taken by digital intermediary platforms in abiding by public interests and national security concerns.

DIPs have taken measures to ensure they act in public interest and do not lead to national security concerns. DIPs comply with the authorities by ensuring that when requested for data by government officials, they comply with the provisions and procedures of the laws.[129] They also share information necessary to address security threats with the government.[130] Some DIPs have danger response protocols, for example Uber has a panic button for its users when faced with

[125] Otieno B, ' Uber, Bolt and Little drivers demand commission cut', Business Daily, 27 October 2022 -<https://www.businessdailyafrica.com/bd/corporate/companies/uber-bolt-and-little-drivers-demand-commission-cut-4000002>- on 4 March 2025.
[126] Wambui J, 'Drivers blame falling earnings for illegal fare hikes on ride-hailing apps' Citizen Digital, 5 August 2024 -<https://www.citizen.digital/business/drivers-blame-falling-earnings-for-illegal-fare-hikes-on-ride-hailing-apps-n347213>- on 4 March 2025.
[127]Wambui J, 'Drivers blame falling earnings for illegal fare hikes on ride-hailing apps' Citizen Digital, 5 August 2024 -<https://www.citizen.digital/business/drivers-blame-falling-earnings-for-illegal-fare-hikes-on-ride-hailing-apps-n347213>- on 4 March 2025.
[129]Uber, 'Law enforcement requests', Uber, 30 December 2024 -< https://www.uber.com/us/en/about/reports/transparency/law-enforcement/ >- on 30 December 2024.
[130] Airbnb, 'Airbnb launches new law enforcement portal', Airbnb Newsroom, 22 September 2019-<https://news.airbnb.com/airbnb-launches-new-law-enforcement-portal/>- on 30 December 2024.

danger which when used automatically sends information on the location of the vehicle, the vehicle model and make and the license plate to the nearest emergency service in case of an accident.[131] DIPs have enforced strict rules internally on who can use their platform to ensure that the users have represented themselves authentically and without fraud.[132] They conduct identity verification and allow for reviews and ratings to be conducted in the platform to enable users to make an informed choice when interacting with their customers or the service providers.[133]

Some DIPs have created law enforcement portals in their platforms where government agencies or officials may submit valid legal requests to the platform to access information collected and processed by the platform.[134] They have created such portals in order to assist the government in keeping society safe while also releasing transparency reports on the law enforcement activities to inform the users on information collected by the government.[135] This is a benefit to the platform as it attracts more customers to the platform due to their accountability in ensuring security and transparency in any action relating to their data.

A major question arises when implementing these measures by the platform which is what is the line in which if crossed leads to a national security or public interest concern? In the case of *Aukot & two others v National Security Council & 5 others*[136] the court described National security as protection against internal or external threats to Kenya's National Interests. The court stated that:

> The National Police Service Act was enacted to give effect to articles 238, 239 243, 244 and 247 of the Constitution. Article 238 is on national security, that is, protection against internal and external threats to Kenya's territorial integrity, sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests.

[131] Uber, 'The emergency button- where to find it, how to use it' ,Uber Blog, 14 April,-<https://www.uber.com/en-PL/blog/przycisk-bezpieczenstwa-gdzie-go-znalezc-i-jak-go-uzyc/>- on 30 December 2024.
[132] Airbnb, 'A statement from Airbnb on Kenya', Airbnb Newsroom, 15 January 2024-< https://news.airbnb.com/a-statement-from-airbnb-on-kenya/ >- on 30 December 2024.
[133] Airbnb, 'A statement from Airbnb on Kenya', Airbnb Newsroom, 15 January 2024-< https://news.airbnb.com/a-statement-from-airbnb-on-kenya/ >- on 30 December 2024.
[134] Airbnb, 'Airbnb launches new law enforcement portal', Airbnb Newsroom, 22 September 2019-<https://news.airbnb.com/airbnb-launches-new-law-enforcement-portal/>- on 30 December 2024.
[135]Airbnb, 'Airbnb launches new law enforcement portal', Airbnb Newsroom, 22 September 2019 -<https://news.airbnb.com/airbnb-launches-new-law-enforcement-portal/>- on 30 December 2024.
[136] (2024) eKLR

It can be said through this case that any action aiming to protect the country's interest from any threat amounts to an action towards protecting national security.

In describing public interest, the case *of Republic v Diana Suleiman Said & another*[138] explains it to be the rights and interests of others or society as it states that:

> When national security and public safety are threatened the very existence of the open and democratic and civilised society is also jeopardized. It must then become a matter of proper balance between the individual rights and the rights of the society so that the individual is entitled to enjoy the greatest extent of his rights consistent with the rights and interests of others or the public interest in the particular matter.

DIPs hence as required in the Data protection Act should disclose information to the relevant authority in case of any threat to national security or public interest.[140] Other data processors are held liable in matters in which they allow for threats to national security and public interest concerns but due to their intermediary nature questions arise on its liability as they are generally not liable for actions of their users.[141] The Act provides for a duty to inform the relevant authority about illegal activities occurring through the platform but there is no duty to monitor or to conduct surveillance.[142] As they rarely surveil or monitor the users of the platforms they have less means of identifying security threats as they can only act with the minimal data they collect as information on such crimes is only available to them if a complaint is lodge which if not it will be hard for government agencies to prevent the crime or punish the wrong doer. The law enforcement platforms are a way to try and prevent this risk by the platforms.

3.3. CONCLUSION

DIPs have enacted different measures to protect the privacy of their user's information and have enacted different policies and portals to help assist government agencies in promoting national security and public interest. As discussed in this chapter DIPs have enacted measures such as privacy polies, panic buttons, law enforcement portals, law enforcement transparency reports,

[138] [2014] eKLR
[140] Section 28, Data Protection Act (Act No. 24 of 2019).
[141] European Parliamentary Research Service, 'Liability of Online Platforms', 2021, 29.
[142] OECD, 'The Role of Intermediaries in Advancing Public Policy Objectives', OECD Publishing, 2011, 13

notifications on updates and opt-in or opt-out features. These measures are an attempt by the platforms to comply with the laws and regulations of the country. Though the measures are sufficient in maintaining privacy of the users, they fail to help prevent any criminal activities that may occur through their platform and there is a need for new obligations to the platforms that ensure they continuously monitor the usage of the platform to discourage any crime from occurring through the facilitation of the platform without their knowledge.

CHAPTER 4

4.0. PRINCIPLES AND ESSENTIAL ELEMENTS OF LAW NEEDED TO ENSURE A BALANCE OF PRIVACY RIGHTS, PUBLIC INTEREST, AND NATIONAL SECURITY

4.1. INTRODUCTION

As discussed in chapter three, there is a need for a legal and regulatory framework that imposes a duty on intermediary digital platforms to monitor the usage of their platform by the users in order to prevent any crime from occurring through the use of the platform. This can be done through requiring general monitoring or surveillance obligations by the platforms. For such laws to be valid certain principles and elements need to be present in order to ensure a balance of privacy rights to public interest and national security concerns in that one does not trump over the other.

4.2. PRINCIPLES AND ESSENTIAL ELEMENTS OF SURVEILLANCE LAWS

Surveillance practices as discussed previously involve focused, systematic and routine attention to personal details for different purposes.[143] There are different laws in Kenya that regulate surveillance but none of them handle matters on digital intermediary platforms hence the need for a specific law imposing a duty to monitor or surveil by DIPs that entails certain principles and elements for surveillance. A major challenge when handling security and public interest concerns is whether DIPs are liable for security concerns that arise through the use of the platforms as they generally have no duty to monitor or surveil. This study recommends that a duty of monitoring and surveillance obligations should be imposed on the DIPs in order to balance individual privacy rights with public interest and national security concerns in light with the recent security risks surrounding them.

[143] Richards N, 'The Dangers of Surveillance', 1937.

There are certain elements and principles necessary in Law to achieve this balance, which are:

a) Recognition that surveillance transcends the public and private divide

Neil Richards proposes a set of four principles necessary to guide formation of surveillance laws which the study agrees are fundamental in forming privacy limiting laws.[144] He states that we should recognize that surveillance transcends the public and private divide, secret surveillance is illegitimate, total surveillance is illegitimate, and that surveillance is harmful.[145] The first principle Richards proposes is that in forming laws touching on surveillance it is important to establish that surveillance can be both private surveillance and public surveillance. Public surveillance is mainly in the form of government surveillance and many laws try to limit the power imbalance that may be caused but one should also consider with an increase in development of technology private surveillance should also be regulated.[146] DIPs should be regulated requiring them to do general monitoring while adhering to the data protection constraints required by law.

b) Secret surveillance is illegitimate.

Richards also proposes that the laws regulating DIPs should also recognise the principles that secret surveillance and total surveillance are illegitimate.[147] If surveillance is secret its legitimacy in court in how it was obtained cannot be admissible hence the need to establish the principle to prevent this problem.[148] One may think secretly surveilling the actions of their driver after requesting a ride through a platform may help them when a crime committed against them is brought to court, but allowing such secrecy leads to greater dangers than benefits to one's privacy and others making it illegitimate. This is as the legal processes are not followed hence cannot be considered by the court as they need to ensure other rights and freedoms are not violated therefore DIPs need to be regulated to ensure they are transparent with their surveillance practices.

In the case of *John Muriithi & 8 others vs. Registered Trustees of Sisters of Mercy (Kenya)t/a "The Mater Misericordiae Hospital & another*[149] the court held that illegally obtained evidence is inadmissible in all criminal cases but can be admissible to civil cases if it is relevant to the case

[144] Richards N, 'The Dangers of Surveillance', 1935.
[145]Richards N, 'The Dangers of Surveillance', 1958.
[146] Richards N, 'The Dangers of Surveillance', 1958.
[147] Richards N, 'The Dangers of Surveillance', 1935.
[148] Richards N, 'The Dangers of Surveillance', 1960.
[149] [2018] eKLR

and its admission does not affect fairness. The court stated that evidence obtained in a way that violates the fundamental rights of individuals renders the trial process unfair and can be detrimental to justice.[150]

Neil Richards posits that to prevent the problems associated with secret surveillance the principles of transparency, accountability to the public and confidentiality should be upheld.[151] The Malabo Convention, which is another name for The African Union Convention On Cyber Security And Personal Data Protection, also provides for the principles of transparency and confidentiality of personal data processing.[152] The convention requires mandatory disclosure of information by the data controller on personal data and for data to be processed confidentially and protected.[153] The principles set out by the Malabo convention highlight the need to ensure that surveillance practices conducted are not secret but known to the users of the platform.

c) Total surveillance is illegitimate.

The third principle Richards proposes is that total surveillance is also illegitimate.[154] This is as if one is monitored for every single activity, having every aspect of their personal life being collected as information may lead to greater risks and no benefit at all. Total surveillance may lead to chilling effects on society as it will force many to censor their speech or conduct as they have the fear that someone is watching them and will prevent people from being innovative hence hindering development.[155]

d) Surveillance is harmful.

The last principle to be observed as proposed by Neil Richards is that surveillance is harmful as it creates risks and dangers to one's privacy and creates a power imbalance between the one being monitored and the one monitoring.[156] As illustrated by the last two principles discussed, surveillance practices can be harmful to one's privacy hence a need for them to be strictly

[150] John Muriithi & 8 others vs. Registered Trustees of Sisters of Mercy (Kenya)t/a "The Mater Misericordiae Hospital & another [2018] eKLR.
[151] Richards N, 'The Dangers of Surveillance', 1959.
[152]Article 13, *African Union Convention on Cyber Security and Personal Data Protection*
[153] Article 13, *African Union Convention on Cyber Security and Personal Data Protection*
[154] Richards N, 'The Dangers of Surveillance', 1961.
[155] Froomkin M, 'The Death of Privacy?', 1470.
[156] Richards N, 'The Dangers of Surveillance', 1962.

regulated. Due to this, surveillance practices should be conducted in a manner that ensures the information collected is managed with great care and is protected.[157]

e) Domestic law should allow for surveillance.

Essential elements of law are emphasized by Steven Feldstein in his work where he emphasizes that the law should consists of certain principles to be considered lawful or unlawful.[158] The regulations on DIPs requirements for general monitoring should take into account whether domestic law allows for surveillance, if the surveillance action meets the international standards of necessity and proportionality and whether the interests justifying the action are legitimate.[159] In the case of DIPs if the law allows and requires for the platforms to conduct surveillance, it will be considered lawful. This is as with the current reports of crimes that have occurred through usage of platforms are being investigated many have great interest in ensuring that the platforms have measures to ensure safety of its users regardless of it being an intermediary with no control over the users conduct as it only acts as facilitative platform for people to provide and access services.[160]

f) Surveillance action must meet international standards and the interests justifying the action should be legitimate.

For surveillance laws to be lawful they must meet the international standards of necessity and proportionality. The laws though must be proportional to the risk they are trying to prevent. In the case for DIPs is the safety of the users from threats by other users which is a legitimate reason and is necessary to uphold public interest and national security. However, the surveillance practice recommended should be proportional to the reason its needed for, while ensuring that it is not secret or total surveillance and that it will not turn out to be harmful. Currently in the legal framework there are different laws that illustrate the need for privacy limiting practices are only conducted if it is necessary and proportional. The Data Protection Act provides for principles of

[157] Richards N, 'The Dangers of Surveillance', 1962.
[158] Feldstein S, Carnegie Endowment for International Peace, Distinguishing Between Legitimate and Unlawful Surveillance, 2019, 11.
[159] Feldstein S, Carnegie Endowment for International Peace, Distinguishing Between Legitimate and Unlawful Surveillance, 2019, 12.
[160] Mumbi L,'Bolt, Uber Team up with NTSA to Launch joint system to ban errant drivers on all platforms' The Eatstleigh Voice, 10 October 2024 -<https://eastleighvoice.co.ke/headlines/81479/bolt-uber-team-up-with-ntsa-to-launch-joint-system-to-ban-errant-drivers-on-all-platforms >- on 31 December 2024.

data protection that should be maintained. The Act requires data collection to be lawful, fair, transparent, accurate, valid, and necessary among others,[161] which as discussed through the various mentioned authors are key principles for surveillance laws or privacy limiting laws.

The Act possesses this strength as it considers the necessary elements for privacy, limiting laws, but it does not put any obligation on data controllers to request any type of information which may be necessary in promoting public interest and national security concerns. Under the Computer Misuse and Cybercrimes Act, though it mainly deals with computers and its software and programs, it introduces the concept of liability providing that intermediaries generally cannot be held to have criminal or civil liability unless they had knowledge on the act being investigated.[162] As the DIPs generally have no monitoring obligation, they do not have knowledge of the activities they are acting as intermediaries for and hence cannot be liable or be of help when promoting public interest or national security. This is a legitimate reason for law makers to consider and ensure the obligation exists in order to help address the national security and public interest concerns.

4.3. CONCLUSION.

Privacy limiting laws or surveillance laws should have specific principles or elements that guide it as discussed in this chapter. The principles as mentioned in this chapter are that we should consider both public and private surveillance, secret surveillance and total surveillance are illegitimate, surveillance can be harmful and that for the surveillance to be lawful the law has to provide for it, the surveillance should be necessary and proportional, and the interests justifying it is legitimate. A law should be formed with regard to DIPs to allow them to conduct surveillance that can assist in managing the platforms to prevent any crime from occurring though it.

[161] Section 25, Data Protection Act (Act No. 24 of 2019).
[162] Section 56, Computer Misuse and Cybercrimes Act (Act No 58 of 2018)

CHAPTER 5

5.0. CONCLUSION AND RECOMMENDATIONS.

5.1. CONCLUSION

Privacy as seen in the above chapters is a fundamental human right subject to limitations by law that are reasonably justifiable. Digital intermediary platforms have recently been used to indirectly promote crime leading to the need to have laws that should be formed to regulate them and prevent such crimes. Chapter One of this study introduced the topic of privacy and digital intermediary platforms highlighting the different platforms and crimes reported to have occurred through the use of the platforms. It discussed the importance of having a law that imposes a duty to the platforms to conduct general monitoring activities as the legal gap present in laws relating to digital intermediary platforms.

Chapter two of this study has established the legal framework relating to digital intermediary platforms. It concluded that the existing legal framework does not provide for any obligation to digital intermediary platforms to monitor or surveil usage of their apps which can be helpful to both the authorities and the platforms to maintain public interest and national security concerns. The legal framework provides for protection of personal data giving scenarios where the data can be used to assist investigations of crime and when the right to privacy can be limited to promote interest and national security but it does not mention digital intermediary platforms.

Chapter three of the study discusses on the measures the digital platforms have taken in protecting their user's privacy and the measures they have taken to help address national security and public interest concerns surrounding their usage by others. This chapter illustrated that the platforms have enforced data protection mechanisms and legal enforcement mechanisms such as their opt in or out options and their transparency reports as a way to help address the issues that surround their usage but due to the fact that they do not have an obligation to surveil it is harder for them to identify crimes occurring through the platforms to report to the authorities.

Lastly, Chapter four discusses that if a legal obligation to generally monitor or surveil is imposed on the platforms it should be done so through a law. The law entailing these obligations should

encompass different elements and principles in order to be lawful and not be harmful as if not it will defeat the purpose of the law. The chapter highlighted the principles and elements of law needed in order to achieve a balance of the privacy rights concerned, matters of public interest and national security concerns in relation to the obligation to surveil by digital trading platforms.

5.2. RECOMMENDATIONS

This study as discussed above observes that as digital intermediary platforms do not have an obligation to conduct general monitoring. The study recommends that a law should be formed to impose such an obligation so as to assist the platform and authorities in detecting crimes occurring through the use of the platforms and reporting them in order to address the public interest and national security concerns surrounding the use of the platform. The study recommends such a law as it will help them in addressing public interest and national security concerns surrounding their ability to detect crimes or help prevent crimes that can be committed through use of the platform. The obligation to monitor usage of the platform will assist them in collecting information necessary to remove and report users that commit crimes and hence do not respect national security or public interest which is beneficial to the platforms as it will increase public confidence in the platform.

The study recommends that the laws should adhere and implement to the principles and elements discussed in chapter four of this study which are to consider both public and private surveillance, ensure that there is no secret surveillance or total surveillance as they are illegitimate, consider the harmfulness that surveillance can cause, and that surveillance is to be lawful. Surveillance can only be lawful if the law has to provide for it, surveillance is necessary and proportional, and the interests justifying it are legitimate. It should also ensure that data collected through surveillance are accurate, fair, transparent, confidential and the platforms are accountable.

The study recommends that the law should evolve with societal needs, which is greatly needed in this digital age where many services are accessed through the platforms. As they have no obligation to surveil which is a recommended solution, the law should hence evolve and impose an obligation to surveil in accordance with the elements and principles of law in order to find a balance between privacy, public interest and national security.

BIBLIOGRAPHY

1. Froomkin M, *'The Death of Privacy?* 52 Stanford Law Review 5, 2000.
2. Richards N, 'The Dangers of Surveillance', 126 Harvard Law Review 7, 2013
3. Solove D, 'I've got nothing to hide and other misunderstandings of privacy,' GWU Law School Public Law Research Paper Number 289, -<https://ssrn.com/abstract=998565>-. 2007.
4. Feldstein S, 'Distinguishing Between Legitimate and Unlawful Surveillance', Carnegie Endowment for International Peace, 2019.
5. Badurdeen F, 'Digital Surveillance and Privacy Concerns in the Counter Terrorism Discourse in Kenya: Policy Implications', SSRN, <https://ssrn.com/abstract=3058666>-, 2017.
6. Gilmore G, 'Legal realism: Its cause and cure', 70(7) The Yale Law Journal, 1961.
7. Alexander G, 'Comparing the two Legal realisms: American and Scandinavian' 50(1) *The American Journal of Comparative Law*,2002.
8. Jones H, 'Law and morality in the perspective of legal realism', Columbia Law Review, 1961.
9. Hart A., 'Scandinavian Realism', The Cambridge Law Journal, 1959.
10. Calo R., 'Privacy Law's Indeterminacy', Theoretical Inquiries L, 2019.
11. Holtermann J, Naturalizing Alf Ross's Legal Realism: A Philosophical Reconstruction' 24 *Revus - Journal for Constitutional Theory and Philosophy of Law*, 2014.
12. Ramisetty R (2024), 'A critical analysis on American legal realism and Scandinavian legal realism: Similarities and differences' 2(2) International Journal of Legal Studies and Social Sciences, 2024.
13. European Institute of Gender Equality, *Femicide: a classification system*, 2021.
14. ECNL Learning Centre, 'Technology and Artificial Intelligence: Surveillance technology' ECNL Learning Centre, 10 December 2024-< https://learningcenter.ecnl.org/learning-package/surveillance-technology >-
15. Owano J, 'Data Privacy And Protection In Kenya: The New Corporate Risk', 8 October 2024 -< https://www.businessdailyafrica.com/bd/opinion-analysis/columnists/data-privacy-and-protection-in-kenya-the-new-corporate-risk-4788892 >-

16. Kiage N and Ngigi E,' Police open probe after Nairobi socialite Starlet Wahu is stabbed to death in South B Airbnb' Daily Nation, 7 January 2024 -<https://nation.africa/kenya/counties/nairobi/puzzle-hiv-test-kit-dead-socialite-starlet-wahu-south-b-airbnb--4483656>-
17. Kupemba D, 'Kenya Femicide: A woman's murder exposes the country's toxic online misogyny', on 15 January 2024, BBC-<https://www.bbc.com/news/world-africa-67987347>-
18. Airbnb, 'A statement fromAirbnb on Kenya' Airbnb Newsroom, 15 January 2024-<https://news.airbnb.com/a-statement-from-airbnb-on-kenya/>-.
19. Folger J, 'How Airbnb works- for hosts, guests and the company itself', Investopedia, 13 December 2024 -<https://www.investopedia.com/articles/personal-finance/032814/pros-and-cons-using-airbnb.asp>
20. https://generisonline.com/understanding-data-protection-and-privacy-laws-in-kenya/>-
21. -<https://nairobiassembly.go.ke/motion/regulation-of-airbnb-services-within-the-county/>
22. Oluwatosin R, Nkechi E, Ehimuan B, Anyanwu A, Olorunsogo T and Temitayo O, 'Privacy Law Challenges In The Digital Age: A Global Review Of Legislation And Enforcement' 6(1) *International Journal of Applied Research in Social Sciences,* 2024.
23. IMF, OECD, UNCTAD and WTO, *Handbook on measuring digital trade,*28 July 2023
24. The Kenya Institute for Public Policy Research and Analysis, 'Strengthening data protection in Kenya: Opportunities and the way forward' KIPPRA, 30 June 2024 -<https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/>-
25. Office of the Australian Information Commissioner, 'What is a privacy policy?', Office of the Australian Information Commissioner, 31 December 2024-<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-a-privacy-policy >-
26. Uber Developers, 'SFTP Data Automation', Uber, 31 December 2024,-<https://developer.uber.com/docs/health/data-automation/introduction>-
27. Bolt, 'Privacy notice for passengers and riders', Bolt, Bolt, 31 December 2024-< https://bolt.eu/en-sa/privacy/privacy-for-riders/>-

28. Usercentrics, 'How important is consent management under the Digital Markets Act (DMA)?', Usercentrics, 30 October 2023-<https://usercentrics.com/knowledge-hub/consent-management-digital-markets-act-dma/>-
29. Airbnb, 'Airbnb law enforcement and transparency reports', Airbnb Newsroom, 31 December 2024 -<https://news.airbnb.com/transparency/>-
30. Office of the Australian Information Commissioner, *Global scan of privacy regulation of digital platforms*, June 2020.
31. Uber, 'Uber rides promotions: Terms and conditions' Uber Newsroom, 9 November 2021-<.https://www.uber.com/en-GB/newsroom/promotion-terms-and-conditions/>-
32. Uber, 'Law enforcement requests', Uber, 30 December 2024 -< https://www.uber.com/us/en/about/reports/transparency/law-enforcement/ >-
33. Airbnb, 'Airbnb launches new law enforcement portal', Airbnb Newsroom, 22 September 2019-<https://news.airbnb.com/airbnb-launches-new-law-enforcement-portal/>-.
34. Uber, 'The emergency button- where to find it, how to use it' ,Uber Blog, 14 April,-<https://www.uber.com/en-PL/blog/przycisk-bezpieczenstwa-gdzie-go-znalezc-i-jak-go-uzyc/>-
35. Airbnb, 'A statement from Airbnb on Kenya', Airbnb Newsroom, 15 January 2024-< https://news.airbnb.com/a-statement-from-airbnb-on-kenya/ >-
36. OECD, 'The Role of Intermediaries in Advancing Public Policy Objectives', OECD Publishing, 2011.
37. Mumbi L,'Bolt, Uber Team up with NTSA to Launch joint system to ban errant drivers on all platforms' The Eatstleigh Voice, 10 October 2024 -<https://eastleighvoice.co.ke/headlines/81479/bolt-uber-team-up-with-ntsa-to-launch-joint-system-to-ban-errant-drivers-on-all-platforms >-