UNIVERSITY *of* LUSAKA

Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

THE IMPACT OF TECHNOLOGY ON THE LAW: EXAMINING DIGITAL PRIVACY AND ELECTRONIC EVIDENCE.

By:

CHILUFYA CHANDA

LLB1611082

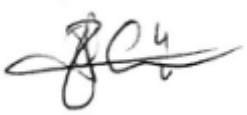
An obligatory essay submitted to the University of Lusaka in partial fulfillment of the requirements for the award of the degree of Bachelor of Laws (LLB).

2025

DECLARATION

I, **CHIUFYA CHANDA**, do declare that this dissertation titled **THE IMPACT OF TECHNOLOGY ON THE LAW: EXAMINING DIGITAL PRIVACY AND ELECTRONIC EVIDENCE.** Which is hereby submitted to the School of Law at the University of Lusaka as part of the requirements for the award of the Bachelor of Laws (LLB) degree, is my original work and has not previously been submitted for the award of a degree at this or any other tertiary institution.

The sources that have been used or quoted have been indicated and duly acknowledged as complete reference.



Signature……

Date……

RECOMMENDATION

I **Kaswalale Kakuwa-Mwauluka** recommend that this dissertation prepared under my supervision by **Chilufya Chanda** entitled **THE IMPACT OF TECHNOLOGY ON THE LAW: EXAMINING DIGITAL PRIVACY AND ELECTRONIC EVIDENCE**, be accepted for examination. I have checked it carefully and I'm satisfied that it fulfills the requirement pertaining to the format laid down in the regulations governing directed research.

Mrs. Kaswalale Kakuwa-Mwauluka

……..

2025

DEDICATION

This paper is dedicated to my Mom Rose S Chanda and Dad George K Chanda, thank you for your unweaving support and seeing in me a lawyer even when I could not fathom it. Your words, counsel, and support have brought me this far and continue to push me to through my journey of life.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Mrs Mwauluka my supervisor for all the counsel you have given me throughout my research, both academic and social. For all the knowledge you have impacted on me I would like to extend my gratitude to you.

To my siblings, Mwamba, Mulenga, Emmanuel and Khadija, I would like to thank you for all your support you have pushed me to be the best vision of myself by seeing in me achievements that I myself did not see. Thank you for inspiring me to reach heights as great as yours and showing me that it is possible to exceed those achievements.

To all the lecturers that have made this possible, I thank you for all the lessons, guidance and encouragements have me law school more bearable. To Ms. Mwaka Chizinga, thank you for making me realize that everything is possible through God and hardwork. Mr. Thomas Malama, thank you for inspiring in me the love of IT law, your passion for IT law has sparked an interest in me for cyber space awareness and the law governing it. Ms. Mutemwa, you have been an inspiration to me, you have sharpened me so that I give my best and not only do the bear minimum. You continue to inspire me to become my best self.

All my friends that have helped and contributed to this, not so easy, journey of law school, I am deeply humbled by your help, support and always pushing me to give it my best.

LIST OF ABBREVIATIONS

AI	**Artificial Intelligence**
CIPESA	**Collaboration on International ICT Policy for East and Southern Africa**
CMCC	**Central Monitoring and Coordination Centre**
CSO	**Civil Society Organizations**
DPC	**Data Protection Commissioner**
ECT	**Electronic Communications and Transactions Act**
GDPR	**General Data Protection Regulation**
ICT	**Information Communications and Transactions Act**
IoTs	**Internet of Things**
MISA	**Media Institute of Southern Africa Zambia**
OECD	**Organisation for Economic Co-operation and Development**
SOPs	**Standard Operating Procedures**
ZICTA	**Zambia Information and Communications Technology Authority**

TABLE OF CONTENT

TABLE OF STATUES

Constitution of Zambia, Act 17 of 1996

Cyber Crimes Act No.4 of 2025

Cyber Security Act No.3 of 2025

Cyber Security and Cyber Crimes Act No. 2 of 2021

Data Protection Act No. of 2021

Electronic and Communication Technologies Act No.4 of 2021

Evidence Act Chapter 43 of the Laws of Zambia

TABLE OF CASES

ABSTRACT

The rapid and pervasive integration of digital technologies into society has fundamentally challenged traditional legal paradigms, creating a critical tension between technological innovation and established legal principles. This research examines this dynamic within the Zambian context, focusing on the interconnected domains of digital privacy and electronic evidence. The study is motivated by the central problem that advancements in technology—such as artificial intelligence (AI), big data, cloud computing, and social media—have outpaced the evolution of Zambia's legal framework, leading to significant gaps in the protection of fundamental rights and the effective administration of justice.

The study employs a qualitative, desk-based research methodology, critically analyzing primary sources including the Constitution of Zambia, the Data Protection Act (2021), the Electronic Communications and Transactions Act (2021), and the newly enacted Cyber Security Act (2025) and Cyber Crimes Act (2025). This is supplemented by a review of secondary sources such as case law, scholarly articles, and regional comparative analyses to situate Zambia's legal response within a broader context.

The investigation reveals that while Zambia has made significant legislative strides in recognizing digital privacy and electronic evidence, the current framework remains fragmented and inadequately enforced. Key findings indicate that the laws exhibit a concerning tilt towards state security and surveillance, often at the expense of the constitutional right to privacy enshrined in Article 17. Provisions within the cyber laws grant broad interception powers with insufficient judicial oversight, creating risks for freedom of expression and dissent. Furthermore, the legal provisions for electronic evidence, particularly under the ECT Act, are undermined by practical challenges in authentication, chain of custody, and a lack of specific procedural rules, leading to inconsistent judicial application.

The research also identifies profound institutional weaknesses that cripple effective implementation. Regulatory bodies like the Zambia Information and Communication Technology Authority (ZICTA) and the Data Protection Commissioner suffer from limited independence, technical capacity, and resources. The judiciary and law enforcement agencies, including the Zambia Police Cybercrime Unit, lack the

specialized training and forensic tools necessary to reliably handle and adjudicate complex digital evidence.

In conclusion, the study asserts that Zambia's legal system, while increasingly cognizant of digital age challenges, is reactive and struggling to maintain a necessary balance between technological utility, individual rights, and state power. To bridge this gap, the research proposes a suite of targeted recommendations. These include legislative reforms to refine vague provisions and enhance privacy safeguards, procedural reforms to establish standardized digital forensics protocols, and institutional strengthening through increased funding, specialized training, and the promotion of inter-agency coordination. By adopting a proactive, rights-centric approach to digital governance, Zambia can forge a legal framework that harnesses technological benefits while steadfastly upholding justice, accountability, and fundamental freedoms.

CHAPTER ONE
GENERAL INTRODUCTIONS

1.0 INTRODUCTION

The evolution of time has come with the evolution of mankind, from the stone-age to the industrial age and more recently the digital age. With the introduction of the digital age comes a fast-paced integration of different technologies in today's world which led to inadequacies in the laws meant to govern said technologies.

The Constitution of Zambia [1] provides for the right to privacy including the right not to be searched (person, home or property); not to have possessions seized; not to have information relating to family, health status and private affairs unlawfully required or revealed; and not to have communications infringed.[2] The fundamental right has been threatened by the advent of emerging technologies that usually require disclosure of personal information as they are used.

Digital privacy can be defined as to the right and ability of individuals to control their personal information—including how it is collected, stored, processed, and shared—within digital environments. This also encompasses the measures, practices, and regulations that protect personal data from unauthorized access, misuse, and exposure in electronic communications and online interactions.

The rapid rise in technologies, such as Deepfake and Artificial Intelligence (AI), have introduced new ways of evidence manipulation that have created challenges in evidence management. Electronic data has become more susceptible to alterations, thus, creating a challenge in its reliability and admissibility in court. Electronic evidence can be defined as any probative information stored or transmitted in electronic form that a party may use in legal proceedings. This may include data generated by or stored on a wide range of digital devices and media such as computers, smartphones, digital cameras, and network servers as well as communications like emails, text messages, and social media interactions.

[1] Act No.17 of 1996

[2] CIPESA, *Zambia: Insights into the Data Protection Act 2021* (CIPESA 2021) https://cipesa.org/wp-content/files/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf accessed 16 April 2025.

Essentially, electronic evidence is the digital counterpart to physical evidence in traditional investigations and must be collected, authenticated, and preserved following strict guidelines to ensure its admissibility in court.

1.1 BACKGROUND OF THE STUDY

The late 2000's marked the initial steps that Zambia's legal framework took to adjust to the digital era, through the enactment of the **Information and Communications Technologies Act (2009)** and the **Electronic Communications and Transactions Act (2009)**, which recognized that digital data could have legal validity and regulated aspects of electronic communications, respectively. These Acts set the stage, but the more granular provisions in the realm of digital privacy and evidence were to follow. In 2021, Zambia reacted to its urgent need for more extensive laws of digital information, with the introduction of several important set of documents.

Zambia enacted the **Data Protection Act, 2021**[3] and the **Electronic and Communication Technologies Act, 2021**[4]**.** To provide for the use and protection of personal data and to regulate the collection, use, transmission, storage and processing of personal data; and to provide a safe, secure and effective environment for electronic communications and promote legal certainty, respectfully. However, despite the fairly drafted law some problematic provisions that deal with processing data for personal use, cross-border data transfers,

Another significant Act that Zambia enacted was the **Cyber Security and Cyber Crimes Act, 2021**[5] which specified offences related to unauthorized computer access, inter alia, and also outlined clearly provisions for the collecting and preservation of electronic evidence. Notably, Part X of the Act dealt specifically with electronic evidence, setting the criteria for its admissibility in criminal proceedings. However, this law has recently been repealed and replaced by the enactment of the **Cyber Security Act, 2025**[6] and the **Cyber Crimes Act, 2025**[7]**,** these Acts are a

[3] Act No.3 of 2021

[4] Act No.4 of 2021

[5] Act No.2 of 2021

[6] Act No.3 of 2025

response to the inadequacies left by their predecessor. However, they undermine the right to privacy in that they have intrusive provisions that give the government power to intercept and survey private communications thus threatening the right to privacy.

1.2 STATEMENT OF THE PROBLEM

Over the past three decades the integration of advanced digital technology into our everyday life has presented both opportunities and complex challenges in the legal systems worldwide. In Zambia, the growing reliance on digital platforms for communication, data storage, and transactions has raised significant concerns regarding digital privacy and the management of electronic evidence within the legal framework. Issues such as unauthorised data access (hacking), online child soliciting, Internet of Things (IoTs), cross boarder data flows, and rapidly emerging technologies such as Deepfake and Artificial Intelligence (AI) have outpaced current laws and contributed to the lack of adequate enforcement and protection of digital privacy and the handling of electronic evidence effectively.

The Constitution of Zambia[8], specifically under Article 17, guarantees the fundamental and inherent right to privacy, which encompasses digital privacy. This is further exemplified by the enactment of the Data Protection Act No. 3 of 2021 which was a significant step in protecting personal data by regulating its collection, processing, storage, and dissemination. However, despite this legislative progress, ambiguities persist regarding the practical enforcement of digital privacy rights and the consistent application of electronic evidence in judicial proceedings. Courts are increasingly tasked with assessing the admissibility and reliability of electronic evidence while also contending with emerging threats to personal privacy. This calls for a comprehensive examination of how existing laws respond to the evolving digital environment.

Therefore, this study will seek to address this problem by first exploring the concepts of digital privacy and electronic evidence to establish a foundational understanding. Second, it will critically examine Zambia's legal framework governing digital privacy,

[7] Act No.4 of 2025

[8] Act No.17 of 1996

and electronic evidence. Finally, the study will analyze the impact of technological advancements on these legal frameworks, identifying existing gaps and proposing recommendations for legislative and procedural reforms to enhance the protection of digital privacy rights and the reliable use of electronic evidence in legal proceedings. Addressing these issues is crucial for developing a robust legal system that aligns with technological advancements and upholds justice in Zambia.

1.3 OBJECTIVES OF THE STUDY

i. To explore the concept of digital privacy and electronic evidence.

ii. To explore the legal framework governing digital privacy and electronic evidence in Zambia.

iii. Critically analyse the impact of technology on the legal framework governing digital privacy and electronic evidence.

1.4 RESEARCH QUESTIONS

During the synopsis of this research the following questions will be asked;

i. What is the concept of digital privacy and electronic evidence?

ii. What is the legal framework governing digital privacy and electronic evidence in Zambia?

iii. What is the impact of technology on the legal framework governing digital privacy and electronic evidence?

1.5 SIGNIFICANCE OF STUDY

The aim of this research is analysing Zambia's current legal frameworks governing digital privacy and electronic evidence and addressing significant deficiencies such as the gap between rapid technological changes and slow legislative adaption. This research seeks to contribute to the development of robust mechanisms that enhance the protection of digital privacy rights, thereby promoting fair and effective legal proceedings. Furthermore, the study's forward-looking approach will explore the

possibilities of reformed legal frameworks that are not only reactive but also proactive in managing future technological challenges. The study's recommendations will seek to influence policymakers and legislators to make necessary updates, like amendments to existing laws or drafting new instruments, to the current legal framework to better align with the digital era. In so doing, the research will seek to establish a balanced perspective on technological innovation and regulation allowing Zambia to harness the benefits of advanced digital technologies while safeguarding individual rights and justice.

1.6 SCOPE OF STUDY

This study will analyse the legal frameworks of Zambia including the **Constitution of Zambia (Article 17)**[9], **Data Protection Act**[10] and **Cyber Security Act**[11] in regards to digital privacy and electronic evidence in Zambia. The research intends to examine further the concepts of digital privacy and its definition in constitutional law along with modern technological challenges. The study will focus on considering the concepts of admissibility, reliability, and challenges of integrating electronic evidence in court. Some emphasis will be placed on new inventions like the Internet of Things (IoT), Artificial Intelligence (AI), Deepfake technologies, and cyber malicious acts of hacking and solicitation of minors. Furthermore, this approach will evaluate how these developments create new challenges for existing legal frameworks.

1.7 LITERATURE REVIEW

In a report prepared by **Collaboration on International ICT Policy for East and Southern Africa (CIPESA)**[12]**,** that provides a descriptive overview of Zambia's Data Protection Act 2021. It highlights key provisions (rights of data subjects, obligations on controllers, heavy penalties) and notes that the Act "highly reflect the

[9] Act No.17 of 1996

[10] Act No.3 of 2021

[11] Act No.3 of 2025

[12] CIPESA, *Zambia: Insights into the Data Protection Act 2021* (CIPESA 2021) https://cipesa.org/wp-content/files/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf accessed 10 April 2025.

internationally acceptable data protection standards" of the OECD Guidelines and EU's GDPR. In particular, it enumerates consent rules, impact assessments, and an (imperfectly independent) Data Protection Commissioner. However, the report is mainly explanatory/advocacy – it catalogues statutory "pros" for example, strong rights, fines and "cons" such as, undefined "personal use" exception, weak regulator independence, broad national-security exemptions. It does not empirically assess how the law works in practice or discuss its intersection with criminal procedure or digital evidence. This research will fill this gap by moving beyond a summary of the statute to analyze how the Data Protection Act operates in courts and investigations, and how it interacts with electronic evidence rules. For example, CIPESA notes privacy protections (GDPR-aligned rights), but my focus will be to study whether law enforcement respects these privacy safeguards when collecting electronic evidence. In short, this research expands on the CIPESA's report by linking the legal framework to the real-world impact of technology on privacy and evidentiary practice.

In their study, **Moola and Kawimbe[13],** investigates the data protection challenges confronting digital platforms in Zambia, focusing on issues such as online privacy practices, personal data breaches, regulatory frameworks, cyber security incidents, user awareness, and the impact of emerging technologies. Published in the Global Scientific Journal (May 2024), the paper situates Zambia's experience within broader global debates on data protection and digital trust. The paper highlights that despite the enactment of legislation on ICT enforcement remains uneven due to limited institutional capacity, scarce resources, and low public awareness. The study's limitation is its *scope*: it relies on literature review (no new data) and emphasizes technical/cyber-security angles, but it does not address legal evidence. It briefly notes privacy's importance but not how courts handle digital evidence. The research portrays a literature gap by explicitly bridging privacy and evidentiary law. While Moola & Kawimbe call for stronger enforcement and awareness, this study will examine why enforcement is weak and how legal processes, such as admissibility of

[13] Nalumino Moola and Sidney Kawimbe, 'Data Protection Challenges on Digital Platforms: A Case for Zambia' (2024) 12(5) *Global Scientific Journal* 61 https://www.globalscientificjournal.com/researchpaper/Data_Protection_Challenges_on_Digital_Platforms_A_Case_for_Zambia.pdf accessed 8 April 2025.

e-evidence, might undermine or protect privacy. In effect, my research goes deeper into the legal-technical intersection that Moola & Kawimbe only outline.

The scholars **Sam Phiri and Zorro**[14] in their report provide an overview of the digital rights environment in Zambia, discussing regulatory frameworks, challenges in digital inclusion, and the role of civil society in advocating for digital freedoms. Its core focus is on "openings and closings" of civic space – e.g. how government actions (laws, censorship) and weak civil society shape online activism. It acknowledges privacy as one of many rights (along with expression and assembly) but does not deeply analyze legal doctrine or technical evidence issues. The report, based on literature and interviews, is qualitative and broad; it lacks detailed legal analysis of new privacy laws or evidence rules. The researcher's study fills a narrower but critical gap, whereas Phiri & Zorro identify the general climate of digital rights (noting that Zambia's civic space has "narrowed" and stressing activism), my research zeroes in on legal processes. It will explore how technological changes (surveillance, cybercrime tools, digital evidence collection) concretely impact privacy rights and trials. In other words, it builds on Phiri & Zorro's context by analyzing the mechanisms (like legislation and court practice) through which technology affects individual rights in Zambia.

Frempong & Danquah[15] in their study survey Ghanaian court cases and practitioners to assess how Ghana handles digital evidence. Its focus is on electronic evidence admissibility: it documents cases where evidence (phone logs, recordings, etc.) was contested and notes common legal issues. For example, it finds courts often reject electronic evidence for lack of warrants or proper foundation, thus implicating privacy and due process. The authors conclude that Ghana's courts struggle with e-evidence reliability due to procedural gaps (e.g. no warrants, privacy

[14] Sam Phiri and Zorro, 'Zambia Digital Rights Landscape Report' in Tony Roberts (ed), *Digital Rights in Closing Civic Space: Lessons from Ten African Countries* (Institute of Development Studies 2021) 61–84 https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/15964/Zambia_Report.pdf accessed 8 April 2025.

[15] Michael Adjei Frempong and Paul Asante Danquah, 'Reliability of Digital Evidence and Legal Matters: Ghana in Perspective' (2022) 184(8) *International Journal of Computer Applications* 9–17 https://ijcaonline.org/archives/volume184/number8/32347-2022922046/ accessed 26 August 2025

breaches). A limitation is its narrow geographic focus and methodology, it analyzes Ghana's context and uses surveys of local officials, so findings may not generalize beyond Ghana. Also, it addresses reliability factors (accuracy, authenticity) but does not cover broader privacy implications of evidence gathering. This work on Zambia will expand beyond Ghana by providing a comparative perspective: It will contrast Zambia's legal framework with Ghana's, noting where Zambian law is more or less stringent. However, this research will examine if Zambia's courts face similar warrant and privacy issues with digital evidence, or if new Zambian cyber laws (e.g. Cyber Crimes Act 2025) change the equation. Thus, the novel contribution is to take insights like those of Frempong & Danquah (court struggles over e-evidence) and test them in Zambia's emerging legal landscape.

Rusakova & Falkina's[16] work is a comparative article that overviews how various African nations (Egypt, Nigeria, South Africa, Kenya, Ghana, etc.) regulate electronic evidence. It summarizes each country's laws on admitting electronic documents and identifies common features (e.g. procedural requirements, evidentiary weight). The authors note a general trend that "the institution of electronic evidence is rapidly developing" in African civil procedure. Its focus is legal-comparative: it catalogues statutes and case law on e-evidence, but mostly from a macro perspective. It does not delve into privacy concerns or country-specific challenges in depth. For Zambia, such a source provides context but not detailed analysis. This study diverges by drilling down on Zambia, it will check whether the trends Rusakova & Falkina identified (rapid development, evolving standards) hold true in Zambia's courts, and examine any unique Zambian issues. For example, while Rusakova & Falkina cover Ghana and Nigeria, this research can contribute new knowledge about Zambia's procedural rules and how they handle, say, electronic records in criminal cases. In sum, Rusakova & Falkina set the continental backdrop, and this research fills a national case-study gap, especially by linking evidence rules to data privacy and tech use in Zambia.

[16] E P Rusakova and G Y Falkina, 'Legal Regulation of Electronic Evidence in African Countries' (2024) **17(5) Gaps in Russian Legislation** 53–60 https://doi.org/10.33693/2072-3164-2024-17-5-053-060 accessed 26 August 2025

GDPR/OECD Guidelines (International Comparisons)[17] many references (including CIPESA) note that Zambia's Data Protection Act was modelled on OECD and GDPR standards. These international frameworks represent global best practices (consent, data minimization, rights) but are by nature broad and generalized. Their limitation is that they do not address local enforcement realities or law enforcement needs. This research is novel in that it can examine how well Zambia's law actually lives up to these standards. For instance, CIPESA praised Zambia's alignment with GDPR principles, but this research might investigate whether Zambia's law enforcement and courts balance those privacy principles against digital investigation needs. Thus, by comparing Zambia's approach to GDPR/OECD, he can highlight unique divergences – an analysis absent in the cited works.

The **World Bank (Digital Governance)**[18] publications provide *macro-level* analysis of data governance and digital economy risks across African countries. They emphasize the importance of robust privacy laws for building trust, but do not focus on legal procedure or evidence. The limitation of such reports is their broad scope; they treat privacy and cyber-security as economic/regulatory issues, not as components of legal adjudication. This author's study adds depth by connecting these high-level concerns to Zambia's legal system. For example, whereas a World Bank report might note that Zambia enacted a Data Protection Act, my research will ask how it is working in practice — especially when electronic data enters the courtroom. Its contribution is to bridge the gap between policy recommendations and on-the-ground legal realities.

1.8.0 METHODOLOGY

1.8.1 RESEARCH APPROACH

[17] Organisation for Economic Co-operation and Development (OECD), 'Privacy and Data Protection' (OECD, 2025) https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html accessed on 26 August 2025

[18] World Bank, *Regulating Digital Data in Africa* (World Bank, 2016) https://openknowledge.worldbank.org/bitstreams/62e27761-1da1-467f-99a2-a6a1a3cf3b54/download accessed 26 August 2025

The research will be carried out using the qualitative research methodology. This approach involves a desk research methodology that will examine, evaluate, and critique existing legislations, case law, textbooks, articles, journals, internet research and other scholarly works[19].

1.8.2 RESEARCH DESIGN

The research will adopt an integrated approach, primarily focusing on library as well as desk research for data collection, and the data analysis process entails a critical and thorough review and description of applicable legal provisions.[20]

1.8.3 RESEARCH TYPE

Descriptive study will be employed to explain the current legal framework governing digital privacy and electronic evidence as fully as possible[21].

1.8.4 DATA COLLECTION

Due to the nature of the study both the Primary and Secondary Data will be collected through relevant legislation, judicial decisions, journals, textbooks, internet sources, research papers and legal reports[22].

1.8.5 DATA ANALYSIS

Due to the qualitative character of the research methodology employed for this study, all collected data (both primary and secondary) will be analysed using the content analysis method and the thematic analysis method[23].

1.8.6 STUDY POPULATION

As this study is primary based on the Zambian legal framework it will include every citizen of Zambia.

---

[19] John W Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th edn, Sage Publications 2014)

[20] Ibid

[21] Ibid

[22] Ibid

[23] Ibid

1.8.7 SAMPLE SIZE

This research will be targeted at all persons with credible knowledge and expertise on the subject matter.

1.8.8 SAMPLING TECHINQUE

This research employed a purposive technique as well as the snowball technique with the aim of obtaining the most accurate and credible up to date information from reliable and trust worthy institutions and experts.

1.9 ETHICAL CONSIDERATIONS

In order to conform with ethical requirements of research, first permission will be sought from the UNILUS research ethics committee, second, permission will be sought from organizations, third, permission will be sought from individual research subject, lastly, researcher will endeavour to follow academic writing requirements like referencing and acknowledgement of other people's work.

1.10 OUTLINE OF CHAPTERS

CHAPTER ONE: Introduces the research topic and discusses the important aspects of this research paper. It comprises of the background of the study, statement of the problem, objectives of the study, research questions and significance of the study as well as the methodology and ethical considerations.

CHAPTER TWO explores the existing conceptual framework on digital privacy and electronic evidence, providing definitions and key themes. It introduces the legal and theoretical frameworks underpinning the research, including right-based theories and evidentiary principles.

CHAPTER THREE critically examines Zambia's legal framework relevant to digital privacy and electronic evidence. It, among other things, assesses how these laws address modern technological challenges and the extent to which they protect privacy rights and regulate electronic evidence. It further considers implementation challenges and gaps in the existing legal framework.

CHAPTER FOUR evaluates how technological developments have influenced Zambia's legal treatment of digital privacy and electronic evidence. The chapter critically analyses whether current laws are adequate to address these challenges and how they are interpreted or enforced in practice.

CHAPTER FIVE is a summary of the major finding of the study and will offer practical recommendations for legal, institutional and policy improvements.

CHAPTER TWO

AN EXPLORATION OF THE CONCEPTUAL FRAMEWORK ON DIGITAL PRIVACY AND ELECTRONIC EVIDENCE

2.0 INTRODUCTION

As society becomes increasingly digitized, the intersection between technology and law continues to evolve rapidly. Central to this transformation are the concepts of digital privacy and electronic evidence. This chapter will delve into the first objective of this research which addresses these two concepts of digital privacy and electronic evidence. The chapter explores these concepts in depth, offering a foundational understanding of their meanings, significance, and interrelatedness. It also analyses how legal frameworks have adapted—or failed to adapt—to address emerging challenges in the digital realm.

This chapter will further seek to show the interplay of the two concepts Digital Privacy (grounded in rights-based theory, emphasizing individual control and consent) and Electronic Evidence (analysed through a legal procedural lens, focusing on admissibility, reliability, and due process). By integrating these perspectives, this research aims to critically assess how Zambia's legal system balances technological change with the protection of privacy rights and procedural fairness.

2.1 Digital Privacy

2.2 Definition and Scope

Digital privacy also referred to as information privacy or data privacy refers to the protection of personal data and communication in the digital environment. This can also refers to the protection of personal information that is collected, stored, processed, and transmitted through digital platforms.[24] It encompasses the right of individuals to control how their data is used and the obligation of institutions to respect this right.

[24] Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, 'Privacy and Information Technology' (Stanford Encyclopedia of Philosophy, 2020) https://plato.stanford.edu/entries/it-privacy/#ImpInfTecPri accessed 10th August 2025

Certain jurisdictions have defined digital privacy differently, such as, the principle of *informational self-determination*, originating in German constitutional law, refers to an individual's authority to decide when and within what limits personal data about their private life may be communicated.[25]

In the digital era, scholars emphasize the complexity of digital privacy, highlighting threats such as surveillance, data mining, and profiling. **Alan Westin** defines privacy as "*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*," introducing key states such as solitude, intimacy, anonymity, and reserve[26]. **Helen Nissenbaum's theory of Contextual Integrity** defines privacy as the preservation of "appropriate flows of information" in specific social contexts, guided by norms concerning actors, data subjects, information types, and transmission principles. **David Flaherty** emphasizes privacy as "information control," highlighting how data collection, use, and sharing must be governed by individuals' consent and control over their personal information[27].

2.1.1 Legal Foundations on Digital Privacy

Article 17 of the **Constitution of Zambia**, safeguards the protection of home, correspondence and communication. However, whether this fully extends to digital privacy remains debatable. In modern society privacy extends to personal data of individuals which has been defined by the **Data Protection Act (2021)** as data which relates to an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

On the global context, digital privacy rights are increasingly being recognized as extensions of fundamental human rights. International instruments such as the **Universal Declaration of Human Rights (Article 12)** and the **International**

[25] *Reinventing data protection?. Gutwirth, Serge. [Dordrecht?]: Springer. 2009.*

[26] Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, 'Privacy and Information Technology' (Stanford Encyclopedia of Philosophy, 2020) https://plato.stanford.edu/entries/it-privacy/#ImpInfTecPri accessed 10 August 2025

[27] Ibid

Covenant on Civil and Political Rights (Article 17) guarantee protection against arbitrary interference with privacy.

2.1.2 Forms of Digital Privacy

- **Information privacy** – is concerned with the interest of individuals in exercising control over access to information about themselves. Think here, for instance, about information disclosed on Facebook or other social media. All too easily, such information might be beyond the control of the individual.[28]
- **Communication privacy** – is the notion that individuals should have the freedom, or right, to communicate information digitally with the expectation that their communications are secure—meaning that emails, messages and other types of communications will only be accessible to the sender's original intended recipient.[29]
- **Locational privacy** – has to do with individual's protection from control over location tracking and GPS data.
- **Online Behavioural privacy** – the notion that individuals have a right to exist freely on the internet, in that they can choose what type of information they are exposed to, and more importantly, that unwanted information should not interrupt them.[30] For example, tracking via internet cookies and algorithms.

2.1.3 Legal Challenges and Concerns

a) State Surveillance vs. Privacy Rights

---

[28] Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, 'Privacy and Information Technology' (Stanford Encyclopedia of Philosophy, 2020) https://plato.stanford.edu/entries/it-privacy/#ImpInfTecPri accessed 13 August 2025

[29] *Hung, Humphry; Wong, Y.H. (2009-05-22). "Information transparency and digital privacy protection: are they mutually exclusive in the provision of e-services?". Journal of Services Marketing.* ***23*** *(3): 154–164. doi:10.1108/08876040910955161. hdl:10397/20138*

[30] Ibid.

A critical tension exists between national security imperatives and privacy protections. Laws granting surveillance powers can conflict with democratic values and the rule of law.[31]

b) Technological Progress Outpacing Legislation

Emerging technologies—like encryption, biometrics, AI, IoT, blockchain—often outstrip existing legal standards, leaving new forms of data use beyond regulatory scrutiny. Blockchain, for example, challenges the "right to be forgotten" due to its immutable nature, complicating compliance with privacy laws.

c) Jurisdictional Fragmentation & Enforcement Gaps

Variations in privacy laws across jurisdictions create compliance complexity for organizations and weaken law enforcement's effectiveness. Regulatory bodies often lack sufficient resources or authority to enforce laws, leading to weak accountability for privacy violations.

d) Evolving Definition of Personal Data and Consent

The scope of "personal data" is expanding, increasing ambiguity for organizations regarding legal obligations. Consent mechanisms are under strain: complex and lengthy policies result in users consenting without understanding the implications.

e) Industry Influence and Regulatory Capture

Apathy or ignorance among the public can allow political or corporate interests to shape privacy laws more than citizen concerns. GDPR, though progressive, has shown signs of being influenced more by market players than users.[32]

---

[31] Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, 'Privacy and Information Technology' (Stanford Encyclopedia of Philosophy, 2020) https://plato.stanford.edu/entries/it-privacy/#ImpInfTecPri accessed 13 August 2025

[32] Bartlomiej Chomanski and Lode Lauwaert, *Digital Privacy and the Law: The Challenge of Regulatory Capture* (AI & Society, published online 10 August 2024, printed in 40(4) 2025, 2777–2787) https://doi.org/10.1007/s00146-024-02041-8 accessed 13 August 2025

f) Transparency and Power Imbalance in Platforms

Terms of use often coerce users into broad consent without meaningful negotiation. Platforms leverage their dominance, leading to privacy-risk trade-offs disguised as convenience.[33]

g) Cross-Border Legal Gaps

Disparate privacy regimes hinder cooperation in international data investigations and enforcement.

2.2 Understanding the Concept of Electronic Evidence

2.2.1 Definition and Nature

Electronic evidence is any probative information stored or transmitted in digital form that may be used in legal proceedings. This includes emails, text messages, digital photographs, logs, videos, and computer files.

Essentially, electronic evidence is comprised of three main elements, the first being binary data, the second being a storage device on which to store that binary data and thirdly, software to read and interpret the binary data. Electronic evidence is fundamentally different to hard copy, such that the rules of evidence surrounding documentary evidence need to be re-examined[34].

Historically, evidence acquisition relied on physical documents, witness testimonies, and tangible items. The advent of technology has shifted this paradigm, introducing sophisticated digital tools that streamline the collection of data, such as video recordings, digital footprints, and electronic communications.

Case law and practice highlight the dynamic nature of electronic evidence, which differs from traditional evidence in terms of format, volatility, and authenticity concerns. For example, in ***Bentry Siamalambwa v Magna Mining Limited****,* the

---

[33] Tong Lin, 'Challenges and Legislative Responses to Privacy Protection in the Digital Age' (2025) *Lecture Notes in Education Psychology and Public Media* vol 95, 21–30 https://doi.org/10.54254/2753-7048/2025.23023 accessed 12 August 2025

[34] Allison R Stanfield, *The Authentication of Electronic Evidence* (PhD thesis, Queensland University of Technology, 2016) https://eprints.qut.edu.au/93021/ accessed 15 August 2025

court highlighted how important it is that the integrity of data message needs to be established and this is done by the certification of the data message sought to be produced in legal proceedings, pursuant to **section 9(4)** of the **ECT Act**.

As legal standards adapt to these technology-driven changes, an on-going dialogue between the legal and technological worlds is essential. Striking a balance ensures that while leveraging technology's benefits, the integrity of the legal process remains intact.

2.2.2 Characteristics of Digital Evidence

- **Easily altered or deleted** – The advent of new technologies makes digital evidence easily alterable or deleted. Deepfakes and AI technologies make it difficult to tell whether evidence has been tempered with or not.
- **Difficult to authenticate** - Is the electronic evidence the same as it was when it was created? Maintaining electronic evidence's integrity has become more and more complex.
- **May be stored remotely (cloud storage)** – Evidence can now be stored on online servers remotely.
- **May require forensic analysis to access** – the delicate nature of digital evidence means that it can be easily tempered with thus it requires forensic experts to access it.

2.2.3 The Role of Electronic Evidence in Modern Litigation

In contemporary legal proceedings, technology significantly impacts the nature of evidence, as the digital realm has fostered new forms of evidence, including social media posts and data from connected devices.

Electronic evidence plays a growing role in both civil and criminal cases. For instance, in criminal law, it may include forensic retrieval of text messages, call logs, or GPS location in investigating crimes. While in civil disputes, emails or transaction logs may serve as proof of contract formation or breach as seen in the case of ***Bentry Siamalambwa v Magna Mining Limited***.

Regulatory bodies also rely on digital records for audit and compliance purposes. However, this shift presents challenges regarding authentication, preservation, and legal admissibility, complicating the traditional understanding of evidence in court.

2.2.4 Admissibility of Electronic Evidence

The admissibility of electronic evidence is governed by legal standards related to relevance, authenticity, reliability, and proper chain of custody. Different jurisdictions may vary in their evidentiary requirements. In Zambia, the **Electronic Communications and Transactions Act (2021)** provides a legal basis for recognizing electronic records and signatures, though practical enforcement remains a challenge.

2.2.5 Challenges of Electronic Evidence

a) Admissibility & Authentication

Legal systems evaluate relevance, authenticity, and reliability of digital evidence. Rigorous chain-of-custody protocols and expert testimony are essential to avoid exclusion. Courts use legal standards to assess whether digital forensic methods meet accepted scientific criteria.

b) Preservation & Integrity

Digital data can be corrupted, tampered with, or deleted. Forensic imaging and secure preservation protocols are needed to maintain evidential integrity.

c) Technical Complexity & Expertise

Proper handling requires specialized forensic skills and tools. Missteps in collection or preservation can lead to inadmissibility. Additionally, judges may find it difficult to understand digital material without expert facilitation.

d) Presentation Challenges

Modern EDRM stages (e.g., presentation) face hurdles: ensuring authenticity, context, formatting, and interpreting AI-generated or social media evidence – such

as memes or chat transcripts—for legal audiences.[35] Courts are ill-prepared for deepfakes and AI-generated media; verifying authenticity and maintaining chain-of-custody remains a growing challenge.

e) Volume & Source Diversity (E-Discovery)

The explosion of digital content (emails, files, logs) makes e-discovery particularly challenging, especially for small firms with limited resources.

f) Jurisdictional & Cross-Border Issues

Electronic evidence often resides on servers scattered across borders. Differing national laws create hurdles for access, cooperation, and admissibility.

g) Security & Cyber-threats

Cyber-attacks (copies, data corruption) can undermine trust in electronic evidence. Stringent cyber-security and audit protocols are required.[36]

2.3 The Interplay between Digital Privacy and Electronic Evidence

The relationship between digital privacy and electronic evidence is complex and sometimes contradictory. On one hand, electronic evidence is essential for effective law enforcement and dispute resolution. On the other hand, its collection and use may infringe upon individuals' digital privacy.

This intersection of digital privacy and electronic evidence raises complex legal questions, particularly in balancing the right to privacy with the needs of law enforcement and the justice system.

For example: *How much personal data can the State access during investigations? Under what conditions private communications are used as evidence? What are the safeguards against the misuse of intercepted or hacked information?*

---

[35] Reuters, *From AI chatbots to social media: data presentation gets a little more complicated* (11 August 2025) https://www.reuters.com/legal/legalindustry/ai-chatbots-social-media-data-presentation-gets-little-more-complicated-2025-08-11/ accessed 15 August 2025.

[36] Ibid

These concerns are central in jurisdictions worldwide and have sparked the need for new legislation, privacy regulations and constitutional protections. In the Zambian context, the newly accented to **Cyber Security Act (2025)** has to an extent addressed the issue of private communications being intercepted and used as evidence.

This tension necessitates a balance between: Privacy rights of individuals, especially against arbitrary surveillance or data seizure on the one part and investigatory and judicial needs to obtain and rely upon digital records for justice on the other part.

The principle of proportionality is often invoked to justify intrusions into digital privacy where necessary and lawful. However, lack of oversight and technical knowledge among enforcement agencies poses a risk of overreach.

2.4 Conclusion

This chapter has unpacked the foundational concepts of digital privacy and electronic evidence. It has shown that while digital tools offer enormous potential for enhancing legal processes, they also raise significant privacy and procedural concerns. As the legal system seeks to adapt to technological change, there is a clear need for robust legal and institutional safeguards to ensure both effective justice delivery and protection of fundamental rights.

This chapter establishes the groundwork for the next chapter, which will examine the current legal framework in Zambia governing these issues.

CHAPTER THREE

EXPLORING THE LEGAL FRAMEWORK GOVERNING DIGITAL PRIVACY AND ELECTRONIC EVIDENCE IN ZAMBIA

3.0 INTRODUCTION

This chapter shall address the second objective of the research which speaks about the legal framework governing digital privacy and electronic evidence in Zambia. This chapter will delve into the existing legislation, such the constitution, the data protection act, the cyber-crimes act and the cyber security act. The chapter will further examine the institutional frameworks such as ZICTA, the Judiciary and Civil Society. The chapter evaluates whether existing laws adequately balance privacy protection, technological realities, and the admissibility of electronic evidence.

3.1 Constitutional Framework on Privacy and Evidence

The Constitution of Zambia being the grand norm of laws gives provides the foundation for privacy and fair trial rights. Like eluded to in the previous chapters, **Article 17** protects citizen's right to privacy, which includes the protection against arbitrary search of person, home, or property and against interference with correspondence. **Article 18** guarantees fair trial right, which extend to the right against unlawful evidence collection. Further, **Article 20** protects freedom of expression, indirectly supporting the confidentiality of digital communication. However, the broad limitation clauses allowing derogations for "defence, public safety, public order, public morality or public health" create room for State encroachment on digital privacy. This scholar argues that this weakens the strength of constitutional protections in the digital era.

3.2 Statutory Framework

3.2.1 The Evidence Act (Cap. 43 of the Laws of Zambia)

The Evidence Act[37] provides general rules on admissibility of evidence. **Section 2** defines a "document" broadly to include "any device by means of which information is recorded or stored." This formulation is flexible enough to cover electronic

[37] Chapter 43 of the Laws of Zambia

documents, computer files, and other digital records. While, **sections 3 and 4** govern the admissibility of documentary evidence in both civil and criminal proceedings, permitting statements in documents to be used if the maker is unavailable or if records are kept in the ordinary course of business. The best evidence rule requires production of primary evidence, though courts have discretion to admit secondary evidence, such as certified copies of electronic records.

While these provisions accommodate electronic evidence by interpretation, they lack explicit standards on authentication, chain of custody, or metadata, creating uncertainty in practice. To address these concerns the ECT Act No.4 of 2021 was enacted.

3.2.2 Electronic Communications and Transactions, Act 2021(ECT ACT)

The ECT Act modernised Zambia's evidence law by recognising "data messages." The Act provided for the definition of "data message" under **section 3** to mean data generated, sent, received or stored by electronic, optical or similar means and includes, but is not limited to electronic data interchange (EDI), voice, stored record, electronic mail, mobile communications audio and video recordings. In other words this means any message that includes emails, mobile communications, audio and video recordings, and other digital records. **Section 9** ensures that data messages cannot be denied admissibility simply because they are electronic or not in original form. Courts must assess evidential weight by considering reliability, integrity, and the originator's identity. Certified business records are admissible upon production and constitute rebuttable proof.

Furthermore, **section 96** excludes evidence obtained through unlawful interception unless admitted with leave of the court, which must weigh national security and fairness to the accused person.

The Act therefore strengthens the evidentiary value of electronic records while protecting against abuse of surveillance powers. However, it does not sufficiently address the standards on metadata or chain-of-custody.

3.2.3 The Data Protection Act, 2021

The Data Protection Act, 2021 was Zambia's first attempt to regulate and safeguard the collection, processing, storage and sharing of personal data. It establishes the office of the Data Protection Commissioner, tasked with monitoring compliance and protecting data subjects. **Section 4** requires that personal data be processed lawfully, fairly and transparently, reflecting international principle of data minimisation and purpose limitation. **Section 15** requires individual consent with regards to the collection of personal data and grants individuals rights to access, rectify, delete personal data and withdraw consent at any time. **Section 71** restricts cross-border transfer of personal data unless adequate safeguards exist.

Despite these safeguards, critics such as CIPESA[38] note that enforcement remains weak, and the Act does not adequately address overlaps with the Cyber Security and Cyber Crimes Act. Furthermore, the Data Protection Commissioner lacked independence as until recent was being housed under ZICTA, which raised concerns about regulatory capture as its office was not fully autonomous. The Commissioner has since established its own offices independent from ZICTA.

3.2.4 The Cyber Security and Cyber Crimes Act, 2021(Repealed)

The Cyber Security and Cyber Crimes Act 2021 was Zambia's first comprehensive cyber law. It provided for the criminalisation of offences such as hacking, identity theft and cyber fraud. While also, explicitly providing for admissibility of electronic evidence in legal proceedings and establishing of the Central Monitoring and Coordination Centre (CMCC) with broad interception powers. However, civil society criticised the Act for enabling mass surveillance without judicial oversight and for vague offence provisions, partly leading to it repeal and replacement by the Cyber laws of 2025.

3.2.3 The Cyber Security Act No. 3 of 2025 and the Cyber Crimes Act No.4 of 2025

In 2025, Parliament repealed the 2021 law and introduced two separate Acts. While, the Cyber Security Act and the Cyber Crimes Act were enacted to streamline

[38] Organisation for Economic Co-operation and Development (OECD), 'Privacy and Data Protection' (OECD, 2025) https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html accessed on 26 August 2025

governance and provide adequate legal response to cyber threats, several provisions have been criticised for their broad and rights-limiting effects. **Section 5** of the Cyber Crimes Act criminalises the unauthorised disclosure of "critical information". Critical information is broadly defined under **section 3** the Cyber Security Act to include data on public safety, health and national security, inter alia. This effectively restricts the free exchange of ideas or information without State approval. **Section 6** prohibits unauthorised possession of such information, making it an offence to hold information related to public safety, health, economic or national security, unless authorised by the State, while **section 19** criminalises deceptive electronic communications, including "falsifying headers," which could potentially be applied against journalists. Furthermore, **section 21** bans disclosure of investigation details without State consent, carrying up to five years' imprisonment. **Section 22** Prohibits transmitting obscene, vulgar, or indecent electronic data intended to harass or distress, and criminalises disseminating "false" information that causes embarrassment or defamation. Offenders face up to two years' imprisonment. These offences are subjective and open to misuse against dissenting voices.

The **Law Association of Zambia (LAZ)** and other advocacy groups have warned that these provisions risk weaponisation against dissent and press freedom.

3.3 Institutional Framework

1. **ZICTA[39]:** The Zambia Information and Communications Technology Authority (ZICTA) is a statutory body established under the Information and Communication Technologies Act No. 15 of 2009 (ICT) to regulate the Information and Communication Technology sector. ZICTA is also responsible for the regulation the Postal and Courier Services sector as well as providing oversight on Cyber Security in the country. However, its institutional independence is questioned since it operates under ministerial control.
2. **Data Protection Commissioner[40]:** The **Data Protection Commission of Zambia (DPC)**, the authority responsible for ensuring the protection of personal data and promoting the rights of individuals in Zambia. The DPC is created under the **Data Protection Act**.

[39] https://www.zicta.zm/about/about-zicta

[40] https://www.dataprotection.gov.zm/about-us/

3. **Judiciary:** Courts interpret admissibility rules under the **Evidence Act** but lack consistent jurisprudence on digital evidence.
4. **Zambia Police Cybercrime Unit[41]:** Responsible for forensic investigation of cyber offences but hampered by limited expertise and resources.
5. **Civil Society (MISA Zambia, Bloggers of Zambia, CIPESA):** Civil society groups such as CIPESA, MISA Zambia, Bloggers of Zambia, monitor and critique laws for rights violations and advocate for reforms.

3.5 Comparative and Regional Perspectives

- **South Africa's POPIA[42]** provides robust rules on consent, accountability, and enforcement through an independent authority. POPIA is largely based on the European Union's General Data Protection Regulation (GDPR), signifying it's compliance with international standards.
- **Kenya's Data Protection Act, 2019[43]** balances digital rights and enforcement via an autonomous commissioner.
- **EU's General Data Protection Regulation (GDPR, 2018)** offers global best practices, with stringent safeguards on data processing and cross-border transfers.

In contrast, Zambia's framework remains fragmented and enforcement mechanisms weak, leaving citizens vulnerable to privacy violations.

3.6 Challenges and Critiques

- Overbroad **surveillance powers** with minimal judicial oversight.

---

[41] https://zambiapolice.gov.zm/the-fraud-investigations-and-interpol-section/

[42]Protection of Personal Information Act (POPIA) 'POPIA' (South Africa) https://popia.co.za/ accessed on 1st September 2025

[43] Kenya, *Data Protection (General) Regulations, Legal Notice No. 263 of 2021* (Rev-subsidiary legislation under the Data Protection Act, No. 24 of 2019) https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2021/LN263_2021.pdf accessed 1st September 2025

- Weak **enforcement** of the Data Protection Act due to limited resources and institutional overlap.
- Lack of **specific rules** in the Evidence Act on authentication, chain of custody, and metadata.
- **Vague offences** that risk criminalising legitimate online expression.
- Absence of a fully independent **data protection authority**, contrary to regional best practice.

As Ng'ambi (2023) notes, Zambia's cyber laws reflect an "over-securitisation of cyberspace" at the expense of fundamental digital rights.

3.7 Conclusion

Zambia's legal framework on digital privacy and electronic evidence has evolved significantly through the **Evidence Act, Data Protection Act 2021**, **Cyber Security Act 2025** and **Cyber Crimes Act 2025**. While these instruments recognise the importance of digital rights and electronic records, weaknesses remain in enforcement, oversight, and statutory clarity. Comparative experience highlights Zambia's need for stronger safeguards, clearer rules for admissibility of electronic evidence, and an independent data protection regime. These issues set the stage for the next chapter, which analyses how technology continues to challenge and reshape Zambia's legal system.

CHAPTER 4

CRITICAL ANALYSIS OF THE IMPACT OF TECHNOLOGY ON THE ZAMBIAN LEGAL FRAMEWORK

4.1 INTRODUCTION

Technological advancements have fundamentally transformed the ways in which individuals communicate, store information, and interact with institutions. While these innovations present opportunities for efficiency, connectivity, and economic growth, they also introduce unprecedented challenges to legal systems, particularly in the areas of digital privacy and the admissibility of electronic evidence. In Zambia, the rapid adoption of mobile technologies, social media platforms, cloud computing, and advanced surveillance tools has placed increasing pressure on the country's legal framework to adapt in order to safeguard constitutional rights and ensure the integrity of judicial processes.

The core challenge lies in balancing the competing interests of privacy, national security, and justice in a digital environment where personal data can be collected, stored, and transmitted across borders with ease. Emerging technologies such as artificial intelligence, encryption, and big data analytics further complicate this balance by making evidence more difficult to authenticate, while simultaneously expanding the State's capacity for surveillance. These realities test the adequacy of laws such as the Evidence Act, the Electronic Communications and Transactions Act, 2021, the Data Protection Act, 2021, and the Cyber Security Act, 2025, and Cyber Crimes Act, 2025.

This chapter critically analyses how technology has impacted Zambia's legal framework governing digital privacy and electronic evidence. It examines the implications of technological change for privacy protections, the admissibility of electronic records, institutional capacity, and judicial practice. By exploring both the opportunities and the risks that technology presents, the chapter seeks to assess whether Zambia's laws are keeping pace with technological realities or whether they lag behind, leaving gaps that undermine the protection of rights and the administration of justice.

4.2 Technological Advancements and Emerging Challenges

4.2.1 Big Data and Cloud Computing

Big data analytics and cloud computing have revolutionised the storage and processing of information. Big Data simply refers to the very large sets of data that are output by a variety of programs. It can refer to any of a large variety of types of data, and the data sets are usually far too large to peruse or query on a regular computer.[44] Cloud Computing refers to the *processing* of anything, including Big Data Analytics, on the "cloud". The "cloud" is just a set of high-powered servers from one of many providers. They can often view and query large data sets much more quickly than a standard computer could.[45]

The Evidence Act and Electronic Communications and Transactions Act are silent on cross-border electronic records, leaving uncertainty about their admissibility and evidentiary weight. Practitioners such as Nyati[46] observe that cloud-stored data also raises issues of data integrity and chain of custody, since third-party service providers may alter, back up, or delete information beyond local judicial control.

4.2.2 Mobile Technology and Social Media

Technological advancements have broadened the scope of evidence that can be admitted in courts, they have evolved the legal landscape to include digital messages. This has however posed a threat to the privacy of individuals as certain laws have given the authority powers to intercept any data messages in protection of national security and public interest.

Zambia has experienced a surge in mobile internet penetration and social media usage, with platforms such as WhatsApp, Facebook, X (formerly Twitter), and TikTok becoming primary channels of communication. These platforms generate vast amounts of digital data that can be used in both civil and criminal proceedings, from voice notes and images to chat logs.

---

[44] IEEE Computer Society, 'Big Data & Cloud Computing' (Tech News – Trends, 18 February 2020) https://www.computer.org/publications/tech-news/trends/big-data-and-cloud-computing accessed 20/08/2025

[45] Ibid

[46] Interview with Patricia Nyati, Data Protection Law Advocate (Lusaka, 17th October, 2025)

Section 9 of the Electronic Communications and Transactions Act[47] (ECT) provides for the admissibility and evidential weight of a data message, this provision has been fortified by recent court cases such as the Dolomite case[48]. This particular case brought out the fact that data messages carry the same evidential weight as their hardcopy counterpart and thus are admissible in the courts pursuant to the provisions of the ECT Act.

4.2.3 Artificial Intelligence (AI) and Algorithms

The advent of AI-driven tools in data analysis, cyber-security and predictive policing raises both efficiency and ethical concerns. Government agencies in Zambia are gradually exploring AI for digital surveillance, cyber-crime detection as well as day to day operations. While AI enhances productivity and investigative capacity, it raises questions about algorithmic transparency, bias and accountability.

The lack of proper training in AI tool capability and regulation poses a threat to the legal system. For example, if an AI system identifies suspects or analyses digital evidence, how does the court verify the reliability of its processes? In Zambia, the absence of statutory or procedural rules governing the use of AI-generated evidence could deeply undermine the credibility and fairness this is afforded to every trial.

Globally, similar concerns have been raised in the European Union and South Africa, where scholars argue that automated data analysis requires explicit legal safeguards to prevent abuse.

4.2.4 Encryption, Anonymity and Cyber-security Threats

Digital privacy is protected by encryption technologies which make data inaccessible to unauthorised users. However, this can also be a hindrance to law enforcement's ability to access electronic evidence during investigations. The Cyber Security Act[49] empowers authorities to demand decryption or cooperation from service providers. However, the lack of adequate judicial oversight poses a risk of overreach.

---

[47] Act No.4 of 2021

[48] Dolomite Aggregates Limited v Paul Marais (APPEAL NO 2542021) 2024 ZMCA 73 (19 March 2024)

[49] Act No. 3 of 2025

Instances of data breaches and cyber-security incidents pose significant risks to user data on digital platforms in Zambia. The findings highlight the prevalence of data breaches and cyber-security incidents affecting digital platforms in Zambia. Analysis of reported cases revealed instances of unauthorized access, data theft, and security vulnerabilities compromising the confidentiality and integrity of user data (Mwansa & Simuyandi, 2019). Research emphasizes the need for robust cyber-security measures and incident response protocols to mitigate the risks of data breaches and protect user privacy. Furthermore, the implications of data breaches extend beyond individual privacy concerns to encompass broader economic and reputational impacts on affected organizations and stakeholders.[50]

4.3 Impact on the Legal Framework Governing Digital Privacy

Technological advancement has shifted the concept and scope of privacy in Zambia, expanding it beyond traditional notions of physical intrusion into a more complex digital sphere.

4.3.1 Expansion of Surveillance Powers

Digital surveillance technologies innovation such as biometric systems, closed-circuit television (CCTV) and electronic monitoring has increased the State's capacity of surveillance. Surveillance within this context refers to any listening, observing, monitoring, or recording by agents of the state of citizens' conversations, correspondence, or communications without due regard for privacy of citizens. The Cyber Security Act[51] and the Cyber Crimes Act[52] grant broad interception powers to State authorities, particularly through the Central Monitoring and Coordination Centre (CMCC) which is continued as established under the **Section 21** of the Cyber Security Act[53]. These provisions, while aimed at combating cyber-crime, have

[50] Nalumino Moola and Sidney Kawimbe, 'Data Protection Challenges on Digital Platforms: A Case for Zambia' (2024) 12(5) *Global Scientific Journal* https://www.globalscientificjournal.com/researchpaper/Data_Protection_Challenges_on_Digital_Platforms_A_Case_for_Zambia.pdf accessed 20/09/2025

[51] Act No. 3 of 2025

[52] Act No. 4 of 2025

[53] Act No. 3 of 2025

expanded governmental access to private communications without sufficient judicial oversight.

Section 29[54] outlines the legal framework governing the interception of communications by law enforcement officers. It authorises an officer, upon having *reasonable grounds* to believe that an offence has been, is being, or is likely to be committed, to apply *ex parte* to a judge for an interception order. A judge may grant such an order if satisfied that the communication in question relates to the commission of an offence or to the whereabouts of a suspect.

The order may authorise or require actions such as:

- directing an electronic communications service provider to intercept and retain specific communications;
- authorising law enforcement, through the designated Centre, to install interception devices on premises;
- requiring persons to provide necessary information or assistance; and
- imposing conditions to protect third-party interests or facilitate investigations.

An interception order is valid for three months, renewable once for a further three months upon application. Once issued, it must be served on the relevant service provider, who must, within 24 hours, route duplicate communication signals to the Centre for access by law enforcement.

Information obtained under such an order, or under equivalent lawful procedures in a foreign state, is admissible as evidence in court. Furthermore, service providers and their agents are granted immunity from legal action for cooperating with such lawful interception orders.

4.3.2 Data Protection Challenges in the Age of Big Data

The Data Protection Act, 2021 was enacted to safeguard personal information and regulate its processing, storage and transfer. However, the exponential growth of

[54] Ibid

data collection through government databases, e-commerce and digital platforms has exposed critical weaknesses in the Act's enforcement.

The Data Protection Commissioner is the oversight authority which until 2023 was operating under the supervision of the Zambia Information and Communication Technology Authority (ZICTA), compromising its institutional independence. However, this has changed since the establishment of the Data Protection Commission Office making it less likely to create conflict of interest, since ZICTA also regulates service providers that process data.

Data collected in Zambia is usually hosted on servers abroad, making it difficult for regulators to enforce local privacy standards. Moreover, the Act does not adequately address data collected by foreign companies that do not have a physical presence or agency in Zambia, this leaves citizens vulnerable to privacy violations through modern data-driven systems.

4.3.3 The Balance between National Security and Privacy

Technology has intensified the long-standing tension between the protection of privacy and national security. The threat of cyber-attacks and terrorism raise concerns, the Zambian State has increasingly relied on the digital surveillance and interception to protect public order. The rule of law is undermined by the absence of independent judicial authorisation and clear procedural safeguards even though these measures are legitimate in principle.

International frameworks such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) advocate for oversight mechanisms that guarantee accountability and proportionality in surveillance activities. Zambia, although a signatory, has is yet to domesticate the Convention's principles. Consequently, the country's cyber laws operate without an independent data protection authority or a robust system of checks and balances.

4.3.4 Public Awareness and Institutional Capacity

The protection of digital privacy is not solely a legal issue but also one of awareness and institutional competence. Many Zambian citizens remain unaware of their rights under the Data Protection Act, while institutions responsible for enforcement such as

ZICTA and the Data Protection Commissioner, lack sufficient technical expertise and resources to audit data controllers or investigate breaches. This limited capacity undermines effective implementation and leaves individuals without practical remedies when their digital rights are violated.

4.4 Impact of Technology on the Legal Framework Governing Electronic Evidence

Technology has revolutionised how evidence is generated, stored, and presented in legal proceedings. The traditional approach to documentary evidence, rooted in physical records, has been replaced by dynamic digital data capable of rapid alteration and mass replication. The biggest challenges faced by Zambia's legal framework, even though it has gradually recognised electronic evidence through instruments such as the Evidence Act, Electronic Communications and Transactions Act, 2021 and the Cyber Crimes Act, 2025, is the pace of the legislative and procedural adaptation remains slow compared to technological change. As a result, questions of authenticity, integrity and admissibility continue to challenge both courts and law enforcement agencies.

4.4.1 Transformation of Evidence through Technology

The digitization of communication and record-keeping has increased the variety of evidence used in litigation. Emails, text messages, social media posts, digital photographs, GPS logs, and CCTV footage are now essential materials. Courts in both civil and criminal cases increasingly rely on electronic evidence to resolve disputes. However, the temporary and easily changeable nature of digital data requires strict procedures for authentication and preservation.

Technological tools like encryption, file compression, and cloud storage make these processes more complicated. Evidence may be scattered across different devices or locations, making it hard to trace the chain of custody. Without clear procedural guidelines, courts in Zambia risk inconsistent handling of this evidence, which can undermine the fairness and predictability of judicial outcomes.

4.4.2 The Evidentiary Value of Data Messages under the ECT Act, 2021

The Electronic Communications and Transactions Act (ECT Act)[55] marked a significant advancement by clearly accepting data messages as valid evidence. **Section 9(1)**[56] prohibits courts from dismissing a data message simply because it is electronic or lacks an original format. **Section 9(3)**[57] instructs courts to evaluate reliability by considering how the data was created, stored, communicated, and verified. **Section 9(4)**[58] states that certified business records in the form of data messages are admissible when presented and serve as rebuttable evidence of the facts they include. **Section 96**[59] establishes that illegally intercepted communications are not admissible unless the court allows it, balancing evidentiary value with fairness and national security concerns.

These provisions show an effort to modernize Zambia's evidentiary framework. However, in reality, courts often lack the technical skills to assess the reliability of electronic systems or interpret digital forensic reports. This shortcoming weakens the Act's enforcement and diminishes the possible advantages of digital evidence in court proceedings.

4.4.3 Authentication and Chain of Custody Challenges

A major challenge in the admissibility of electronic evidence is proving authenticity—confirming that a digital record is genuine. Because electronic data can be easily changed or fabricated, keeping an unbroken chain of custody is crucial. However, Zambia's Evidence Act (Cap. 43) does not provide detailed guidance on authentication standards, digital signatures, or forensic certification.

Law enforcement agencies, including the Zambia Police Cybercrime Unit, often lack specialized tools for forensic imaging, metadata extraction, and secure preservation. As a result, vital evidence may be compromised or deemed inadmissible. The lack of uniform procedures, such as those in South Africa's Electronic Communications and Transactions Act, 2002 or Kenya's Evidence (Amendment) Act, 2016, creates uncertainty and erodes public trust in the treatment of digital evidence.

---

[55] Act No of 2021

[56] Ibid

[57] Ibid

[58] Ibid

[59] Ibid

4.4.4 Cloud Computing, Cross-Border Data, and Jurisdictional Complexities

The growth of cloud computing has introduced jurisdictional difficulties in evidence collection. Many companies in Zambia, including banks and government agencies, store data on servers located abroad. Accessing this information for investigation or court purposes often requires mutual legal assistance (MLA) with other countries, which can be a slow and bureaucratic process.

Current Zambian laws do not clearly address cross-border electronic evidence or outline procedures for obtaining digital records stored overseas.[60] This issue is especially problematic in cybercrime investigations involving international actors, where timely access to data is crucial. Models like the Budapest Convention on Cybercrime offer clearer frameworks for cross-border collaboration, but Zambia has not yet domesticated these methods.

4.4.5 Admissibility of Social Media and Mobile Evidence

The growing reliance on WhatsApp messages, text records, and social media content in both criminal and civil trials shows that everyday technology has become a key source of evidence. However, challenges emerge regarding the verification of authorship and context. Screenshots and forwarded messages are often submitted in court, yet many lack metadata or timestamps that verify their origin.

Courts have allowed such evidence on a case-by-case basis, but without consistent standards, results can vary greatly. Additionally, the Cyber Crimes Act 2025, which criminalizes “deceptive” or “false” communications, might discourage individuals from presenting digital communications as evidence due to fear of potential legal repercussions.

4.4.6 Digital Forensics and Institutional Capacity

The use of forensic science in digital investigations remains underdeveloped in Zambia. The Zambia Police Forensic Laboratory and the ZICTA Cyber-security Unit handle most electronic evidence examinations but face acute resource shortages and skill gaps. Without advanced digital forensics capabilities, investigations risk

[60] CIPESA, Zambia: Insights into the Data Protection Act 2021 (CIPESA 2021) https://cipesa.org/wp-content/files/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf accessed 10 April 2025.

dependence on manual methods or external assistance, compromising both efficiency and evidential reliability.

Training judges, prosecutors, and defence attorneys on handling digital evidence is equally important. Scholars such as Nyati[61], emphasise that without judicial literacy in information technology, courts cannot effectively assess the reliability of digital forensic reports or the credibility of expert witnesses.

4.4.7 Comparative and International Standards

Other countries have implemented forward-thinking approaches that Zambia can learn from. South Africa incorporates digital evidence handling in its Law of Evidence Amendment Act, supported by technical guidelines for electronic discovery. Kenya has clear procedures for authenticating electronic records under **Section 106B** of its Evidence Act[62]. The European Union's eIDAS Regulation treats electronic signatures and timestamps as equivalent to handwritten ones, ensuring reliability and cross-border acceptance.

Zambia's legal framework, while improving, still lacks equivalent procedural clarity. Adopting such standards could greatly enhance the admissibility and judicial confidence in electronic evidence.

4.4.8 Summary of Findings

Technology has significantly influenced the evidentiary landscape in Zambia by introducing new forms of data and communication that traditional laws were not meant to govern. Although the ECT Act 2021 and the Cyber Crimes Act 2025 recognize electronic records, issues remain with authentication, chain of custody, and forensic standards. Cross-border data storage, low institutional capacity, and inadequate judicial training further limit the effective use of digital evidence. Therefore, Zambia's legal system acknowledges electronic evidence in theory but struggles with its practical management, revealing a pressing need for procedural reforms and capability building within the judicial system.

4.5 Practical and Institutional Implications

[61] Interview with Patricia Nyati, Data Protection Law Advocate (Lusaka, 17th October, 2025)

[62] Cap 80 of the Laws of Kenya

The success of Zambia's legal framework on digital privacy and electronic evidence relies on both legislation and institutional capacity for effective implementation. While laws like the Data Protection Act 2021, Electronic Communications and Transactions Act 2021, and the Cyber Security Act 2025 and Cyber Crimes Act 2025 mark important legal progress, their enforcement has been inconsistent. Institutions responsible for overseeing digital privacy and electronic evidence face limitations in resources, expertise, and independence, which restrict their responsiveness to the rapidly changing technological environment[63].

4.5.1 The Role and Limitations of ZICTA

The Zambia Information and Communications Technology Authority (ZICTA) is the main regulatory body for ICTs, data protection, and cyber-security. It supervises electronic communication service providers, enforces compliance with the ECT Act and the Data Protection Act, the function to oversee the implementation of cyber security related functions assigned to it under the ICT Act, and collaborate with other relevant institutions while carrying out its duties.

However, ZICTA's dual role as both regulator and enforcer creates structural conflicts. While it is meant to protect citizens' privacy, it also implements State surveillance infrastructure through the CMCC. This conflict undermines public trust and raises accountability issues. Furthermore, scholars like Mambwe (2023) argue that ZICTA lacks full independence since it operates under the Ministry of Technology and Science and follows ministerial guidance. Without operational autonomy and technical capacity, ZICTA's effectiveness in safeguarding data privacy remains limited.

4.5.2 The Data Protection Commissioner

The Data Protection Act 2021 created the Data Protection Commissioner to oversee data controllers, ensure lawful handling of personal information, and address complaints. However, the Commissioner's office is administratively located within ZICTA, which limits its independence and enforcement power.

[63] Interview with Patricia Nyati, Data Protection Law Advocate (Lusaka, 17th October, 2025)

With the rapid rise of digital platforms, online banking, and e-governance systems, the amount of personal data processed in Zambia has surpassed the Commissioner's ability to monitor compliance. The lack of strong investigation powers, staff training, and technical audit mechanisms has led to minimal enforcement of data protection duties. As a result, both private and public institutions continue to gather and process personal data with little oversight, weakening privacy protections in practice.

4.5.3 Judiciary and the Adjudication of Digital Evidence

The judiciary plays a vital role in interpreting and enforcing laws regarding electronic evidence and digital privacy. However, courts in Zambia face challenges with technical knowledge, procedural clarity, and forensic understanding of digital materials. Many judges and magistrates lack specialized education in digital forensics, metadata analysis, or the verification of electronic communications.

This knowledge gap often leads to inconsistent decisions on the admissibility of electronic evidence. For instance, while some courts accept screenshots and electronic communications, others reject similar evidence due to lack of authentication. The judiciary's reliance on expert witnesses—often from outside government agencies—adds complexity to proceedings, as unclear evidentiary standards can result in conflicting expert opinions.

4.5.4 The Zambia Police Cybercrime and Digital Forensics Units

The Zambia Police Cybercrime Unit, established under the Cyber Crimes Act[64], is tasked with investigating cyber offenses and managing electronic evidence. However, the Unit suffers from on-going underfunding, limited access to advanced forensic tools, and a shortage of personnel trained in cyber forensics. Investigations involving encrypted data, cloud storage, or international digital transactions are especially difficult, often needing international support. This dependency slows investigations and can hurt the chain of custody for electronic evidence. Further, poor collaboration between the police, ZICTA, and the judiciary leads to procedural inconsistencies that can threaten prosecutions.

[64] Act No. 3 of 2025

4.5.5 Civil Society and Public Advocacy

Civil society organizations (CSOs) such as the Media Institute of Southern Africa (MISA) Zambia, Bloggers of Zambia, and the Centre for Internet and Society have taken on important roles in advocating for digital rights and privacy. These groups have openly criticized aspects of the Cyber Crimes Act 2025 that penalize “false information” and grant broad surveillance powers without judicial oversight.

However, CSOs face mounting pressure and struggle for access to policymaking discussions. The lack of multi-stakeholder engagement in drafting cyber laws has further eroded public confidence in the government’s commitment to balance privacy and security. Despite these hurdles, civil society continues to be vital in raising awareness, promoting digital literacy, and pushing for legal reforms that align with regional and international standards.

4.5.6 Inter-Agency Coordination and Policy Coherence

Effective digital governance requires collaboration among various institutions, including ZICTA, the Data Protection Commissioner, the Judiciary, the Zambia Police, and the Ministry of Justice. However, there is limited collaboration among these bodies, leading to overlapping responsibilities and fragmented policies.

For example, while ZICTA manages both cyber-security and data protection, the police focus on cybercrime investigations, and the judiciary decides on the admissibility of digital evidence. Without a central coordination system or clear data-sharing protocols, enforcing privacy and evidence laws remains unpredictable. Additionally, the absence of a national digital evidence management policy or cyber forensics framework limits the ability of institutions to standardize how they collect, preserve, and present electronic evidence.

4.5.7 Summary of Institutional Implications

The institutional setup governing digital privacy and electronic evidence in Zambia reflects both progress and on-going weaknesses. The establishment of specific laws and regulatory bodies shows an acknowledgment of technological realities. However, insufficient technical expertise, limited funding, and lack of independence have restricted these bodies' effectiveness.

ZICTA’s dual role as regulator and enforcer, the Data Protection Commissioner’s weak capacity, the judiciary’s limited digital knowledge, and the police’s lack of forensic infrastructure all hinder robust digital governance. Strengthening inter-agency collaboration, enhancing capacity, and ensuring independence are therefore crucial for Zambia to effectively manage the relationship between technology, privacy, and evidence.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

This final chapter sums up the main findings and conclusions based on the research objectives. It offers practical and policy recommendations to help strengthen Zambia's legal and institutional framework for digital privacy and electronic evidence as technology advances. These suggestions address the challenges found in the study and use lessons from other countries for comparison.

5.1 General Conclusion and Findings

Advances in technology have changed both the opportunities and risks in digital communication and information management. While Zambia's laws have slowly adapted to include electronic evidence and data protection, they have struggled to keep up with the fast pace and complexity of new technologies.

Zambia's current laws focus more on security and surveillance than on protecting individual privacy. This creates an imbalance that weakens constitutional rights under Articles 17. The lack of clear rules for collecting and verifying electronic evidence also affects the reliability of the courts. The research suggests that Zambia should take a proactive approach, planning ahead for technological changes and making privacy protection a core part of digital governance.

5.2 Summary of Chapters

The study had three main goals: to explore what digital privacy and electronic evidence mean, to review the laws in Zambia that cover these topics and to look at how technology affects those laws.

Chapter One gives the background of the study and explains the main problem: how law and technology meet, and what this means for digital privacy and electronic evidence in Zambia. It points out the gap between new technologies and current

legal protections. This chapter sets the stage for the rest of the study by outlining the objectives, research questions, and why the topic matters.

Chapter Two looks at the main ideas and theories behind digital privacy and electronic evidence. It shows that digital privacy is not just about keeping secrets, but also about controlling personal information and preventing misuse. The chapter defines electronic evidence as any digital information that can be used in court. It also reviews different scholars' definitions and explains how new technology has made legal ideas about privacy, ownership, and evidence more complex.

Chapter Three reviews Zambia's main laws on digital privacy and electronic evidence. It finds that while several acts form the legal foundation, their enforcement is inconsistent. These laws recognize electronic evidence and privacy, but they suffer from unclear definitions, weak enforcement, overlapping responsibilities, and not enough technical know-how. The chapter also points out that some parts of the Cyber Security Act and Cyber Crimes Acts of 2025 could limit constitutional rights.

Chapter Four examines how new technologies like AI, big data, cloud computing, and social media have changed privacy and the use of electronic evidence. It finds that technology is moving faster than legal reforms, creating gaps in data protection, evidence verification, and surveillance oversight. Weaknesses in institutions like ZICTA, the Data Protection Commissioner, the Judiciary, and the Police Cybercrime Unit make enforcement difficult. The chapter concludes that although Zambia's laws now address digital issues, the institutions and procedures are not fully ready for today's challenges.

5.3 Recommendations

5.3.1 Legislative Reforms

1. Amend the Data Protection Act No.3 of 2021

It is important to clearly define what counts as "personal use" to stop this exemption from being misused for privacy violations. There is also an urgent need to create and issue detailed regulations to put the Act into practice, especially on data subject rights, security breach notifications, and handling sensitive data like biometrics,

health, and genetic information. The law should also include rules for automated decision-making and profiling, making sure people have the right to an explanation and a human review.

2. Refine the Cyber Security Act No.3 of 2025

The definition of “critical information” should be made more specific so it is clear, focused, and fits the needs of a democratic society. Oversight should be improved by requiring court approval before interception and surveillance, and by having a review afterward by a group that includes civil society members.

3. Amend the Electronic Communications and Transactions Act 2021

Set up clear legal standards for verifying new types of evidence, such as social media posts, blockchain records, and Deepfake media. Also, provide simple and technology-neutral definitions for all kinds of electronic evidence.

5.3.2 Procedural and Institutional Reforms

1. Develop Digital Forensics Standard Operating Procedures (SOPs)

The Judiciary and Zambia Police Service should work together to create and use required procedures for handling electronic evidence. These should include clear steps for keeping a secure chain of custody, using write-blockers, checking hash values and storing evidence properly.

2. Enhance Judicial Capacity and Expertise

Provide ongoing training for judges and magistrates on the technical side of digital evidence, new technologies like AI and Deepfakes, and the legal rules for deciding if this evidence can be used and how much it should count.

3. Strengthen the Data Protection Commission

Make sure the Data Protection Commissioner has enough funding, technical skills, and independence to properly monitor compliance, investigate complaints, and enforce penalties for breaking the Data Protection Act.

5.3.3 Institutional Strengthening

Strengthen ZICTA's independence and skills by making it a fully independent regulator, free from government influence, and by improving its technical ability to monitor and enforce rules.

Increase skills in the Judiciary and law enforcement by offering ongoing training in digital forensics, cybercrime investigation, and evidence analysis for judges, prosecutors, and police officers.

Set up a national digital forensics lab as a central, accredited place for all government agencies to handle, store, and verify electronic evidence.

5.4.3 Policy and Procedural Improvements

Create a national framework for electronic evidence to standardize how it is collected, stored, and presented making sure the process is the same everywhere.

Encourage input from civil society, universities, and businesses in making policies to ensure digital governance is inclusive and respects rights.

Raise public awareness by running national education campaigns about digital rights, data privacy, and safe online habits.

5.4.4 Regional and Comparative Collaboration

Work with neighboring countries and international partners on digital forensics, sharing data across borders, and prosecuting cybercrime.

Join global digital governance groups to keep up with changing international standards on privacy and electronic evidence.

5.5 Final Remarks

The journey of this research has traversed the complex and rapidly evolving landscape where law and technology converge. It has revealed that the digital age is not merely a new context for applying old rules, but a paradigm shift that demands a fundamental re-imagining of legal principles. The Zambian experience, as examined in this study, is a microcosm of a global challenge: the struggle to reconcile the boundless potential of technology with the enduring need to protect human dignity, privacy, and justice.

The findings of this research lead to an inescapable conclusion: the current trajectory of Zambia's legal and institutional framework is one of reactive adaptation, often lagging perilously behind technological reality. This lag creates a dangerous vacuum where state surveillance powers can expand without robust oversight, where personal data becomes a commodity vulnerable to exploitation, and where the very evidence that secures convictions or resolves disputes can be compromised by a lack of technical rigor. The consequence is not merely legal inefficiency; it is a tangible erosion of public trust in the digital ecosystem and the judicial system that governs it.

Therefore, the path forward cannot be one of incremental adjustments alone. It requires a conscious, strategic, and principled commitment to building a proactive and resilient digital legal order. This entails moving beyond viewing technology as a mere disruptor to be controlled and instead embracing it as a domain to be thoughtfully governed. The bedrock of this new order must be a steadfast adherence to constitutional values, where the right to privacy is not treated as a secondary concern to security, but as its essential foundation. The integrity of electronic evidence must be upheld not as a technical formality, but as a cornerstone of the right to a fair trial.

The recommendations put forth in this chapter, from legislative refinement and institutional capacity-building to public awareness and regional collaboration, are not isolated fixes. They are interconnected components of a holistic strategy. Empowering the Data Protection Commission, equipping the judiciary with digital literacy, and establishing clear forensic standards are all part of forging a system that is both technologically competent and ethically grounded.

As Zambia continues its digital transformation, the choices made today will define its future as a society. Will it be one where technology empowers citizens and enhances justice, or one where it becomes a tool for control and inequality? The answer lies in the courage to enact reforms that prioritize human rights, the wisdom to invest in the institutions that uphold them, and the foresight to anticipate the next wave of technological change. By anchoring its digital future in the principles of transparency, accountability, and justice, Zambia can ensure that its legal framework does not just respond to the digital age, but actively shapes it for the benefit of all its citizens.

BIBLOGRAPHY

STATUTES

Constitution of Zambia, Act 17 of 1996

Cyber Crimes Act No.4 of 2025

Cyber Security Act No.3 of 2025

Cyber Security and Cyber Crimes Act No. 2 of 2021

Data Protection Act No. of 2021

Electronic and Communication Technologies Act No.4 of 2021

Evidence Act Chapter 43 of the Laws of Zambia

BOOKS

Creswell JW, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th edn, Sage Publications 2014).

CASES

Bentry Siamalambwa v Magna Mining Limited (2022/HPC/0624) [2024] ZMHC 136 (1 February 2024)

Dolomite Aggregates Limited v Paul Marais (APPEAL NO 2542021) 2024 ZMCA 73 (19 March 2024)

JOURNALS

Hung H, Wong Y.H. "Information transparency and digital privacy protection: are they mutually exclusive in the provision of e-services?" (2009) Journal of Services Marketing 23

Moola N and Kawimbe S, 'Data Protection Challenges on Digital Platforms: A Case for Zambia' (2024) 12(5) *Global Scientific Journal* 61 https://www.globalscientificjournal.com/researchpaper/Data_Protection_Challenges_on_Digital_Platforms_A_Case_for_Zambia.pdf accessed 8 April 2025

Mulenga C, 'Assessing Zambia's Legal Framework on Cybercrime and Electronic Evidence' (2021) *Zambia Law Journal* 15(2) 45

Soko J, 'Social Engineering Attacks via AI Chatbots in Zambia' (2021) 4(1) *Zambia Information Security Journal* 55.

ARTICLES

Drejer C, Riegler MA, Halvorsen P, Johnson MS, and Baugerud GA, 'Livestreaming Technology and Online Child Sexual Exploitation and Abuse: A Scoping Review' (2023) 25(1) *Trauma, Violence, & Abuse* 260

INTERNET SOURCES

BBC News, 'Zambia's Cybersecurity Law Sparks Free Speech Concerns' (12 March 2024) https://www.bbc.com/news/articles/cj451xd0ezwo accessed 16 April 2025

CIPESA, *Zambia: Insights into the Data Protection Act 2021* (CIPESA 2021) https://cipesa.org/wp-content/files/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf accessed 10 April 2025

IBM, 'What Is the Internet of Things (IoT)?' (12 May 2023) https://www.ibm.com/think/topics/internet-of-things accessed 8 April 2025

IEEE Computer Society, 'Big Data & Cloud Computing' (Tech News – Trends, 18 February 2020) https://www.computer.org/publications/tech-news/trends/big-data-and-cloud-computing accessed 20 September 2025

Lin T, 'Challenges and Legislative Responses to Privacy Protection in the Digital Age' (2025) *Lecture Notes in Education Psychology and Public Media* vol 95, 21–30 https://doi.org/10.54254/2753-7048/2025.23023 accessed 15 August 2025

Phiri S and Zorro, 'Zambia Digital Rights Landscape Report' in Roberts T (ed), *Digital Rights in Closing Civic Space: Lessons from Ten African Countries* (Institute of Development Studies 2021) 61–84 https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/15964/Zambia_Report.pdf accessed 8 April 2025.

Protection of Personal Information Act (POPIA) 'POPIA' (South Africa) https://popia.co.za/

Reuters, *From AI chatbots to social media: data presentation gets a little more complicated* (11 August 2025) https://www.reuters.com/legal/legalindustry/ai-chatbots-social-media-data-presentation-gets-little-more-complicated-2025-08-11/ accessed 12 August 2025

Stanfield AR, *The Authentication of Electronic Evidence* (PhD thesis, Queensland University of Technology, 2016) https://eprints.qut.edu.au/93021/ accessed 12 August 2025

Stryker C and Kavlakoglu E, 'What Is Artificial Intelligence (AI)?' (IBM, 9 August 2024) https://www.ibm.com/think/topics/artificial-intelligence accessed 8 April 2025

Van den Hoven J, Blaauw M, Pieters W, and Warnier M, 'Privacy and Information Technology' (Stanford Encyclopaedia of Philosophy, 2020) https://plato.stanford.edu/entries/it-privacy/#ImpInfTecPri accessed 16 April 2025

INTERVIEW

Nyati Patricia, interview by Chilufya Chanda, Lusaka, Zambia, 10/17/2025

UNIVERSITY of LUSAKA

SCHOOL OF LAW

L400B / Dissertation II – DIRECTED RESEARCH (OBLIGATORY ESSAY)

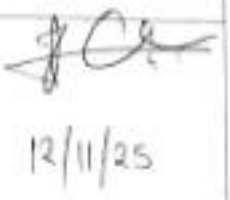
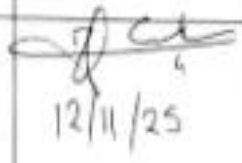
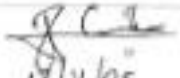
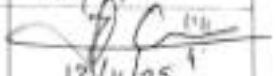
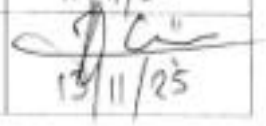
RESEARCH CLEARANCE FORM

NAME: Chilufya Chanda STUDENT NUMBER: LLB1611082

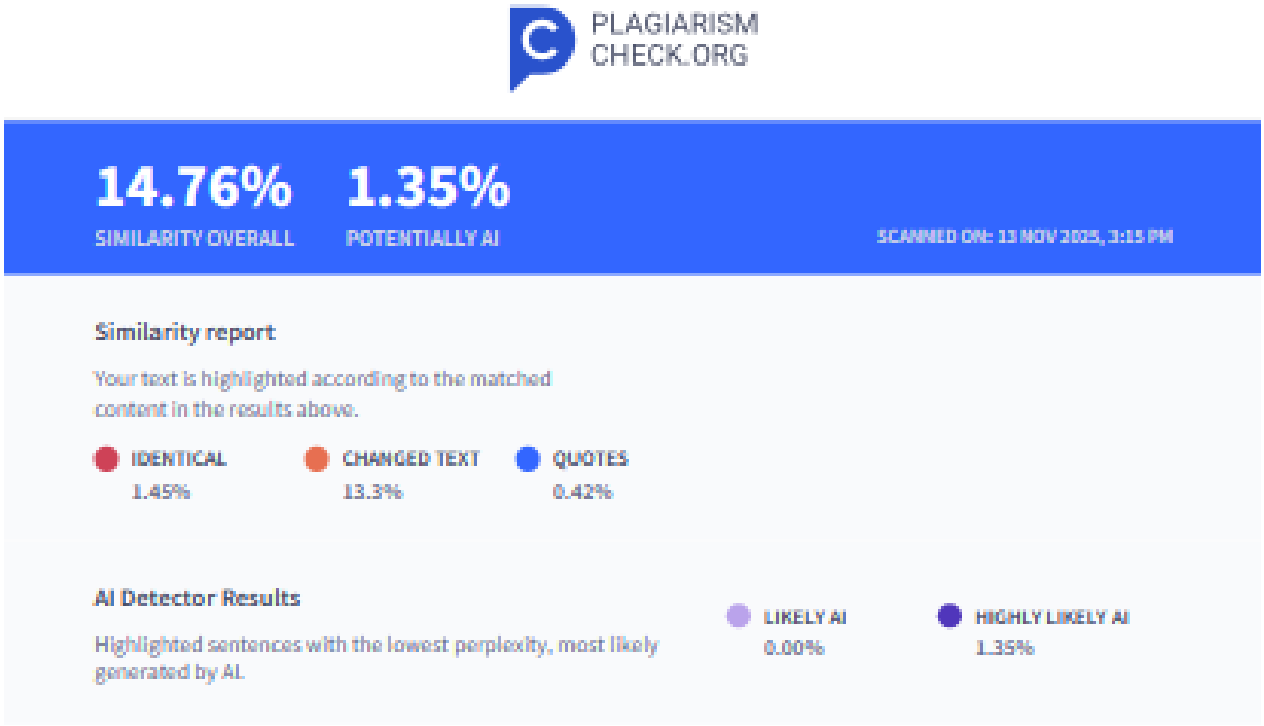
SUPERVISOR: K.K Mwauluka TOPIC: The Impact Of Technology On The Law: Examining Digital Privacy And Electronic Evidence.

Stage	Supervisor's Comments	Supervisor's Signature & Date	Student's Signature & Date
Research Proposal	APPROVED		05/08/25
Chapter 1 – Introduction	APPROVED		05/08/25
Chapter 2 –	APPROVED		28/08/25
Chapter 3 –	APPROVED		23/09/25
Chapter 4 –	APPROVED		15/10/25

Page 1 of 2

Chapter 5 – Conclusions & Recommendations	APPROVED		
Abstract, Table of Contents, Bibliography and Appendices	APPROVED		
First Draft	APPROVED		
Second Draft	APPROVED		
Final Draft	APPROVED		

**Please attach this form to the back of your dissertation at the end of the research, before submission via the Moodle e-learning platform.*



Report #29951105

SCHOOL OF LAW THE IMPACT OF TECHNOLOGY ON THE LAW: EXAMINING DIGITAL PRIVACY AND ELECTRONIC EVIDENCE. By: CHILUFYA CHANDA LLB1611082 An obligatory essay submitted to the University of Lusaka in partial fulfillment of the requirements for the award of the degree of Bachelor of Laws (LLB). 2025 DECLARATION I, CHIUFYA CHANDA, do declare that this dissertation titled THE IMPACT OF TECHNOLOGY ON THE LAW: EXAMINING DIGITAL PRIVACY AND ELECTRONIC EVIDENCE. Which is hereby submitted to the School of Law at the University of Lusaka as part of the requirements for the award of the Bachelor of Laws (LLB) degree, is my original work and has not previously been submitted for the award of a degree at this or any other tertiary institution. The sources that have been used or quoted have been indicated and duly a cknowledged as complete reference. Signature.....