EXPLORING ROLE OF MEDIA CONVERGENCE IN INTRUSION OF PRIVACY: EXPERIENCES OF REGULAR INTERNET USERS IN NAIROBI CITY COUNTY, KENYA

KUNGU NANCY WANJIRU

(MSC. MASS COMMUNICATION)

M88/28111/2014

A RESEARCH THESIS SUBMITTED FOR THE AWARD OF THE DEGREE OF DOCTOR OF PHILOSOPHY(COMMUNICATION AND MEDIA STUDIES) IN THE SCHOOL OF CREATIVE AND PERFORMING ARTS, FILM AND MEDIA STUDIES OF KENYATTA UNIVERSITY

MAY 2021

DECLARATION

This thesis is my original work and has not been presented for a degree in any other University or any other award.

Signature_____Date_____

KUNGU NANCY. W (M88/28111/2014)

Department of Communication, Media, Film and Theatre Studies

SUPERVISORS:

We confirm that the work reported in this thesis was carried out by the candidate under our supervision as University Supervisors:

Signature_____Date_____

DR. GEORGE NGUGI KING'ARA

Department of Communication, Media, Film and Theatre Studies

Kenyatta University

Signature_____Date_____

PROF. JOHN MUGUBI

Department of Communication, Media, Film and Theatre Studies

Kenyatta University

DEDICATION

This thesis is dedicated to my late dad, John Kungu, and my dear mum, Wanja Kungu.

ACKNOWLEDGEMENTS

Special gratitude goes to my study supervisors: Dr. George Ngugi King'ara and Prof. John Mugubi of Kenyatta University. You provided immense inputs into this research. Thank you for the unfailing academic guidance you offered at every stage of this study.

I thank all the seven institutions where this study was conducted. I wish to thank all the key respondents from the Media Council of Kenya (MCK), the Communications Authority of Kenya (CA), the ICT Authority of Kenya (ICTA). Amidst tight schedules and duties, you sacrificed time and space to participate in this study. I particularly acknowledge your willingness to share your expertise in this study. Much appreciation also goes to the FGD participants from Kenyatta University, Multimedia University (Nairobi CBD Campus), African Nazarene University (Nairobi Campus) and Kenya Methodist University (Nairobi Campus). This study would not have been possible without your participation.

To Richard and Macharia, I appreciate your respective roles in preparation and coordination during data collection.

To my family-Thank you for your material and moral support. I sincerely appreciate the insights you provided throughout the journey. God bless you!

TABLE OF CONTENTS

DECLARATION ..... **ii**
DEDICATION ..... **iii**
ACKNOWLEDGEMENTS ..... **iv**
LIST OF TABLES ..... **ix**
LIST OF FIGURES ..... **x**
ABBREVIATIONS AND ACRONYMS ..... **xi**
OPERATIONAL DEFINITION OF TERMS ..... **xiii**
ABSTRACT ..... **xv**
CHAPTER ONE: INTRODUCTION TO THE STUDY 1
1.1 Introduction 1
1.2 Background of the Study 3
1.3 Statement of the Problem 7
1.4 Purpose of the Study 7
1.5 Research Objectives 8
1.6 Research Questions 8
1.7 Assumptions of the Study 9
1.8 Justification of the Study 9
1.9 Scope of the Study 10
1.10 Limitations of the Study 10
CHAPTER TWO: LITERATURE REVIEW AND THEORETICAL FRAMEWORK 12
2.1 Introduction 12
2.2 Multimediality and Proliferation of Content on Private Information 12
2.3 Hypertextuality and News of Shock, Violence, Crime and Sexual Assault 15
2.4 Interactivity and Intrusion of Bereavement and Family Grief 17
2.5 Mitigating Infringements of Privacy 19
2.6 Research Gap 22
2.7 Theoretical Framework 23
2.8 Conceptual Framework 25
2.9 Research Variables 26
2.9.1 Independent variable 26

2.9.2 Dependent variable 28
2.9.3 Intervening Variables 28
2.10 Conclusion 31
CHAPTER THREE: RESEARCH METHODOLOGY 32
3.1 Introduction 32
3.2 Research Methodology 32
3.3 Research Design 32
3.4 Target Population 33
3.5 Sampling Procedure 33
3.5.1 Purposive Homogeneous Sampling 33
3.5.2 Purposive Expert Sampling 34
3.6 Sample Size 34
3.7 Inclusion and Exclusion Criteria 36
3.8 Data Collection Instruments 36
3.8.1 Discussion Guides 36
3.8.2 Interview Guides 37
3.9 Data Collection Techniques 37
3.10 Validity and Reliability 37
3.11 Data Analysis 38
3.12 Logistical and Ethical Considerations 39
3.13 Conclusion 39
CHAPTER FOUR: DATA ANALYSIS AND DISCUSSION OF FINDINGS 40
4.1 Introduction 40
4.1.2 The FGD Participants 40
4.3 Multimediality and Proliferation of Private Information 41
4.3.1 Multimedia Devices Used for Internet Activities 41
4.3.2 Functions Performed by Multimedia Devices 42
4.3.3 Private Content Encountered on the Social Sites 44
4.3.4 Internet Applications and Tools Attributed to Intrusion of Privacy 47
4.3.5 Internet Activities Escalating Invasion of Privacy 48
4.3.6 Nature of Private Data Accessed on the Internet Protocol 52
4.4 Hypertexuality and News of Shock, Violence, Crime and Sexual Assaults 57

4.4.1 Publication of News of Shock 58
4.4.2 Acts of Violence and Crime 60
4.4.3 Publication of Content on Sexual Assault 63
4.5 Interactivity and Intrusion on Grief 66
4.5.1 Nature of the Cyberspace that Supports Real-time Interactivity 67
4.5.2 Internet Activities Intruding on Bereavement and Grief 70
4. 6 Conclusion 77
CHAPTER FIVE: STRATEGIES FOR MITIGATING PRIVACY INFRINGEMENTS 79
5.1 Introduction 79
5.2 Prevalent Privacy Issues Arising from Internet Usage 81
5.2.1 Harvesting of Personal Data 81
5.2.2 Disclosure of Confidential Information 86
5.2.3 Susceptibility of Social Sites to Cyber Attacks 89
5.2.4 Proliferation of Fake News 91
5.3 Factors Escalating Infringement of Privacy 93
5.3.1 Tracking of Users on the Internet 93
5.3.2 Online Anonymity 94
5.3.3 Proliferation of Unregulated Social Sites. 96
5.4. Factors Limiting Protection of Privacy on the IP 98
5.4.1 Internet User Vulnerability 98
5.4.2 Surveillance 100
5.4.3 Data Storage and Portable Media 102
5.4.4 The Need to Access Information 103
5.5 The Aspects of the Internet Undermining Control of the IP 105
5.5.1 Searchability of Virtual Networks 105
5.5.2 Internet Penetration and Access 107
5. 6 Mitigation: Guarding Against Online Privacy Infringement 110
5.6.1 Legislation and Policy Making 110
5.6.2 Enforcement of Compliance to Regulation and Policy 113
5.6.3 Access Restriction 120
5.6.4 Data Minimization 123

5.6.5 Internet User-skills and Awareness 125
5.7 Conclusion 131
CHAPTER SIX: SUMMARY, CONCLUSION AND RECOMMENDATIONS ... 133
6.1 Introduction 133
6.2 Summary of the Research Findings 133
6.2.1 The Role of Multimediality and proliferation of Private Information 133
6.2.2 Hypertexuality and Shocking News, Violence, Crime and Sexual Assault. .. 134
6.2.3 Interactivity and Intrusion on Bereavement and Grief 135
6.2.4 Strategies for Mitigating Infringements of Privacy 135
6.3 Study Conclusions 138
6.4 Recommendations of the Study 139
6.4.1 Recommendations for Policy 139
6.4.2 Recommendations for Practice 139
6.4.3 Recommendations for Research 140
REFERENCES 141
APPENDICES 155
APPENDIX I: Letter of Introduction 155
APPENDIX II: Discussion Guide for Focus Groups 156
APPENDIX III: Interview Guide for Key Respondents 158
APPENDIX IV: Transcripts from Participants 159
APPENDIX V: Research Authorization Documents 163

LIST OF TABLES

Table 4.1: Functions Performed by the Devices 43
Table 4.2: Internet Activities and Invasion of Privacy 57
Table: 4.3: News of Shock, Acts of Violence, Crime and Sexual Assault 70
Table 4.4: Aspects of Media Convergence that Support Interactivity 77
Table 5.1: Interview Response Rate 79
Table 5.2 Respondents' Identity Codes 80
Table 5.3: Prevalent Privacy Issues Related to Internet Usage 92
Table 5.4: Control and Regulation of Online Platforms 109
Table 5.5: Strategies for Mitigating Violation of Online Privacy 130

LIST OF FIGURES

Figure 2.1: Conceptual Framework 26

ABBREVIATIONS AND ACRONYMS

The following abbreviations and acronyms have been used in this Thesis:

2G	-	2nd Generation
3G	-	3rd Generation
4G	-	4th Generation
AMWIK	-	Association of Media Women in Kenya
ATM	-	Automated Teller Machine
CA	-	Communications Authority of Kenya
CCTV	-	Closed Circuit Television
CD	-	Compact Disc
DVD	-	Digital Versatile Disc
CIRTs	-	Computer Incident Response Teams
COP	-	Child Online Protection
CPJ	-	Centre to Protect Journalists
DCI	-	Directorate of Criminal Investigations
DNS	-	Domain Name Server
DVD	-	Digital Video Disc
EU	-	European Union
FGD	-	Focus Group Discussion
FTP	-	File Transfer Protocol
GPRS	-	General Packet Radio Services
GPS	-	Global Positioning System
HD	-	High Definition

HTTP	-	Hypertext Transfer Protocol
ICT	-	Information Communication Technology
ICTA	-	Information Communication Technology Authority
IDS	-	Intrusion Detection Systems
ILO	-	International Labour Organization
IP	-	Internet Protocol
IPSO	-	Independent Press Standards Organization
IT	-	Information Technology
KE-CIRT	-	Kenya Computer Incident Response Team
MCK	-	Media Council of Kenya
NACOSTI	-	National Council for Science, Technology and Innovation
NIS	-	National Intelligence Service
PUK	-	Personal Unlocking Key
SD	-	Secure Digital
UK	-	United Kingdom
UNESCO	-	United Nations Educational, Scientific and Cultural Organization
UNHR	-	United Nations Human Rights
UNICEF	-	United Nations International Children Education Fund
URL	-	Uniform Resource Locator
USA	-	United States of America
USB	-	Universal Serial Bus
WHO	-	World Health Organization
WI-FI	-	Wireless Fidelity
WWW	-	World Wide Web

OPERATIONAL DEFINITION OF TERMS

Breach of Privacy: Unauthorized accesses, collection, usage, or disclosure of personal information.

Convergent Platforms: Communication networks or social sites that are Interconnected on the Internet Protocol.

Digital Technologies: Electronic devices, infrastructures, software, or applications that can be used in the production, processing, storage, retrial, or distribution of information.

Experiences: Online activities and interactions of the regular Internet users, their observations, incidents witnessed, and personal encounters on the social platforms.

Hypertexuality: The capability of the Internet that permits the production and distribution of large user-generated content such as texts, sounds, pictures on the Internet protocol.

Interactivity: The capability of the Internet that enables sharing information such as texting, photos, sounds, or videos, in reciprocal dimensions.

Internet Affordances: The Internet capabilities that permit users to perform a variety of functions by the use of smart devices, Internet applications, and software.

Internet Traffic: Information flowing over the Internet platform.

Internet User: An individual who utilizes Internet platforms, applications, and services in online communication.

The intrusion of Privacy: Access, collection, or disclosure of private information without consent.

Media Convergence: A communication paradigm represented by merging of media platforms, permitting free flow of information on the Internet Protocol (IP).

Multimediality: Integration and presentation of audio and visual elements such as video clips, podcasts, images, animation, sounds, and texts through digital devices.

Online Actor/Internet Actor: An individual who is creating, distributing, or accessing the information on the Internet/ online networks.

Online Communication: An interactive process incorporating creation, distribution, access of information on the Internet.

Ordinary Internet User: An individual who utilizes the Internet social sites but may not necessarily possess explicit ICT skills.

Privacy Intrusion Mitigation Strategies: Procedures or measures of averting privacy invasion or minimizing harm arising from privacy intrusion incidences.

Privacy Protection: Keeping personal information away from unauthorized access and disclosure.

Regular Internet Users: Individuals who actively and constantly utilize the Internet platforms, applications, or services.

Virtuality: The intangible nature of the cyberspaces that supports online communication.

ABSTRACT

Media convergence has triggered unlimited production and consumption of the Internet content by embracing novel smart devices and interactive tools that permit users, including audiences, to create and to share massive information on the cyberspaces; hence, raising unprecedented online privacy concerns. This study therefore explored role of media convergence in intrusion of online privacy based on the experiences of regular Internet users in Nairobi City County in Kenya. The theoretical framework adopted in the study comprised the Theory of Media Convergence by Henry Jenkins and the Privacy Theory of James Moor. The study used four FGDs drawn from four selected universities in Nairobi City County and eight key expert interviewees from government organizations related to communication. FGD discussion and Interview guides were used in data collection. Data was analyzed qualitatively based on related thematic concepts. Findings depicted a proliferation of unrestricted user-generated information where online players, who are not journalists, were constantly creating and distributing information of private nature, news of shock, acts of violence, crime, sexual assault, and messages of bereavement and grief. Infringement issues isolated by the key expert respondents included harvesting of personal data, disclosure of information, data breach, identity theft, impersonation, and fake news. Susceptibility of social sites to cyber-attacks, the proliferation of unregulated social sites, user vulnerability, Internet tracking tools, Internet penetration, searchability, and online anonymity were deemed to challenge regulation of the IP. The study concluded that: Internet users were divulging vast amounts of private information on the IP; privacy violations were being witnessed and; an array of mitigation strategies was adopted including legislation and policy-making, enforcement of compliance, incidents response, capacity building, consumer education and outreach programmes. The study made the following recommendations: media regulation and policy-making to continually focus on reviewing of cyber regulatory environment; to consider making a law that would, primarily, focus on online privacy; to explore the possibility of collaborations among nations in dealing with Internet violations; to encourage data minimization and; to consider extending consumer outreach programmes to university students. Recommendations made for further research include: investigating implications of privacy infringements on the cyberspaces and; exploring user-awareness of cyber privacy risks.

CHAPTER ONE: INTRODUCTION TO THE STUDY

1.1 Introduction

This Thesis consists of six chapters. Chapter One presents the introduction to the study, an overview of the background to the study, the problem statement, the research objectives the research questions, the assumptions of the study, the study purpose, justification, the scope and the study limitations.

Chapter Two presents the literature reviewed in the areas related to media convergence and intrusion of privacy of Internet users, the theoretical framework, the conceptual framework, and the research variables.

Chapter Three outlines the research methodology applied in the study including the research design, target population, sampling procedure, sample size, criteria for participants sampling, data collection instruments, data collection techniques, inclusion and exclusion criteria, data analysis, logistical and ethical considerations.

Chapter Four accounts for the research data analysis, interpretation, and discussion arising from the four FGDs comprising students from four universities in Nairobi City County, namely: Kenyatta University, Multimedia University (CBD campus), Kenya Methodist University (Nairobi Campus) and Africa Nazarene University (Nairobi Campus). The participants discussed the questions in the discussion guides prepared for the study. The FGDs were used to obtain data for objectives One, Two, and Three of this study.

Chapter Five focuses on the analysis, interpretation, and discussion of data from the eight key experts drawn from government institutions related to information and communication namely: The Media Council of Kenya (MCK), the Communications Authority of Kenya (CA), and the ICT Authority of Kenya (ICTA). The data collected from the key respondents focused on objective Four of the study that explored mitigation strategies for guarding against intrusion of privacy of Internet users.

Chapter six presents the summary of the study findings, the conclusions, and recommendations arising from the findings of this study.

The research adopted a qualitative approach in the analysis of the data collected from both the FGD participants and the interview respondents. The data emerging from the FGDs included conversations based on their online experiences, their Internet activities, and the nature of the content they witnessed or encountered during their online interactions.

The key respondents provided expert knowledge and recommendations concerning online infringements and mitigation strategies for guarding against intrusion of online privacy. The key experts responded to the questions in the interview guide prepared for the study. Data analysis and findings were presented according to the relevant thematic concepts guided by the objective of the study and the research questions.

The first thematic part focused on the analysis of the role of multimediality in the proliferation of user-created content on private information. In this section, the researcher analyzed the devices used for communication on the Internet and the functions performed by the participants in the FGDs. Internet applications and tools attributed to intrusion of privacy were also analyzed. The section also comprises the analysis of the discussions of Internet activities that escalate invasion of personal privacy. The accounts of the participants' encounters and activities on the Internet were qualitatively analyzed.

The second thematic area was based on data analyzed on the contribution of hypertexuality in real-time streaming of news of shock, acts of violence, crime, and sexual assault and its role in privacy infringement. The data was analyzed based on the focus group discussions on publications of news of shock, acts of violence and crime, and personally identifiable content on cases of sexual assaults.

The third theme focused on data analysis in the role of interactivity on intrusion of bereavement and private grief. The section presents discussions emanating from FGD conversations on the content that intrudes the privacy of the bereaved and the nature of Internet platforms that support dissemination of news of bereavement and grief.

The fourth thematic area was based on the strategies of mitigating infringements of online privacy. The data was obtained from the interviews conducted with the key experts selected for the study.

1.2 Background of the Study

Media convergence has transformed the communication landscape by merging previously discrete modes of communication media. Media convergence has embraced a new information paradigm characterized by Internet affordances such as multimediality, hypertextuality, and interactivity (Ruggiero, 2000; Jenkins, 2006). In the media convergent realm, information is transmitted through the Internet spectrum. According to Turner (2006), the Internet network began to operate in the 1960s through the World Wide Web (WWW) where the modern cyberculture roots can be traced. The use of electronic devices in the 1980s ushered in computer-mediated communication in the early 1990s.

The convergent Internet platforms have created a vibrant environment with access and exchange of massive mass communication content on the Web (Baran and Davis, 2010; Vickers 2012; Adams, 2012). Kalamar (2016) observes that the development of information communication technology represents the formation of a new technological era with a series of deep structures cutting across all parts of social life. The Media convergence phenomenon has altered the logic of media action as a consequence of information technological development, popularization, and use of the Internet. In reality, the full spectrum of digital space is quite broad and includes a wide host of technology. The new communication technology comprises concepts such as wireless and mobile media, satellite radio, digital television, and other new or emerging technologies for mediated public communication (Pathak, 2016). Communication in the convergent era, therefore, involves emerging new platforms accessed through digital delivery media, many of which, serve specialized audiences and communities and not a mass audience in the traditional sense. Jenkins (2002) observes that due to media technological convergence and the availability of web user tools, modern communication has led to the emergence of what the author refers to as ‘collective intelligence’. This has moved communication from the

authorship of a single person to collaborative authorship and mass production of user-created content.

The convergence of media platforms on the Internet protocol is deemed to increase the proliferation of information via a single interactive platform (Baran and Davis, 2010). The media convergent era is characterized by uncontrolled production of enormous data where the role of audiences is continuously changing. Media Convergence is marked by changes in various aspects of communication in terms of media products, audiences and digital devices (Kalamar, 2016; Zhao *et al.*, 2017). Surmatisa and Hafizni (2017) observe that the media industry expanded the broadcast network to embrace the Internet Protocol and the reaching power has become more widespread. In the current media convergence environment, audiences participate more in journalism than ever before because the Internet allows more fluidity and openness in creation of the news. This communication order represents the notion of 'liquid' journalism. Deuze (2007) asserts that 'Liquid' Journalism involves immediacy in relaying of messages. Therefore, individuals are in constant contact with each other via the convergent and networked platforms on the Internet.

Carpenter and McLuhan (1960) observe that the coming of the electronic age would facilitate a transit from visual to 'Acoustic Space', which would be boundless, directionless and horizonless, dynamic, always in flux, creating its own dimensions moment by moment, and have no fixed boundaries. The usage of the Internet, thus, justifies McLuhan's concept of the world becoming a 'global village' where the Internet facilitates quicker opportunities of sending comprehensive information. This concept is realized through the current media convergence on virtual cyberspace (Schafer, 2007). Today, the world communities connect without restrictions. This new convergent media type has become popular, leading to convenience in the relaying of content in form of texts, audios and visual formats. The content is accessed concurrently and simultaneously in real-time because the Internet Protocol is characterized by the use of digital technology that supports streaming of content through online sites and networks. As Borgmann (2012) notes that globalization of society is increasingly leading people from various cultural backgrounds to live together in a

universal communication environment. Jenkins (2006) remarks that media convergence involves proliferation of large numbers of uncontrolled Internet users who create abundant media content and large numbers of online audiences are increasingly consuming this content.

Internet usage has increased with the emergence of 2.0 and 3.0 Networks. The Internet cyberspace has supported an upsurge and widespread use of digital information through novel communication technologies. The communication landscape has provided users with versatile devices and tools, increasing their capacity to constantly interact on the IP (Gómez-Díaz and Arroyo-Almaraz, 2015; Pathak, 2016). Media convergence, as noted by Yualabi (2014), has immensely revolutionized all aspects of human life. With 3G telephony, mass media companies can include consumer technologies such as mobile phones and video games. We have blurred the lines between info-tainment, promo-tainment, and edu-tainment, and now it is hard to separate intrapersonal, interpersonal, and mass communication. These changes represent a seismic shift in the way we view communication and are typically referred to as 'Convergence'.

The Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights reaffirm the human right to protection of privacy. The Vienna Declaration (1993) states that no one shall be subjected to arbitrary or unlawful interference on his or her privacy, family, home or correspondence. Sundar (2008) remarks that the online communication environment is often much more complex than traditional media contexts due to the multiplicity and multimediality of information sources. Adams (2012) observes that there is great interactivity permitted by media convergence and Internet usage as communication devices have become more technologically alike and network platforms have been joined. Hence, the simplest form of interactivity concerns the action of the consumer clicking on provided links.

With the development of content production and publishing systems, it is now easier to produce content for several output media channels. Furthermore, as audiences choose to consume content using several different digital devices, media actors are meeting the

audience by providing content in various publishing channels. Appelgren (2007) asserts that convergence is, therefore, a process where separate media entities such as technological devices, networks, content or markets become more alike or are approaching each other. According to Ruggiero (2000), the interactivity of digital convergence has led to task-oriented Internet users who, extensively, connect and exchange roles in their mutual discourses. This change has moved communication from the authorship of a single individual to a collaborative production of user-generated content (kammer 2013; Sumartias and Hafizni, 2017). Due to the proliferation of user production and publication of content, sensitive personal data may be created and circulated without the knowledge or consent of the concerned person(s).

The Editors' Code of Practice in the United Kingdom (2011) provides that everyone is entitled to respect for his or her private and family life, home, health, and correspondence, including digital communications. The same is emphasized in Germany (Borgmann, 2012). Numerous media codes of ethics discourage journalists' reportage that invades privacy or that which seems to glamourize violence and crime (AMWIK, 2014; Reuters, 2008; Code of Conduct for Practice of Journalism in Kenya, 2013). Similarly, privacy protection is provided under the Kenyan Bill of Rights entrenched in the Kenyan Constitution (2010). In the current media convergence environment, there is a need for considering new parameters regarding universal media ethical values arising from globalization in the practice of journalism. Dissemination of content in real-time on the Internet seems to raise serious communication concerns about potential intrusion of privacy and respect of human dignity (Ward, 2005). According to American Civil Liberties Union, in recent times, as more and more of personal lives is moving online, Internet intrusions have great and devastating implications for the right to personal privacy.

Devi and Roy (2012) indicate that the Internet is a multipurpose tool with numerous potentials. Internet users have experienced great autonomy in the creation and consumption of online news. A similar observation has been made by Dueze (2006) who asserts that in the current globally networked and 'always on' media environment everyone can create copy, modify and share any kind of media. Huge data is produced and consumed by

Internet users. Newman (2014) notes that there has been an unfathomable magnitude of content published on Facebook with the ability to intrude into the personal lives of other users. By examining and analyzing the activities and the encounters of the research participants, this study therefore explored the role of media convergence dynamics in intrusion of privacy of Internet users.

1.3 Statement of the Problem

Universally, communication and media best practices underscore the protection of privacy and minimizing of harm when sourcing and disseminating information. Privacy is one of the fundamental rights recognized by the United Nations Declaration of Human Rights (1948). Privacy right is also protected by many international, regional and national instruments. Today, the convergence of the virtual platforms on the IP has triggered a shift in communication creating a multi-faceted information ecosystem. The change is marked by the proliferation of versatile communication tools and devices, audience transformation, and unrestricted production and distribution of information, in the cyberspaces, in real-time. Hence, unprecedented privacy concerns arise, and consequently the need to interrogate privacy infringements on the convergent platforms. This study therefore explored role of media convergence in intrusion of online privacy in Nairobi City County in Kenya. Data was collected based on the experiences of regular Internet users. The study further examined the strategies for mitigating online privacy infringements occasioned by the apparent communication drift on the Internet protocol.

1.4 Purpose of the Study

This study explored role of media convergence in intrusion of privacy based on the experiences of regular Internet users in Nairobi City County in Kenya. The study examined and analyzed online experiences such as the activities of regular Internet users and the incidents witnessed on social platforms. The aspects of media convergence explored in this study include multimediality, hypertextuality, interactivity, and their role in intrusion of online privacy. This study also explored strategies for mitigating infringement of online

privacy by analyzing the data emerging from interviews with the key expert respondents. The research also provided conclusions and recommendations arising from the study.

1.5 Research Objectives

1) To assess the role of multimediality in proliferation of user-created content on private information.

2) To determine the contribution of hypertextuality in real-time streaming of shocking news, acts of violence, crime and sexual assault.

3) To examine the role of Internet users' interactivity in intrusion of private bereavement and personal grief.

4. To explore strategies for mitigating infringement of privacy on media convergent platforms.

1.6 Research Questions

1) What is the role of multimediality in the proliferation of user-created content on private data?

2) What role does hypertextuality play in real-time streaming of shocking news, acts of violence, crime and sexual assault?

3) What is the role of Internet users' interactivity in intrusion of bereavement and personal grief?

4. What are the strategies for mitigating infringement of privacy on media convergent platforms?

1.7 Assumptions of the Study

According to Mugenda and Mugenda (2003), to state assumptions is very important. Stating assumptions helps the researcher to justify the study and consequently the findings. The following were the assumptions of the study:

1. Multimediality of media devices enables individuals to use a smart device to create and share data in different interactive formats, to capture, store, download, upload, modify and even publish the data through numerous networked media channels which, potentially, may jeopardize the protection of private information.
2. Hypertextuality of media convergence supports uncontrolled production and transmission of enormous volumes of digital content such as, texts, videos, and photos, hence, permitting circulation of news of shock, acts of violence, crime, and sexual assault that aggravate harm on that affected.
3. Interactivity of media convergence creates a vibrant exchange and reciprocal communication, permitting Internet users to access and publish data that might cause intrusion on bereavement and personal grief.
4. The study also assumed that mitigation strategies can be put in place to abate infringements on privacy arising from media convergence and uncontrolled Internet usage.

1.8 Justification of the Study

This study explored role of media convergence in intrusion of online privacy. The study findings will benefit media regulators and policy-makers in reviewing the cyber regulatory environment because the concerns that need attention were illuminated through this research. For instance, the study explored privacy intrusions emerging from the advent of media convergence. Through the FGDs, the study assessed Internet privacy infringements arising from media convergence by exploring online experiences and activities of the regular Internet users, their observations, incidents witnessed and personal encounters on the social platforms. By interviewing experts in the area under study, the research established the existing mechanisms adopted in combating cyber violations of privacy on

the IP. The key respondents also provided expert insights on the strategies for mitigating privacy infringements. The study further made recommendations and suggestions for further research areas.

1.9 Scope of the Study

The research utilized a sample of regular Internet users from Nairobi City County in Kenya. Four FGDs were formed from university students. The participants were sampled from the following universities: Kenyatta University, Multimedia University (Nairobi CBD Campus), Kenya Methodist University (Nairobi Campus), Africa Nazarene University (Nairobi Campus). Findings from previous studies indicate that university students are avid Internet users as they constantly and intensively utilize Internet services and resources. For instance, Ani (2010) investigated the level of Internet access and the use of electronic resources, in undergraduate students in Nigerian, and revealed that undergraduate students used the Internet extensively. This is in agreement with the survey by Devi and Roy (2012) whose findings indicate that university students frequently interact, share ideas, knowledge and experiences through the Internet. University students, therefore, were considered resourceful in the area under study. The participants, through the FGDs, provided crucial information due to their regular Internet interactions, activities, experiences, and encounters across the Internet traffic.

This study used another sample of eight key experts drawn from three government organizations related to communication. The sample comprised respondents from the Media Council of Kenya (MCK), the Communications Authority of Kenya (CA), and the ICT Authority of Kenya (ICTA). The key respondents participated in face-to-face interviews and provided crucial information due to their expertise and knowledge in the area under study.

1.10 Limitations of the Study

Some of the limitations in this study included the study shortcomings and challenges faced in the process of undertaking the study. The limitations included:

i) The researcher found out that data collection was time-consuming. Interviews with the key respondents, in particular, were extensive and time-intensive extending beyond the proposed study timelines.

ii) This study focused on the media convergence and intrusion of privacy among Internet users in Nairobi City County in Kenya. This means that the scope of the study was delimited to the urban area. This suggests that the findings in this research emerged from an urban population. This research has not captured the contributions of people living in the rural areas of Kenya. It is not clear what the experiences of rural populations are and what the responses would be if the same study was conducted among members of a rural population in Kenya.

iii) The study was delimited to a sample of regular users of the Internet represented by university students. Older populations of Internet users were not included in the study. The trends of Internet consumption may not be similar in older populations. Varied findings are likely to be obtained if a similar study was undertaken among populations of different ages.

CHAPTER TWO: LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This study explored the role of media convergence in intrusion of privacy by examining the online experiences of regular Internet users in Nairobi City County in Kenya. This chapter presents literature reviewed in the area related to media convergence. Relevant local and international instruments of human rights were reviewed to explore the concept of privacy protection in the context of the existing regulatory environment. The chapter also presents the conceptual and the theoretical framework of the study. The study variables investigated in this research have also been elaborated in this chapter.

The areas reviewed included:

1. Multimediality and proliferation of user-created content on private information.
2. Hypertextuality and real-time streaming of content on news of shock, acts of violence, crime and sexual assault.
3. Interactivity and intrusion of private bereavement and family grief.
4. The Strategies for mitigating infringement of personal privacy.

2.2 Multimediality and Proliferation of Content on Private Information

Invasion of privacy occurs when a person cannot maintain a substantial degree of control over personal information and its usage (Culnan, 1993). According to Kammer (2013, media convergence and technological affordances permit unrestricted flow of information on the Internet Protocol. Multimediality has allowed communication through multiple sophisticated media platforms and smart devices which are symptomatic of modern media technologies. The nature of the Internet, therefore, enhances asynchroneity of multimedia platforms hence supporting mobile phone conversations, texting, transfer of photos, videos, and other images captured by computing devices. The content can be gathered, stored or shared over the web environments. The convergence supports information fluidity enabling a free flow of content across numerous convergent and networked IP platforms (Gomez-Diaz and Arroy-Almaraz, 2015). The technological evolution of communication and the

Internet affordances allow databases of information to be connected allowing even greater quantities of data to be processed. Individuals are therefore increasingly getting concerned about the control of private information that is collected and stored in retrieval systems.

A research study conducted by Kammer (2013) indicates that Internet affordances were considered to impact the way the news was being processed. The finding concurs with Kalamar (2016) who conducted a study, on the technological dimension of news websites, and their affordances and on how the affordances are used and found out that multimediality allows content to be produced and presented in multimedia formats such as written text, audio and moving images. This represents a new communication landscape, indicating a shift from traditional to digital formats. Erdal (2007) explains the multimodal aspect in a broader sense, where convergence is seen to extend to professional news making. The author expounds that multimodal convergence and digitization of media production have facilitated a shift in the practices of journalism. The change emanates not only from technological and media convergence but from organizational convergence as well. The drift has influenced the way in which news is made. News makers have changed the practices of news production. The basis of this development is the digitization of information production systems. The shift enables content to travel across media boundaries on the web. This development is often described using the all-encompassing term 'convergence', which covers a wide range of technological, social and cultural processes.

Dwyer and Martin (2012) note that the emergence and use of digital devices, has been remarkable. Image, Photo and video sharing applications such as Flickr, Facebook, Twitpic, YouTube and Vimeo have become great sources of live data that supplement professional photographic and video journalism in environments that emphasize visualized storytelling. The content is then exchanged among the Internet users through social sites including Facebook where people are able to connect with one another on the sites (Thorne, 2012). Multimodal convergence has also been associated with the changing roles of audiences. These new experiences have altered habits and patterns in audience behaviour, which works in a transformed competitive environment and is integrated into new

circumstances. The process of transformation thus alters the original role of the audience (Kalamer, 2016).

Vickers (2012) explains that digitization of media is therefore a new paradigmatic moment, where the majority of the population in the modern world not only has access to a camera in their phone devices, but they have it with them at all time. This means that Internet users are provided with the opportunity to document their lives and the surroundings. The trope of the camera phone as an exemplary daily form of image capture provides crucial communication implications by creating unprecedented turn in photography (Gagging, 2006).

The European Union (EU) Charter of Fundamental Rights (2000), provides that data protection principles should be observed and applied to data processing in its entirety including gathering and use. The EU Charter states that human rights enable individuals to develop their own identities, to lead independent lives and to exercise other rights and freedoms. Privacy right is a fundamental human right (UN Declaration of Human Rights, 1948). According to the United Kingdom National Heritage Committee (1992), everyone is entitled to respect of private family life, home, health and correspondence. It is also unacceptable for journalists to use long lens photography to take pictures of people in private places without consent. Zhao (2017) observes that when private data is disclosed, it will be not reversible. As Mendel *et al*. (2012) note, media technology creates new capacities for government and private actors to analyze personal information. Increased computing power means that vast quantities of information, once collected, can be cheaply and efficiently stored, consolidated and analyzed.

The right to privacy is a fundamental human right and, presumably, should be fully protected. The right to privacy is protected by many instruments of human rights, constitutions and media policies. Such instruments include the United Nations Declaration of Human Rights (1948), the Kenyan constitution (2010), and the Media Council of Kenya Act (2013). Personal information includes facts about personal health, relationships,

financial affairs, sexual activities, and sexual preferences or practices (Media Council of Kenya Act, 2013).

The literature reviewed demonstrated that multimediality of media convergence may have the potential to intrude on privacy in online communication. The literature also indicates that protection of online privacy in the current media convergent environment is an issue of global concern. This research therefore aimed at assessing the role of multimediality of media convergence in intrusion of private information.

2.3 Hypertextuality and Publication of News of Shock, Violence, Crime and Sexual Assault

Media convergence has led to the porosity of communication networks that afford everyone, who has access to the Internet, the ability to create abundant content on the IP. Media convergence has embraced a myriad of actors beyond the journalistic profession and institutions. The Internet has transformed audiences' online activities where users generate media productions resembling that of journalists (O'Reilly, 2005; Deuze, 2007). A study by Kammer (2013) indicates that there is a transformation that has altered the original role of the audience. The Convergence has also enabled globalization of communication leading to the creation of a global informational society.

Media convergence is therefore marked by a changing audience, as the field of news production has become more complex and differentiated. In the new communication trend, the high audience participation has led to collaborative publishing of user-generated content (Jenkins, 2006). Communication has become more diverse in terms of content and audiences (Erdal (2007). News content now comes in a variety of forms delivered by online technologies with enhanced 24-hour capabilities. The era has, therefore, introduced a collective form of authorship through audience participation. Digitization of communication platforms has transformed the process of production of information (Ruggiero, 2000; Jenkins 2002, Gomez-Diaz and Arroy-Almaraz, 2015). Lartzer (2013) notes that the media convergent paradigm has created flexibility in communication. Due to

the introduction of the 2.0 Internet, decentralization of the Internet networks and audience transformation takes place.

According to Kalamar (2016), the paradigm has altered experiences and the activities of mass media audiences. Lartzer (2013) agrees with Ruggiero (2000) who asserts that the availability of web-user tools has moved modern communication away from the authorship of single persons towards collaborative authorship and production of content created by online audiences.

Media ethics across the globe provide guidelines on sourcing and reporting news of shock, acts of violence and crime. For instance, in Bhutan, the Information, Communications and Media Act (2006) impresses on the media not to publish any matter which offends against good taste and decency. According to the Act, journalists should avoid publishing matters which have the effect of glamourizing gratuitous violence. Similarly, the Code of Conduct for the Practice of Journalism of Kenya (2013) recommends that publication of photographs showing mutilated bodies, bloody incidents and abhorrent scenes should be avoided unless the publication or broadcast of such photographs will serve the public interest. In the circumstances that demand the material of this nature to be broadcast, discretion should be advised.

A study by Kammer (2013) focused on digital technology and its affordances which constitute instantaneity. The study indicated that these Internet affordances impacted the way the news was being processed in terms of the speed and the potential of real-time reporting of occurrences. Jenkins (2006) notes that due to hypertextuality and fluidity of information flow in the convergent platforms, there are large numbers of amateurs producing media and large numbers of audiences are consuming the amateur content.

The American Society of Journalists states that one of the core principles of journalism is responsibility in news gathering and reporting. Media are expected to observe relevant ethical values when sourcing information and reporting on sensitive cases to avoid revictimizing the affected persons. Some of the cases where caution is advised include

reporting of cases involving sexual assault. In Lesotho, for instance, the Sexual Offences Act (2003) prohibits publication of certain kinds of information relating to legal proceedings of sexual offenses. In Kenya, the Media Council of Kenya Act (2013) stipulates that media should not identify victims of sexual assault or publish material likely to contribute to such identification. As a general rule, the media is expected to apply caution in the use of pictures and names. Responsibility and sensitivity must be emphasized when there is a possibility of harming, stigmatizing and embarrassing the persons concerned.

Hypertextuality of media convergence permits the embedding of materials from different Internet sites and applications or feeds from other convergent networks, social sites and communication platforms such as Twitter and Facebook (Adams, 2012; Thoene, 2012; Kammer, 2013). The digitized devices allow the entry of extensive and limitless data. This causes concern about the protection of the dignity of the victims of sexual offenses, their relatives and institutions. According to Reuters (2008), more often than not, media has to deal with graphic, sexually explicit and other sensitive material, but in such extreme circumstances, there is always the need to alert the audience that graphic or explicit content follows so they may take the appropriate shielding measures.

The literature review describes the professional requirements for reporting news of shock, acts of violence, crimes and sexual assault. The literature also indicated that hypertextuality of in the current media environment supports uncontrolled production and instantaneous dissemination of content on the IP by online players who are not journalists including audiences. Therefore, adherence of communication protonorms guiding the process of sourcing and reporting on the IP needed to be determined. This study therefore investigated the contribution of hypertextuality in publication of shocking news, acts of violence, crime and sexual assault.

2.4 Interactivity and Intrusion of Bereavement and Family Grief

Media convergence has provided new communication experiences and interactive services. The explosion of digital media content and the availability of modern technology and communication devices have increasingly led to the accessibility of a lot more information

from a wide range of sources than at any time in the history of mankind (Metzger and Flanagin, 2008). The readily available Internet tools and free webspace enabled a new vibrant interactive environment for breaking news to swiftly develop.

The technological convergence today has allowed an inclusive communication culture and collective production that embraces sharing of media content on the networked systems (Adams, 2012; Lartzer, 2013). Globally, nations of the world are experiencing an overwhelming effect in communication caused by the technological shift leading to a media convergent landscape. A study on the interactivity of media convergence conducted by Thoene (2012) revealed that social media and its usage has increased. The research findings indicate that most people connect with their friends on the sites such as Facebook. The findings represent the aspects of interactivity and inclusivity described by Jenkins' theory of media convergence.

Transmission of user-generated content is supported by the advancement and availability of wireless smart devices and Internet applications, through the broadband Internet, 3G and 4G Mobile Telephony (Goggin, 2006). These technologies have transformed the audience's consumption patterns and demand for media content. The simplest form of interactivity concerns the action of the consumer clicking on provided links (Appelgren, 2007). In this digital convergence era, most devices used to gather and distribute information are highly networked. Borgmann (2012) observes that due to the emergence of an increasingly globalized society, people from various cultural backgrounds live together in a universal communication environment in which many people access media. Therefore, the customs of the various groups have to be considered in media in practice.

In the current communication regime, the web is not only a means of information distribution but a platform for mass interaction, sharing and audience participation. With the development of Web 2.0, the communication paradigm has witnessed a shift from a receptive web platform to a participative medium on Internet servers. There is more participation of the audience in content production than ever before (O'Reilly, 2005). The intangible nature of the Internet affords the web users access to high-speed broad-band

virtual services that allow instantaneous or real-time streaming of global events. This would, possibly, involve the publication and circulation of sensitive information of bereavement and private grief.

Media professional values require journalists to give timely warning before transmitting graphic materials that could be frightening to the audiences. Media regulations across the globe impress on journalists to observe respect for the privacy of people in their grief. Media is expected to communicate sympathy when sourcing and publishing sensitive news from vulnerable sources and bereaved families in their moments of bereavement (Reuters, 2008). The World Health Organization (WHO) at Moscow Convention (1998) outlined certain guidelines for media professionals which recommended respect for the feelings of bereaved persons, especially when communicating bad news on tragic disasters. The guidelines provide that, close-up photography or images of deceased victims, survivors or their families should be avoided wherever possible. The convection also emphasized sensitivity to situations involving personal grief as well as respect for the privacy of the sick and their families (PressWise, 2003). The Media Council of Kenya requires that, in cases involving personal grief, inquiries should be made with sensitivity and discretion, Media Council of Kenya Act (2013).

The reviewed literature revealed the interactive capability of the IP in real-time communication. The literature also indicated that media professional values underpin the need to uphold the privacy of persons during bereavement and grief. This study therefore sought to examine the role of Internet users' interactivity in the intrusion of private bereavement and grief.

2.5 Mitigating Infringements of Privacy

People have become increasingly dependent on global networks when engaging in social, business and educational activities in recent years due to the new technological advancements (Pathak, 2016; Anwar *et al.,* 2017). This paradigm has led to volatile usage of computer network systems raising some privacy protection issues on the Internet Protocol.

An assessment carried out on data security in seven European countries indicated that one of the most important regulations in the European Union, and even at a global level, is the protection of persons concerning the processing of private information and its circulation. The report set standards for data security and privacy protection among nations in the European Union and beyond. According to Report, the member states are required to enhance the protection of the fundamental rights and freedoms of individuals especially their right to privacy regarding the processing of their personal data (Report on ICT and Privacy in Europe, 2006). The Report indicated that such personal data includes any forms of surveillance of digitized content including CCTV images, surveillance of traffic or communications from mobile phones, data generated by the use of shop cards, credit cards and ID cards. Even though mobile technologies increase safety by allowing people to be located in emergencies, the report indicated that excessive use of the devices did not leave enough private space for individuals.

Another key development within the European Union was the passing of the Cybercrime Convention of the Council of Europe in 2001. This pact extended authorization of interception of data in cases where violation of privacy is detected; hence communications on the Internet open for real-time interception and retention of such traffic data.

Contributors to online forums may have no professional and ethical knowledge about how such kinds of data could be harvested and disseminated without aggravating harm to the affected individuals and those related to them. This could intensify privacy invasion (Shilton and Sayles, 2016). Loss of control or unauthorized access of personal information often results from inadequate privacy-enhancing designs of the digital systems. The personal privacy concept in existing legislations reflects the need to consistently negotiate privacy requirements. There is a need to meet the requirements of communication compliance (Gordon, 2007). Compliance with communication standards is essential in preventing unauthorized access, divulgence and disclosure of private data.

A survey by Bijone (2016) indicates that privacy concerns may be mitigated by the installation of detection systems. Detection systems are an essential element for network

security infrastructure and play a very important role in detecting of cyber-attacks. Automated enforcement of policy with reporting and auditing capacities could be a solution to automatically block traffic deemed to violate the policies.

Mitigation measures may involve gateway-based structures such as Firewalls. A firewall is either a software or hardware system used to control incoming and outgoing traffic based on predefined rules. According to Anwar *et al.* (2017), firewall access control is one of the main defensive mechanisms deployed against intrusions. The mechanism functions as the first line of defense of any network-connected and computer-based system. A firewall permits the arriving traffic through the Internet to access open available services such as hypertext transfer protocols and domain name servers. The content categorizes the traffic and acts on it accordingly. For instance, data may be allowed to pass, quarantined, blocked or Black-listed. It is essential to consider the potential security risks when modifying a firewall rule to avoid future issues (Walsh, 2018).

According to Kenjebaev (2008), user education is also essential for creating awareness. Many Internet users may not be aware of the traces they leave after using the Internet. Educating Internet users and reinforcement of policy requirements are essential strategies in data protection. Users need to be made cautious of their responsibilities with regards to their Internet usages and handling of confidential information (Parliament Assembly Council of Europe, 2011).

From the literature reviewed, protection from infringements is occasioned by the new technological developments in communication. Some authors cited the lack of professional and ethical knowledge of online contributors on the kind of data created, the process of harvesting and disseminating the data without aggravating harm. Although the reviewed literature identified various strategies for mitigating privacy infringements, it was important to adequately determine the enforcement of communication standards and regulatory apparatus being conducted in addressing online privacy infringement in the current media convergent environment. This research therefore focused on exploring strategies for mitigating infringement of privacy on Internet platforms. The research was

conducted to determine the strategies adopted in mitigating the infringement of online privacy.

2.6 Research Gap

The literature reviewed in this section focused on two variables: i) media convergence and; ii) protection of privacy in communication. The literature reviewed indicates that the media convergence landscape has altered communication on the IP. The change signifies a drift in communication in terms of production of data, information consumption and interactions on the Internet social platforms, raising concerns about the protection of privacy in online communication. Although the reviewed literature indicated that Internet affordances permit privacy intrusions, the specific experiences and encounters of infringements of Internet users on the Internet platforms were not adequately revealed. Therefore, there was the need to explore the privacy infringements being witnessed on the convergent sites. To fill this gap, this research investigated the role of media convergence in intrusion of online privacy based on the experiences of regular Internet users in Nairobi City County in Kenya.

Findings arising from the study revealed that privacy infringements were being witnessed on the IP as depicted by unrestricted user-generated content on private information, publication news of shock, acts of violence, crime, sexual assault, and grief. The proliferation of smart devices and applications, and the open nature of the IP were deemed to trigger the production and publication of huge data. The key experts isolated infringement issues that included harvesting of personal data, disclosure of confidential information, data breach, identity theft, impersonation and fake news. Mitigation strategies from the interview data included legislation and policy-making, enforcement of compliance, ICT capacity building and training, and provision of consumer-awareness and outreach programmes.

The study made recommendations as follows: the media regulation and policy-making need to continually focus on reviewing of cyber regulatory environment; to consider making a law that would, primarily, focus on the aspect of online privacy and; to explore the possibility of collaborations among nations in dealing with Internet violations;

encouraging of data minimization and; the need to consider means of extending consumer outreach programmes to university students. Finally, the study also recommended the following areas for further research: i) investigating implications of privacy infringements on the cyberspaces and; ii) exploring user-awareness of cyber privacy risks.

2.7 Theoretical Framework

This research explored the role of media convergence in intrusion of online privacy. Therefore, to adequately form a theoretical framework for the study, two theories were adopted, namely: The Media Convergence Theory by Henry Jenkins (2006) and The Theory of Privacy by James Moor (2004)

The media convergence Theory by Henry Jenkins (2006) focused on media convergence, which is the independent variable. The theory of privacy by James Moor (2004) was used to address invasion of privacy as the dependent variable in this study. Therefore, the two theories were adopted because they were found to complement each other in forming the theoretical framework for this study. Consequently, the theories were integrated in data collection, analysis and interpretation.

Media Convergence by Henry Jenkins (2006)

The Media Convergences Theory posits that new technology merges different communication platforms, and consequently redefines the media environment, reshapes everyday life, and alters media consumption. The theory also advances that media convergence has influenced patterns of media creation and interpersonal interactions. This theory further proposes that, in this media convergence paradigm, producers and consumers will interact in unpredictable ways, with the audiences becoming not only consumers but media creators as well. Jenkins advances that media convergence is a novel communication environment denoted by technological shift, audience participatory culture, collective authorship and transmedia storytelling. According to the theory, media convergence represents a postmodern communication pattern that indicates a participative process. According to the theorist, media convergence embraces three Cs that include

Computing, Communication and Content. The theorist further describes the media convergence paradigm as a communication phenomenon that has altered the way Internet users interact with the created content.

This theory was important in the process of data collection, and consequently the analysis and interpretation of findings. The theory offered extra information needed in clarifying and evaluating findings. The first research question focused on multimediality of media convergence and intrusion of private information. As Henry Jenkins advances, the media convergence environment embraces the aspect of multimediality. Findings indicated that participants used devices with abilities to create multimedia content such as videos, audio, photos and screenshots. The second research question examined the aspect of hypertextuality by exploring the activities of the regular Internet users and the materials they witnessed on news of shock, acts of violence, crime and sexual assault. As the theory proposes, hypertextuality permitted unlimited production of user-generated content on the IP. Similarly, materials considered to aggravate the intrusion of grief were examined. Findings indicated that materials on matters of grief were being shared on social sites. From the key respondents, it was found out that the open nature of the Internet, new communication technologies and the rate of Internet absorption enabled sharing of unrestricted data on the convergent platforms. This is an indication that media convergence has altered the role of the audience from passive to active content creators. The findings were in agreement with the concepts proposed in the theory of media convergence by Jenkins (2006).

The Theory of Privacy proposed by James Moor (1997, 2004)

This theory was first proposed in 1997. In 2004, Moor articulated this theory of privacy concerning the modern electronic age by proposing that the communication environment has presented uncertainty about the protection of communication protonorms. For instance, in the data-gathering techniques used to collect and record personal information, often without the knowledge or the consent of users; interactivity and data transmission techniques used to transfer and share personal data across and between digital databases; data mining methods used to source and generate consumer profiles and patterns and;

merging communication media platforms where users extract information from many discreet and unrelated databases and incorporate them it into composite information files. The theory focuses on the media invasion and violation of personal privacy in communication. The tenets of this theory consist of non-intrusion, non-interference and restricted access to personal information. The theory posits that an individual has privacy only in a situation where one can exercise control over personal information when protected from intrusion, interference, and information access by others.

This theory was found essential during data collection, analysis and interpretation of findings. The theory was useful in supplementing information that helped in the analysis and interpretation of the findings. From the collected data, access and distribution of private information were revealed in the activities and the experiences of regular Internet users. Findings depicted unrestricted production and distribution of private information on the social sites. As the theory of privacy proposes, personal privacy is assured if the individual is protected from intrusion, interference and information access by others.

The data from the key respondents, on prevalent privacy violation issues, depicted considerable levels of Internet user vulnerability in terms of online privacy. The autonomy and the anonymity of the virtual platforms increased the susceptibility of Internet users to privacy infringements. The theory also describes the aspects of electronic communication that have led to the ease of accessing, mining and retention of private data. These factors were deemed to aggravate privacy violations on the convergent platforms.

2.8 Conceptual Framework

The Independent variable in this study is media convergence while the dependent variable is intrusion of online privacy. The indicators of media convergence are illustrated in the Conceptual Framework. These include multimediality, hypertextuality and interactivity. The fourth indicator incorporated in the study was the strategies for mitigating invasion of online privacy. In this study, therefore, these indicators of media convergence were examined to establish their role in Internet intrusion of online privacy. The study variables have been illustrated in Figure 2.1 below.

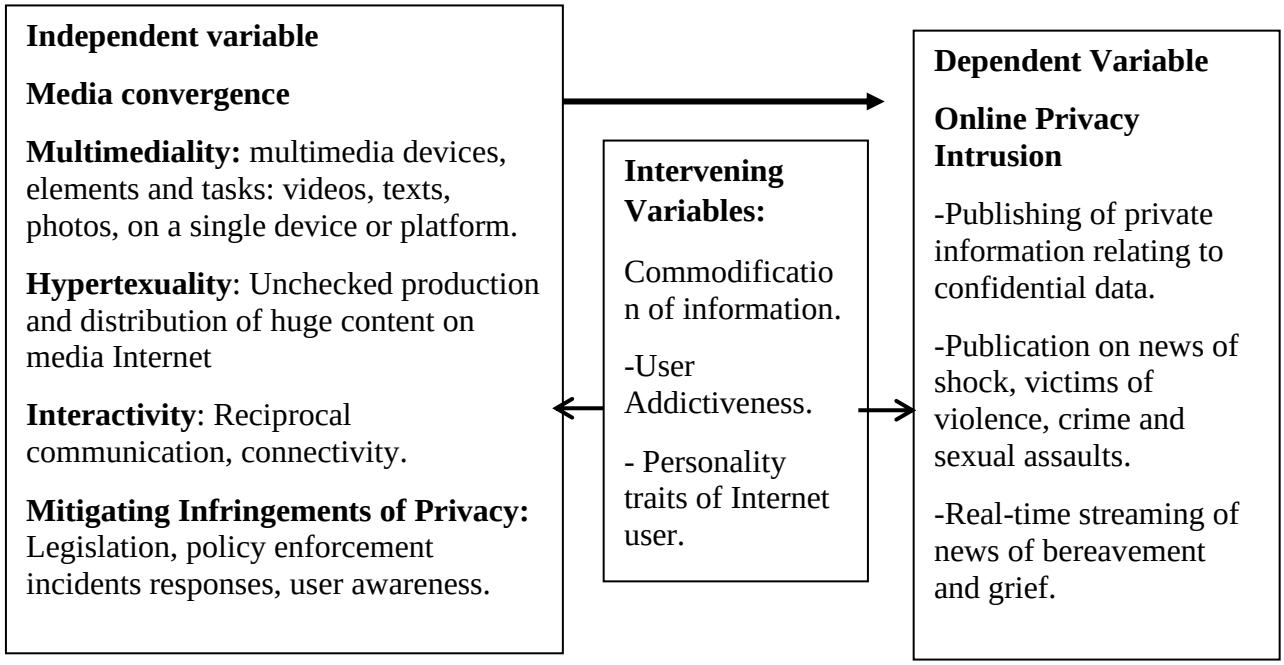


Figure 2.1: Conceptual Framework

2.9 Research Variables

In this research, the independent variable is media convergence while the dependent variable is intrusion of online privacy. The study also identified the intervening variables described in 2.9.3 below.

2.9.1 Independent variable

Media convergence in this study is the independent variable. The variable is represented by the following indicators:

i) Multimediality of media convergence encourages the use of high-speed digital devices to undertake varied media tasks (Adam 2012). The devices are multi-functional and enable users to create multimedia content such as text formats, videos, photos and images (Kun *et al.* (2012; Vickers, 2012, Tran 2015). The

multimedia devices have huge storage capacities such as internal memory chips that may be mounted for large data storage, access, sharing and retrieval of content. This research examined the role of multimediality of media convergence in online invasion of personal information.

ii) Hypertextuality involves uncontrolled proliferation and production of enormous data by Internet users and creators on Internet Protocol (IP). Online production involves the creation of social sites and platforms such as Facebook and blogs (Adams 2012; Sumartias and Hafizni, 2017). Internet users also upload video clips, music, pictures, articles, video games. Web-users apply Internet tools to edit and modify by crop or clone photos and other graphics. The materials produced are transmitted virtually to other users across the Internet Protocol. This research explored the contribution of hypertextuality of media convergence to determine its contribution of shocking news of violence, crime and sexual assault.

iii) The interactivity of media convergence allows vibrant exchange and reciprocal communication through Internet platforms such as Twitter, Facebook, Skype, Instagram, WhatsApp or Telegram. The intangible nature of the converging media networks contributes to the globalization of communication that occurs beyond time and geographical bounds. Globalization embraces both immediacy and automatic data connectivity. According to Jenkins (2006), the virtuality of the Internet also permits data accessibility and user interactivity. This research examined the interactivity of the Internet to establish the role it plays in invasion of privacy of bereavement and grief.

iv) Strategies for mitigating online privacy infringements consist of interventions that address or lessen privacy threats posed by media convergence. The rationale of this research is based on the premise that adherence and compliance to journalistic values and ethics, that guard against intrusion of individuals' privacy in communication, may be hampered by the affordances of media convergence such as multimediality, hypertextuality and interactivity. According to the European Data Protection Supervisor-EDPS (2015), fundamental rights to privacy and the protection of personal data have become more important for the protection of

human dignity than ever before. The rights are enshrined in the EU Treaties and the EU Charter of Fundamental Rights. The data protection principles defined in the EU Charter focus on necessity, proportionality, fairness, data minimization, purpose limitation, consent, and transparency in data processing in its entirety, to the collection as well as to use. Given the necessity of the protection of online privacy, this study explored strategies for mitigating violation of privacy on media convergent platforms.

2.9.2 Dependent variable

The dependent variable in this study is intrusion of privacy of Internet users. Intrusion of privacy of the Internet users, as a dependent variable in this study. This research explored the influence of the aforementioned independent variable on the dependent variable by examining the indicators of media convergence and their role in invasion of privacy of Internet users on the Internet protocol. Therefore, the indicators of media convergence and their role in privacy intrusion were analyzed and conclusions were made. The indicators of Internet privacy intrusion explored in this study included:

i) Publishing of private information relating to confidential data
ii) Publication on news of shock, victims of violence, crime and sexual assaults
iii) Publication of news of bereavement and grief

2.9.3 Intervening Variables

Intervening variables comprise variables that a researcher is not intentionally studying in Research. Walker and Maddan (2019) note that intervening variables are variables that may be between the independent and the dependent variable and are actually causing change on the dependent variable. This study identifies three intervening variables including Commodification of information, Internet addictiveness and user personality traits.

2.9.3.1 Commodification of Information

Internet is a virtual resource and offers open access to world markets through the media convergent environment. Numerous economic activities and transactions are being conducted on Internet platforms. Media convergence has become a global phenomenon offering vast opportunities for socio-economic growth and development. These opportunities range from e-commerce activities such as e-banking, online advertising, business skills training, commercial research to innovation.

According to Jenkins (2004), a micropayment system would allow media producers such as recording artists, independent game designers, web comics' artists and authors to sell their content directly to the consumers, cutting out many layers of middle folk, adjusting prices for the lowered costs of production and distribution in the digital environment. Marchione (2009) asserts that viral marketing illustrates the extent to which marketers and advertisers will go to exploit every media avenue and ensure the conflation of content and advertising. Some of the most vibrant social networks include: shopping sites, Facebook pages, Websites, YouTube, Twitter handles and Emails. Media convergence has embraced use of modern multimedia smart devices, tools and software applications.

The Internet is endowed with vast Internet explorers such as web browsers and search engines that help in accessing the information across the virtual space. This creates a wealth of openings for business actors from both the demand and supply sides. Participation in the era of convergence permits increased commercial interactions with the industries and virtual markets. The to expand in cyberspace is to exploit new spaces for advertising and marketing.

In the present communication environment, new marketing firms get closer to their customers, and e-commerce is conducted on the Internet protocol. Trade operations are optimized through the collaboration of participants in sharing commercial techniques, products and service outsourcing. Media convergence, therefore, becomes essential in the improvement of efficiencies of commercial activities. The tension between making profits and maintaining professionalism is therefore a difficult one to resolve (Khumalo, 2013).

Due to these activities, organizations and customers are bound to divulge substantial information such as names of individuals or companies, physical addresses, emails, phone numbers and banking details. Such disclosures increase threats of privacy as information may be accessed by unauthorized parties.

2.9.3.2 Internet Addictiveness

The Internet has been linked to obsessive behaviour where the users find it hard to refrain from engaging in Internet activities. Internet addiction is the excessive usage of the Internet that manifests in a non-chemical addictiveness related to an obsession with machine interaction (Shaw and Black, 2008). Addicted users are preoccupied with compulsive tendencies of engaging in Internet activities that may include extensive disclosure of information concerning their own private lives.

Previous studies have indicated that university students have a strong affinity towards the Internet because typically students have free and unlimited Internet access (Kuss *et al*, (2013). Shaw and Black (2008) observe that compulsive computer users present computer dependency and Internet addiction. Internet addictiveness produces cravings in users. The users hence become overly involved in compulsive online habits such as gambling, shopping and compulsive sexualships. Internet addictiveness potentially leads users to develop uncontrollable Internet use.

2.9.3.3 User Personality Traits

Disclosure of personal information on the Internet forums, presumably, may be influenced by personality traits that influence intensities of interactivity from one person to the other. Some Internet users, depending on their disposition, willingly permit others to know information about them. On the other hand, some users maintain sharp limits and boundaries between themselves and others. It can be assumed that an individual's general willingness to self-disclose is one of the predictors for a person's self-disclosure on the social web. A survey by Taddicken (2014) established that self-disclosure in the social web has gained popularity in recent years where the Internet users share personal information through different Internet applications such as social networking sites blogs,

wikis, picture and video sharing platforms. The general willingness to let others know something about oneself can be seen as a dispositional personal characteristic.

2.10 Conclusion

This chapter presented the literature reviewed, the Conceptual and the Theoretical Framework, and the research variables.

The next chapter presents the research methodology applied in data collection in the study.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the research methodological details adopted in conducting the study, study population, sampling, the data collection instruments and techniques utilized in the study, the criteria for inclusion and exclusion, validity and reliability, data analysis, and the logistical and ethical procedure followed during data collection.

3.2 Research Methodology

This study used a qualitative research methodology. As Kumar (2011) observes, qualitative research approach is more appropriate for studies exploring any aspect of social life. In this study, the data collection techniques applied included FGDs and interviews which generated content of attribute nature that was analyzed qualitatively.

3.3 Research Design

This research adopted an exploratory research design. Exploratory research design is commonly applied in qualitative studies (Creswell, 2009). Baxter and Jack (2008) note that the exploratory research design is generally applied in social sciences surveys when a researcher intends to cover a contextual condition. This study explored the role of media convergence on intrusion of online privacy. Exploration design, therefore, allowed inquiry within the context of media convergence and intrusion of privacy because it used respondents who had specific experiences and expert knowledge in the area under study. The FGD sessions allowed exploration of Internet user experiences and areas of privacy infringements on the IP. The interviews involved engaging with experts in exploring mitigation strategies for guarding against infringements of online privacy. The interview guides prepared for the study had open-ended questions that allowed probing and seeking clarifications during the interviews. Therefore, exploratory research design was suitable for this study due to the data collection instruments adopted and the nature of the data sought in this study.

3.4 Target Population

This study focused on two study populations. First, the study targeted regular Internet users represented by university students in Nairobi City County. University students were found resourceful in this study because they are considered avid users of the Internet. According to (Kuss, *et al*, 2013), students have a strong Internet affinity for the Internet. Students generally utilize devices that have various digital applications and software (Ani 2010). A study by Devi and Roy (2012) found out that university students are regular users of the Internet. In this study, therefore, data was collected on the experiences of regular Internet users and the nature of Internet traffic encountered during online communication. Secondly, the study targeted skilled communication experts. This population was represented by experts drawn from three government organizations related to communication. This sample was useful in the exploration of specific expert knowledge concerning strategies for mitigating privacy infringements arising from Internet usage on the media convergent platforms.

3.5 Sampling Procedure

This study used purposive sampling method. Purposive sampling is a non-probability sampling method commonly used in studies where researchers choose to use qualitative approaches in data collection. According to Showkat and Parveen (2017), in purposive sampling, the researcher chooses the participants as per his/her own judgment, keeping back in mind the purpose of the study. This type of sampling is used in exploratory research. In this study, both purposive homogenous and purposive expert sampling methods were used to obtain two samples for this study.

3.5.1 Purposive Homogeneous Sampling

This study targeted a population of regular Internet users. In purposive homogeneous sampling, the researcher selects participants for having a shared characteristic or set of similar characteristics or experiences. Foley (2018) observes that homogeneous sampling aims to achieve a sample whose units share the same characteristics. This method is used

when a researcher is investigating a typical case or average or a norm for the members of the population. This study, therefore, focused on a homogenous population of university students in Nairobi City County. Within the context of this study, the population was considered because they shared common characteristics in terms of regular Internet usage. This is consistent with findings of the study by Devi and Roy (2012) who found out that students are constantly in online communication. Therefore, the university students' population experiences great volumes of digital traffic in their daily interactions and conversations on the Internet platforms. Using university students in this study, as regular Internet users, was beneficial in exploring and determining the role of media convergence in intrusion of online privacy based on the Internet activities and experiences revealed in the FGDs.

3.5.2 Purposive Expert Sampling

According to Schreiber and Kimberly (2011), the sample size in qualitative methodology should be information-rich informants. In this research, eight respondents were purposively sampled from government institutions related to information through purposive expert sampling method. The attributes considered for the respondents to be selected included knowledge and expertise in the area of study interest. According to Kumar (2011), in expert sampling, the respondents should be known experts in the field of interest. This sampling strategy is more common in qualitative research where a researcher identifies persons with demonstrated or known expertise in an area of interest. The key respondents had expertise and knowledge in the following areas: Multimedia Services (CA), Legal Services (CA), Cybersecurity (CA), Programmes and Standards (ICTA), ICT (ICTA), Media Analyst and Monitoring (MCK), Media/ICT (MCK) and Accreditation and Compliance (MCK).

3.6 Sample Size

The Sample size included four FGDs from universities in Nairobi County which were selected through purposive sampling. As McCombes (2019) states, purposive sampling is applied in qualitative research, where the researcher is interested in detailed knowledge on a specific phenomenon rather than making statistical inferences. In purposive sampling,

the researcher uses personal judgment to choose cases that may help achieve research objectives. In this case therefore, the researcher purposively selected the four Universities used in the study. The Universities included the Multimedia University (CBD Campus), the Kenya Methodist University (Nairobi Campus), Kenyatta University and the Africa Nazarene University (City Campus). To obtain the study participants, the researcher approached the universities selected from the study. The researcher presented a letter of introduction and other research authorization documents. After obtaining approval for data collection from the respective universities, the researcher sought the assistance of staff members in obtaining students from different years of study. From the students availed in each of the universities, five male and five female participants were randomly selected to form each focus group. Each group consisted of 10 participants.

The number of the FGDs used in this study was guided by the recommended rule of thumb, for qualitative research studies utilizing focus groups for data collection. For instance, Morgan (1997) recommends that 3-5 focus groups are enough for data saturation to be achieved in a study. Zeller (1967) observes that for social sciences, more groups seldom provide meaningful new insights. The data collected may be repetitive and eventually becomes superfluous. The decision to use 10 participants per FGD was also based on the rule of thumb, which recommends, that one FGD may consist of 6-10 participants who are purposively drawn from a homogeneous population (Morgan, 1997).

The second study sample included eight key experts who were purposively sampled from Kenyan government institutions related to communication. The participants were recruited based on their expertise and knowledge in the area under study. This is in tandem with the assertion of Kumar (2011) that, in qualitative studies, a researcher is guided own judgment as to who is likely to provide the best information. Three experts were recruited from the Media Council of Kenya; three from the Communications Authority of Kenya and two from the ICT Authority of Kenya as indicated in 3.5.2 above.

3.7 Inclusion and Exclusion Criteria

Criteria for participants sampling entails the characteristics or traits that study subjects should possess for eligibility to participate in the study. To focus on the problem of this study, there were salient elements considered in determining the inclusion of the participants for the FGDs. Kumar (2011) notes that, in purposive sampling, a researcher only goes to those people who in his/her opinion are likely to have the required information and are willing to share it. The elements determining the participants included students aged between 19-26 years, regular Internet usage and the willingness to share information. This population provided crucial information on Internet user experiences and the Internet traffic that intruded on online privacy. The eight key respondents were considered based on their expertise and knowledge in the area under study as indicated in 3.5.2 above. The respondents thus provided crucial information related to strategies for mitigating online invasion of privacy. The two sets of study participants were essential sources of information in the area under study.

3.8 Data Collection Instruments

The researcher prepared and utilized two types of data collection instruments. The instruments included FGD discussion guides and interview guides. By using both FGD discussion and interview guides, qualitative data was collected during the study.

3.8.1 Discussion Guides

In this research, discussion guides were utilized in collecting data from the study focus groups. The FGDs generated discussions as the participants responded to the questions in the discussion guides. Leslie *et al.* (2009) observe that focus groups are guided discussions where the conversations are conducted. The FGD guides were useful in the study as the participants shared information required to answer the research questions in the study.

3.8.2 Interview Guides

The responses of the eight key respondents were collected using interview guides prepared for the study. Wimmer and Dominick (2011) state that interview guides are effective data collection instruments because they help researchers to explore topics in great depth. According to Orodho (2009), interview guides enable standardization of questions and allow probing. The respondents were engaged in face-to-face interviews using the guides. The interview guide had open-ended questions that helped the researcher to prompt respondents for more information.

3.9 Data Collection Techniques

In this research, the members of the FGDs were engaged in discussions by use of the discussion guides prepared for the study. The FGDs discussions involved conversations about Internet user activities, the experiences and the Internet traffic witnessed by the participants. Face-to-face interviews with the key respondents from government organizations were conducted using interview guides prepared for the study. Explanations were sought based on the interview questions aligned to the themes of the study. The data collection process involved both audio recordings and notes taking. The data generated during FGD discussions and the interviews were important in answering the research questions in this study.

3.10 Validity and Reliability

Validity determines the accuracy of research instruments in obtaining objective data. Reliability means that a measuring instrument provides consistent results. According to Serem *et al*. (2013), validity is critical in data collection as it indicates the degree to which an instrument measures what it is expected to measure. This research used two different sets of study respondents which included FGD participants and key interview respondents. To collect the two sets of data, two types of data collection tools were prepared. The tools included FGD and interview guides. To ensure the validity of the instruments, the research tools were submitted to the study supervisors for evaluation. The supervisors reviewed the

questions in the instruments and discussed them with the researcher. Modifications were made as found appropriate to ensure precision.

Validity was also ensured through triangulation by the use of different data sources, data collection tools and study theories. According to Heale and Forbes (2013), triangulation may include two or more sets of data collection using the same methodology, such as from qualitative data. Triangulation may also involve the use of multiple theories within the study of a single phenomenon. The research targeted two different populations that included the FGDs of avid regular users of the Internet and experts from three major government organizations who were versed in the area of communication. The study utilized both FGD guides and Interview schedules in data collection. The research adopted two different theories to adequately investigate the variables of the study. The theory of media convergence addressed the independent variable, while the theory of privacy focused on the dependent variable of the study. The researcher also used findings from previous studies to evaluate the research findings.

To test for validity and reliability of the interview guide, the researcher interviewed one expert in the area of Licensing, Compliance and Standards. On the accuracy of the questions in the focus group discussion guide, a pre-test was conducted on focus group of 10 participants before the main study was undertaken. The responses of the subjects involved in the pre-test were not included in the main study. According to Porta (2008), a pilot test is a small-scale test on proposed research procedures to be applied on a larger scale study after which the instruments are applied in data collection.

3.11 Data Analysis

This research generated qualitative data which was analyzed thematically according to their broad attributes. The themes were created by locating the precisely connected ideas from the transcripts of recorded audio content and the data in written notes. Therefore, data analysis in this research was done by categorizing the findings into related thematic sets. This is in tandem with Schreiber and Kimberly (2011) who observe that in qualitative analysis, researchers look at words, phrases, and observed behaviour. Creswell (2009)

notes that qualitative data is classified as attribute and non-numeric in characteristics, hence, such data is analyzed qualitatively. Therefore, the concepts were grouped as follows: Multimediality and invasion of private information; hypertextuality and news of shock, violence, crime and sexual assault; interactivity and intrusion on bereavement and grief and; strategies of mitigating privacy infringements. From the analyzed data, conclusions and recommendations were made.

3.12 Logistical and Ethical Considerations

After obtaining research approval and research authorization from Kenyatta University, the researcher sought a research permit from the National Council for Science, Technology and Innovation (NACOSTI). Approval was also sought from Nairobi City Commissioner and the Ministry of Education Science and Technology-Regional Coordinator of Education, Nairobi. A notification was also made to the Sub-County Director of Education, Starehe Sub-County of Nairobi City County. To obtain permission to conduct the research from concerned universities and government institutions sampled for the study, the researcher presented the research authorization documents to the institutions. Once permissions were granted, the researcher proceeded with data collection. The data collection was conducted through audio recordings and note taking. Participation in this study was voluntary. All the participants were assured of confidentiality. Therefore, the identities of the respondents were coded to ensure anonymity and confidentiality.

3.13 Conclusion

Chapter Three focused on the research methodology, research procedures, ethical and logistical procedures applied during the research.

In the next chapter, data is organized and analyzed according to respective thematic concepts.The conceptual framework and the study theories were integrated in the interpretation of the research findings. The theories include: The Media Convergence advanced by Henry Jenkins (2006) and the Theory of Privacy proposed by James Moor (1997, 2004)

CHAPTER FOUR: DATA ANALYSIS AND DISCUSSION OF FINDINGS

4.1 Introduction

This chapter presents the analysis of data arising from the responses of the participants in the FGDs used in the study. The data analysis adopted in this research is purely qualitative. The analysis was done based on thematic areas. The themes were aligned to the objectives of the study as follows: i) Multimediality and proliferation of user-created content on private information; ii) Hypertextuality and publication of news of shock, acts of violence, crime and sexual assault and; iii) Interactivity and intrusion on bereavement and grief. The organization and the presentation of the themes in this study is consistent with Kumar (2011) who observes that, in the process of organizing data for qualitative analysis, the researcher first identifies the main themes by keywords and then classifies responses under the main themes. The researcher then integrates the themes into text. Schreiber and Kimberly (2011) note that analysis of non-numeric data requires a researcher to generate a summary sheet based on field notes. The researcher then determines category connections and develops relations among patterns and themes. In this study, the recorded audio content and the written notes were analyzed where the data with close links were placed under that same theme. Therefore, concepts were arranged with respect to the thematic areas to maintain coherence with to the study objectives and the research questions. The researcher also provides summary highlights of responses in form of tables in various segments.

4.1.2 The FGD Participants

The focus group participants comprised students from universities in Nairobi City County. The participants formed four FGDs. Each group consisted 10 members. The total number of participants was 40. The participants were drawn from Kenyatta University, Multimedia University (Nairobi CBD Campus), Kenya Methodist University (Nairobi Campus) and Africa Nazarene University (Nairobi Campus). The age bracket between 19-21 years had 12 participants, 22-23 years had 26 participants, and 2 were aged between 24-26 years. The participants discussed the questions in the discussion guides prepared for the study. The focus group discussions sought to answer the following three research questions:

1) What is the role of multimediality in the proliferation of user-created content on private data?

2) What role does hypertextuality play in real-time streaming of shocking news of violence, tragedies and crime?

3) What is the role of Internet users' interactivity in intrusion of bereavement and personal grief?

4.3 Multimediality and Proliferation of Private Information

According to Kalamar (2016), multimediality is a characteristic of digital media that can take numerous shapes and forms. Multimediality incorporates a combination of multimedia elements such as videos, pictures, graphics, sounds or texts. The data analysis from the FGDs looked into the novel communication devices and the Internet user activities considered to escalate intrusion of online privacy. The nature of the Internet traffic witnessed by the FGD participants was also analyzed.

4.3.1 Multimedia Devices Used for Internet Activities

This section focused on the first study objective of the study that assessed the role of multimediality in proliferation of user-created content on private information.

In this section, the study sought to answer that the following research question:

What is the role of multimediality in the proliferation of user-created content on private data?

To elicit information concerning the activities regularly conducted by the FGD participants, the researcher collected data on the devices used by the participants and the functions the devices are enabled to perform.

When asked to identify the devices they frequently used on the Internet, the participants across all the focus groups provided an almost similar list of devices including personal computers or desktops, laptops, tablets and smartphones. Some participants also observed that the communication devices are used alongside various accessories and data storage devices. The devices mentioned included USBs and devices such as DVDs, SD cards, external hard disks and flash disks. The devices can copy, transfer or store large amounts of data. The findings are consistent with Jenkins's theory (2006) that advances that media convergence has embraced a communication environment denoted by the emergence of new technologies.

The smartphone, in particular, was the most mentioned device by the participants across the FGDs. All the members from all the groups indicated that their mobile handsets were connected to Internet services. According to Vickers (2012), the most networked digital media device today is the mobile phone. This is in tandem with Fleury (2012) who observes that:

> Mobile phones are so omnipresent in our everyday lives. They are convenient, personal, private, small and active. People carry them around everywhere and constantly rely upon them for communication purposes as well as for performing a plethora of secondary activities, such as checking emails and surfing the Internet.

A study by Adam (2012) validates the assertion by indicating that, smartphone technology has grown and increased the amount of information users store on their mobile phones. As smartphones, tablets, and other technologies become more portable, accessing information has become easier and quicker.

4.3.2 Functions Performed by Multimedia Devices

This section analyzed the general tasks conducted by the participants using multimedia devices. The list of functions consisted of activities such as making calls, texting, taking

videos, capturing photos, recording audio content, editing of images, uploading photos and images, updating profile pictures and personal statuses, researching, surfing the Internet, sending and receiving emails, storing of files such as academic documents, keeping a personal diary, photo gallery, entertainment including listening to music and playing of video games. Other functions included conducting transactions such as sending and receiving money, advertising, online shopping, using google maps, weather updates, requesting taxi transport and ordering for services. From the responses, the participants executed numerous tasks due to various abilities and applications in the devices. The participants also indicated that they used other applications such as Bluetooth, Xender and Flashshare to connect and to share information from one device to another. The findings indicated that the Internet has changed communication where Internet users create, publish and share content with other people on social sites. As Jenkins (2006) asserts, media convergence represents a postmodern communication pattern that indicates a participative process. This was portrayed by the activities conducted by the participants on the IP.

Table 4.1: Functions Performed by the Devices

	Devices	Functions
Devices	Mobile Smartphones	Making calls, taking photos, editing of photos, screenshots, texting, video calls, recording, surfing the Internet, downloading, sending and receiving emails, online shopping, money transfer, calendar, keeping of dairy, storing notes, researching, advertising, entertainment, google maps, alarm, taxi transport services and ordering for services.
	Laptops:	Editing photos, surfing the Internet, researching, downloading, sending and receiving emails, online shopping, money transfer, keeping of dairy, storing notes, advertising, online shopping, google maps, ordering for services.
	Desktops:	Editing photos, surfing the Internet, researching, downloading, sending, and receiving emails, online shopping, keeping of dairy, notes, google maps, and ordering for services.

	Ipads /Tablets:	Making calls, taking photos, editing of photos, texting, audio, and video calls, recording, making calls, surfing the Internet, researching, downloading, sending and receiving emails, online shopping, calendar, keeping of dairy, alarm, keeping notes, advertising, google maps, taxi transport services and ordering for services.
Data storage media and file transfer Apps:	SD cards, DVDs, flash disks	Data transfer, sharing, copying data, data storage.
	USBs, Bluetooth, Xender, Flashshare	Data transfer, sharing, copying of data, connecting devices.

4.3.3 Private Content Encountered on the Social Sites

Concerning the content encountered online, the participants were asked to identify the information they considered private. The FGD participants mentioned various types of private and personally identifiable information they regularly encountered on the Internet platforms. The information identified included peoples' real names, personal addresses, age, places of residence, locations, financial records, properties, and health status. Other types of content frequently witnessed concerned peoples' family details such as marital status, pictures of spouses, parents and siblings. From the responses, the study participants had adequate knowledge of what personal privacy content entails.

Despite the awareness of possible privacy vulnerabilities, majority of the participants indicated that private information is commonly disclosed. Most participants observed that personal details are generally disclosed when people are creating social media accounts. A participant noted that:

> When Internet users are creating their Facebook or email accounts, some of the details requested include names, place of residence, education background, place of work and

> names of siblings. In most cases, people enter real information concerning their personal life…

From this observation, it is apparent that real identities and other personally identifying materials are generally disclosed on the Internet Protocol, particularly, when creating a social site such as Facebook, Instagram or Twitter accounts. Most of the participants felt that such information could be a source of infringement of privacy of the concerned persons. Some other participants indicated that a user has little or no control over the usage of the personal information shared on social platforms. One of the participants observed that:

> Users who access information such as photos, download it using smartphones and can store in their phone gallery, tag it in Facebook or Instagram or even forward. Furthermore, people may manage to trace users' activities from their content and their conversations on the social sites. It becomes hard to control the information once it is accessed by others on the Internet.

Most of the participants seemed to be concerned about photos and their usage in propagating intrusion of privacy. The participants admitted having had their photos circulated to other people on the social sites without their consent. Many of the participants indicated they were uncomfortable with their images being captured with or without their knowledge. It was noted that photos can be modified by cropping or photoshop. A respondent commented about manipulating photos:

> Photos can be changed by editing…using tools that are installed in smart devices, especially in PCs and smartphones. This portrays a different image and identity of the person than the real one. I have seen such pictures being circulated…it shows disrespect to personal dignity.

This is inconsistent with media ethics in dealing with photos. According to the Media Council of Kenya ACT (2013), manipulation of pictures in a manner that distorts reality should be avoided.

Based on the functionalities of the devices owned by the FGD participants and the activities conducted, it was apparent that the participants have extensive experiences with digital devices which they use to conduct a variety of online tasks. This demonstrates that the participants were regularly creating, publishing, accessing and consuming information on the Internet platforms by use of smart devices. The theory of James Moor (2004) emphasizes that privacy needs to be ensured by restricting access to personal information. The observation is supported by Kalamar (2016) who asserts that technological development and user experience strive for promptness, accessibility through various platforms such as the Internet and mobile applications and are the driving force of media convergence development. As Metzger *et al.* (2008) observe, in light of their special relationship to digital tools, users are especially well positioned to navigate the complex media environment successfully as they have great familiarity with the media apparatus.

The findings of this study are validated by a study conducted in Malaysia by Muniandy (2010) that revealed that:

> University students are among the avid users of Internet content. The Internet has grown exponentially and has emerged as the foremost source of disseminating information quickly to a large audience, transcending the limitations of time and space. The usage of the Internet has risen tremendously and the use of the Internet by university students now is common in Malaysia.

Similarly, Sumartias and Hafizini (2017) indicate that people, especially the youths, are getting necessary information by reading online sites through digital gadgets or smartphones. As phones and mobile devices have become omnipresent, the ability to

access all of the owner's accounts and the vast amounts of information stored on the devices has become almost effortless (Galterio *et al*, 2018).

The findings are in line with Jenkins (2006), in the theory of media convergence, who proposes that the era of media convergence is marked by changing roles of audiences. The theorist asserts that audiences are no longer passive but active creators of media products. This change is replicated by Internet users' online activities. According to James Moor's Theory of privacy, control of personal information is central in privacy protection. However, from the FGD responses, it is apparent that private data often ends up in the hands of other unexpected users on social platforms. This means that personal information is redistributed to other users without the knowledge or consent of the persons concerned. This is consistent with the findings of the study by Adams (2012) that found out that the people you share information with can always share your information with others, for instance, through Facebook.

4.3.4 Internet Applications and Tools Attributed to Intrusion of Privacy

When answering the question on the Internet applications and tools that they considered to intrude on privacy, the FGD participants demonstrated familiarity with various Internet interactive tools and applications. The participants were using Internet social platforms and applications to interact with friends. For instance, all the participants in the focus groups were registered and users of Facebook; 34 were already using Instagram; 29 were using Telegram; 21 had Imo; 16 of them maintained working Twitter Handles and 6 had LinkedIn accounts. The participants across the focus groups also mentioned platforms interactive and Applications such as blogs and WhatsApp. The participants expressed interest in the Internet and social media activities based on the tasks they regularly conducted on the social platforms. This is an illustration of constant involvement in communication on the convergent sites.

The FGD participants identified Internet applications and software that enable users to access online content concerning other individuals. These included Internet search engines and web browsers. The participants observed that the Internet user tools permit unlimited

access to information available on social platforms. Adams (2012) argues that since sufficient details are not provided to the users of these applications, it is, therefore, the users' responsibility to research any application before allowing it to access personal content. According to Davis and Eldridge (2012), there is some awareness of the potential harm of breaches, but as the concerns for securing data and records increase, the old notion of privacy has been complicated and somehow undermined by the spread of social media ranging from practices such as emails, blogs and Facebook.

4.3.5 Internet Activities Escalating Invasion of Privacy

The participants in the FGDs identified the activities they considered to escalate invasion of privacy. From the discussions, Internet users use devices that are capable of capturing and sharing huge information of personal nature. The participants agreed that Internet users were commonly involved in photography, filming, uploading of photos and texting. Some of the activities identified included using smart devices' cameras, tagging of photos. There was also evidence of unrestricted production of content on social media sites.

4.3.5.1 The Smart Devices' Camera

All the FGD participants admitted that they have always used their mobile phones or ipads' cameras to take photos or to film various events. Some of the participants attested to the fact that they have often witnessed their friends take photos or film different scenes that could be considered private. One of the respondents noted that nobody questions the habit. When such data is recorded and stored, nobody controls how and when to use the recorded information. One of the FGD participants recounted:

> We once attended an event of one of our friends where almost all of us used smartphones to film the occasion. Photos were taken and videos were recorded. All the people present at the event had footage covering almost every activity that took place at the event…this information was

> later seen on personal Instagram and Facebook of the people who had attended the occasion.

The data collected indicated that the FGD participants acknowledged that users created various content in form of texts, photos and videos considered to intrude on privacy. However, the students have continued sharing private content on social platforms. For instance, a majority of the participants admitted that when people record audio and video clips in various events, the content is quickly uploaded or shared across a network of friends. This kind of uncontrolled creation and sharing of personal information in form of pictures or videos was considered intrusive by a majority of the participants. The findings of a study by Adams (2012) indicate:

> Social media networks, such as Facebook, have enabled people all over the globe to connect with friends, professionals and strangers in a way that was previously non-existent. The advent of social media sites has transformed the way that people present information about themselves and others. Sharing of private information on the Internet platforms in form of videos and photos is due to the Internet capability to transfer information among the users.

This is in tandem with the observation of Vickers (2012) who states that photography has continuously evolved from traditional print to new pixel-oriented, screen-based and networked practice. The continuous improvement in image sensors has resulted in the innovation of new breeds of camera phones that record Full High Definition (HD) videos.

4.3.5.2 Tagging of Photographs

Tagging of photos is done when a person identifies another by post. By tagging somebody's picture, a person identifies the subject in that particular post. Tagging of photos on Facebook and Instagram was mentioned by many FGD participants. The participants indicated that photos, in most cases, are tagged without the knowledge or the consent of

the concerned persons. The participants said that when tagging is done, it discloses the identities of the concerned persons. One of the participants explained that:

> It is disturbing when old photos of past lives of others are tagged. It has been a common habit, especially where 'throw-back images of the past lives concerning celebrities or public figures are tagged…revealing their early life before fame and money. The content could be truthful about the particular persons but nobody knows if the owners have approved.

Across the focus group discussions, the participants admitted that they often had their photos tagged or have known someone close to them whose photos have been tagged without their knowledge. A respondent explained that:

> Someone tagged my photos in Facebook without my consent and made negative comments about my love affair. I had not been informed and neither had approved of it. The worst is that these comments were done on the timelines and therefore was visible to public.

The Participants who commented on tagging of photos argued that such usage amounted not only to intrusion of privacy but also affected their relationships with the persons who may have viewed the pictures. Some FGD participants were uncomfortable with the tagging of photos citing privacy concerns. The participants agreed that photographs need to be treated as private content. One of the participants also said that celebrities are also intruded on the Internet. The participant said that:

> Many celebrities having relationships have been posted in social media…their own property is put in social media.

Form the responses, pictures are personally identifiable content that was associated with privacy violations by the participants. The Media Council of Kenya Act (2013) requires the media to apply caution in the use of pictures and names and avoid publication when there is a possibility of harming the persons concerned. In Reuters Hand Book of Journalism (2008), material such as photographs could reasonably be expected to cause offense.

4.3.5.3 Unrestricted Production of Online Content

There was evidence of uncontrolled communication activities conducted by the members of the FGDs. In the discussions, participants admitted that everyone who can access the Internet is capable of producing content and communicating to persons connected to them on social platforms. Most of the participants attributed intrusion of privacy to the fact that the Internet has permitted users to create unlimited content on the platforms.

A large number of the FGD participants indicated that they have been authoring content on the Internet. According to the participants, production of content on Facebook, Twitter, and Instagram was a regular practice. For instance, among the focus group participants, six of them said they have created blogs; almost all of them said that they visited the Internet on daily basis; a large number of them said received or sent at least more than 50 text messages in a day. One participant commented that text messages are created '*all the time'*; meaning there is unlimited production and sharing of information through short text messages (SMS). The participants indicated that they were frequently uploading and updating profile pictures on their social accounts. This scenario demonstrates that Internet users generated amounts of information and published it on convergent sites. One participant observed that when such data is uploaded, it can always be accessed by other users. Such data is viewed or retrieved in form of screenshots or downloads.

Other participants felt that such online posts are done for the sake of popularity and getting followers, while some of the posts are done by other people without their knowledge. One participant commented:

> Sometimes people do it willingly, some others don't… sometimes they don't know it is there…It very much depends on exactly the reason behind why people are uploading it, because, when you look at celebrities…they publish so that they can get followers.

It is apparent therefore, that Internet authorship has contributed to uncontrolled proliferation of production of online content. This is in agreement with Kun *et al* (2012) assertion that there is high participation of Internet users in production of content including bloggers, micro-bloggers, and other amateur journalists. The people who have been made subjects of news articles are responding online by posting supplementary information to provide context and counterpoint.

The data from the FGDs, concerning their Internet activities, reflected Henry Jenkins's theory of media convergence (2006). The theory denotes the new communication paradigm as a phenomenon characterized by 'collective intelligence and collective authorship'. In this study, the concept is represented by the involvement of Internet users in uncontrolled production of online media content. The findings are supported by Flanagin and Metzger (2008) who note that, with the sudden explosion of digital media content and access devices, there is now more information available to more people from more sources than at any other time in human history. The communication network is not a single entity any more, but is a conduit, a mechanism to disperse and consume electronic content. The expectation of privacy for any particular delivery mechanism is contingent upon the technology utilized (Davis and Eldridge, 2012).

4.3.6 Nature of Private Data Accessed on the Internet Protocol

When asked to highlight the personally identifiable content they usually witnessed across the Internet, the FGD participants generated a list of the content they regularly encountered on the Internet. Some of the cases mentioned include personal health issues, private financial statuses, family matters or domestic violence. It was noted that when people post information, other users share it further by reposting the same content. Sometimes the

content published generates speculations and conversations about the concerned individuals. The participants agreed that, in some cases, people discuss matters they are not fully aware of. For instance, one participant observed that sharing is done through posting and reposting of issues without proper details. The participant stated that:

> … people share by posting…reposting things that you are not well aware or you don't know much about.

A large number of the participants also agreed that some Internet users unknowingly allow exposure and access to their private information when they log into certain applications or sites that eventually harvest their information. For instance, one participant explained that a user is not allowed to use the application or the site unless they grant the permission requested. The participant explained:

> There are applications or sites that if you log in, they give you a pop-up…and you cannot use the site until you allow them to gather your information. They actually don't even tell you that, they just tell you to probably allow cookies. …some sites are just malicious, when you log in there, they start harvesting data from your phone or from your wall or from your Internet account.

Another FGD participant indicated that the people who conduct business online also disclose plenty of their private details on the marketing sites. The information volunteered contains details that would be considered private. One participant noted that:

> …the details include your name, where you live, how they can get the you, and telephone contacts…

In one focus group, online dating was identified as a common area of privacy intrusion. Most participants, in this particular focus group, supported the observation. They agreed that online dating is a common habit. Participants indicated that Internet users generally

disclosed many details. Generally, the participants agreed that the details shared on such social sites are of private nature. The details mentioned included photos, names, age, careers, level of education including preferences. One participant noted that some people leak conversations by taking screenshots of private conversations. A participant further commented that personal details, such as names and photos shared on dating sites, may be accessed and used to create other accounts by other users.

FG -(*Focus Group Participant*) is a code created to identify participants in a given FGD conversation.

The following are the remarks in the conversation concerning online dating :

FG01: People give a lot of information (*laughing…),* names, pictures…

FG02: Like…the kind of the person you are looking for.

FG03: The age, your age…

Do you smoke?

Do you drink?

What kind of relationship do you want?

FG04: Do you have children?

Follow-up question: What other kind of personal information is shared?

FG04 ...if you have had another relationship.

Follow-up question: Do you think people are intruded on because of the information they give?

Answer: Yes *(in a chorus*)

Follow-up question: Why do you say so?

FG04: Someone might be stalking and you are not interested, so...

FG05: A person can take screenshots of private conversations.

FG06: Your details can be used to open an account by somebody else…names and photos.

This conversation illustrated that infringement of personal privacy on the IP was common. Internet users who upload such private content risk disclosure of their privacy. Gross and Acquisti (2005) state that there are some privacy risks as the Internet users are, perhaps unconsciously, divulging information that might be inappropriate for some audiences in the virtual platforms.

In the FGDs, the participants, generally, demonstrated adequate knowledge of the details that entail personal privacy. However, in as much as this concern and awareness of privacy risks was demonstrated, most of the participants did not seem to refrain from publishing and divulging personal data on the networked sites. All the participants, for instance, indicated that they often uploaded personally identifying information, such as names and photos on their social sites, especially on Facebook and Instagram accounts. A study by Nosko *et al* (2010) found out that there is a high magnitude of information revelation of private information. In 70% or more of the profiles studied, private information revealed ranged from personal profile pictures, date of birth, list of friends, college or university studied, the city lived, consistent wall postings, gender, applications used, Facebook groups, personal pictures, tagged photos and photo albums were openly disclosed and visible to the public. There is concern that people do not realize the implications of publishing online. For instance, the material published will be globally available to other Internet users and some are oblivious of the fact that some of the content will be undeletable.

The findings are corroborated by the study by Adams (2012) that indicates that Facebook allows users to share pictures, status updates, GPS locations, birth dates, and many other

revealing bits of personal information. While the intent of sharing this information is just meant to connect with friends online, many Internet users fail to question whether their information is at risk of being misused. User information can be misused when personal information is leaked to other Internet users or applications. These types of leaks have a considerable impact on users' privacy. The privacy threats can worsen when users neglect reading privacy policies on how user information can be secured. Mendel *et al*. (2012) surveyed the global Internet privacy and freedom of expression and observed that:

> While people are often concerned about privacy in the abstract, they seem less concerned about privacy in practice. It is clear from a cursory use of the Internet; people give out personal information to a surprising degree.

In this section, Internet users' activities emerging from the FGDs depicted a constant usage of multimedia technological devices in production and consumption of Internet content. In the conceptual framework, this research presumed that multimediality of media convergence plays a role in intrusion of privacy of Intermit users on the media convergent platforms. This is consistent with Henry Jenkins' media convergence theory (2006) that proposes that new technologies in different communication platforms have redefined the media environment and reshape everyday life in terms of media consumption and creation. In this research, most of the focus group participants admitted that they freely divulge their information on social sites. The participants' online activities exhibited unrestricted production and consumption of user-generated content. The Internet users may require more awareness on Internet usage and ICT products, to understand the potential privacy risks involved in divulging personal information on the convergent networks.

Table 4.2: Internet Activities and Invasion of Privacy

Private content	Names, photos, ID numbers, telephone contacts, age, relationships, family life, health issues, properties, place of residence.
Applications and Tools	Facebook, Instagram, Twitter, Imo, Telegram, LinkedIn, blogs, WhatsApp. Smart camera, Search engines, web browsers.
Unrestricted Activities	Photographing, filming, uploading of photos, downloading, updating profiles, creating social accounts, posting, re-posting, tagging of photos, screenshots, photoshop, texting, commenting, searching the Internet,

4.4 Hypertexuality and News of Shock, Violence, Crime and Sexual Assaults

This section focused on the second objective of the study that sought to determine the contribution of hypertextuality in publication of news of shock, acts of violence, crime and sexual assault.

The section aimed at answering the following research question:

What role does hypertextuality play in real-time streaming of shocking news, acts of violence, crime and sexual assault?

This segment consists of data analysis based on the responses emerging from the FGDs on the role of hypertextuality in the production and publication of content related to the following aspects: i) News of shock, ii) Acts of violence and crime and; iii) Sexual assault.

According to the Media Council of Kenya Act (2013), news of shock involves the publication of horrific images showing mutilated bodies, bloody incidents and abhorrent scenes. Acts of violence involve acts of armed robberies, banditry and terrorist activities, genocides, and war-like activities, ethnic, racial or religious hostilities; while, sexual assault involves cases of rape, defilement, incest or sexual harassment which can consist of a single intense or severe act, multiple persistent or pervasive acts.

Hypertexuality of the Internet permits production and publication of extensive content on the convergent platforms. Hypertextuality involves creation of a variety of content in form of texts, sounds, pictures or graphics on the Internet Protocol. According to Kammer (2013), Internet hypertextuality supports the embedding of material from different websites and Internet applications platforms or feeds from other networks, sites and micro blogging applications such as Twitter and Facebook.

4.4.1 Publication of News of Shock

The participants in the FGDs observed that shocking information is often published and accessed on the Internet social sites. A majority of them admitted having either encountered, received or posted information concerning news of shock to other users connected to them on the social platforms. The cases frequently identified by the participants included experiences of distressing text messages, videos and graphic images. A large number of the participants agreed that people use their multimedia devices to search and share such stories. The information highlighted included content displaying shocking scenes with injured and bleeding victims, dead bodies, scenes of accidents, domestic violence, victims of hunger, murder, persecutions and suicide.

For example, in one of the FGDs, some participants provided the following responses:

Question: What shocking information have you encountered on the Internet?

FG01: I have seen mobs lynching criminals.

FG02: Images of people suffering from hunger.

FG03: Dead bodies…bleeding bodies.

FG04: Videos of people being killed… videos of religious persecutions.

Follow-up question: What do you think the relatives felt when they saw the videos?

Answer: The fact that it was all over the media, the family must have seen…and felt bad about it.

Follow-up question: And you? what did you feel?

FG04: I felt bad because it was torture.

Such materials were commonly posted by people who filmed the scenes. The information is then posted further to groups or individual social sites. One of the participants stated that:

> People arrive at the scenes of accidents before the police and they start taking videos and photos…they post them.

Some participants indicated that their Internet experiences were unpleasant and disturbing. Other participants felt that the intrusion on the privacy of the concerned victims and their families is unwarranted. One participant noted that:

> …Some of these contents are usually too graphic and are disturbing, for example, photos of badly injured, bleeding or dead bodies…in some cases, it creates curiosity and causes

more and more people to search the Internet for more information.

The findings indicate that there is unlimited production of shocking information by Internet users. The Media Council Act of Kenya (2013) guides the practice and outlines the expectations of persons publishing news of shock. The Act recommends that in cases involving news of shock, inquiries should be made with sensitivity and discretion should be advised. This is a demonstration that sharing of materials related to shock leads intrusion privacy of the affected persons. Therefore, such publications are seen to be inconsistent with the requirements of the Act.

As Dwyer and Fiona (2012) observe, there a need for moderation attempts to create a balance between ethical expectations for online users' privacy and self-expression, reliability, accountability, accessibility and security. Similarly, a report produced by the Media Council of Kenya in collaboration with the International Media (Special Edition, Kenya, 2014) implores journalists to treat victims they approach at a tragic event with sensitivity, dignity and respect. In the report, journalists are cautioned, as they record graphic and bloody images, to consider whether the content is essential enough for historical purposes or if it is too graphic for the readers or viewers.

4.4.2 Acts of Violence and Crime

In the FGDs, many of the participants admitted that they often encountered content displaying traumatizing scenes of crimes and violence on the Internet platforms. The participants across the groups indicated that Internet users, in some cases, publish identities of both the victims and the perpetrators of crimes. Most of the participants observed that publications of identities are done with little or no considerations of the victims and the feelings of family and relatives. The Independent Press Standard Organization (IPSO) Editors' Code of Practice (2019) requires that, when reporting on crime, relatives should not be identified without their consent.

The participants across the FGDs mentioned a range of Internet content related to violence and crime frequently posted on social platforms. The content identified includes news of wars, shootings, bombings, police brutality, sieged hostages, terrorist attacks, ethnic clashes, robberies, mob justice, executions and threatening text messages. From the focus group participants, some of them personally identifiable content frequently published included showing the faces of victims in photos and videos, publishing of names and text messages that identify the victims.

It was indicated that news on incidences of crimes and mayhem are circulated shortly after happening hence; jeopardizing the privacy of the affected persons and their relatives. One participant commented:

> Mostly, a lot of the information shared concerning violence, apart from being informative, causes fear. Some contents published are exaggerated to make people panic…sometimes it is confusing and can interfere with privacy of court processes in cases where investigations are being conducted because it can leak information required to pass judgement.

The responses demonstrated that personally identifiable content published on acts of violence and crime may jeopardize the privacy of the concerned individuals. One FGD participant noted that the exposures that identify persons involved in crime or violence could also have some unforeseen but far-reaching privacy risks to the victims. The participant noted that:

> In some cases, people won't be able to get jobs, because, during the interviews, they would like to know everything about you and they will search and if they ever find something that you ever did…so automatically you won't qualify.

As Erdal (2007) comments, in a cross-media environment, dynamic media contents are republished on the web, alongside texts and still images. Tran (2015) proposes that privacy torts laws are suitable to regulate the illegal distribution of sensitive information not meant for public dissemination. Concerning reportage of news of traumatic and conflict situations, the Media Council of Kenya underpins responsibility in news reportage and that effort is made to offset some of the hazards of exaggerated rumors that promote fear and violence (Media Council of Kenya Act, 2013). A study by Gómez-Díaz and Arroyo-Almaraz (2015) revealed that it is not palpable to control activities enabled by the new media, but rather, it is important to understand to what extent the advantages of incorporating digital communication technologies could contain certain, as yet unseen, disadvantages.

Some of the participants noted that personally identifiable content such as pictures, names, place of residence or family members of the victims affect other innocent persons. It was noted, for instance, that exposing names and pictures of people involved in crime or violence during traumatizing moments embarrasses family members and relatives. For instance, a participant commented that:

> If the identity of criminals is exposed, innocent family members are disgraced and also information uncovered affects the family members who in the first place, did not take part in the crime.

Another participant observed that:

> Personally, I feel that it is good that people know that the person is a criminal, but...the family will be concerned that…now our son is a criminal…so it has two sides.

Another participant stated that eyewitnesses and reporters may be exposed to risks if they are displayed to viewers:

> In cases of crime, the eyewitnesses and the investigating reporters are exposed to great risk as they are visible to the public while volunteering sensitive information and the criminals involved might plan to retaliate by striking back on the persons because it is possible to identify them.

In Kenya, media ethics require the media to avoid presenting acts of violence, armed robberies, banditry and terrorist activities in a manner that glorifies such anti-social conduct including social evils, warlike activities, ethnic, racial or religious hostilities. Such publications do not serve any legitimate journalistic or public need and may bring social opprobrium to the victims and social embarrassment to their relations, family, friends, community and religious order and to the institutions to which they belong (Media Council of Kenya Act, 2013).

4.4.3 Publication of Content on Sexual Assault

Publication of news on sexual assaults involves the circulation of content related to incidences of sexually related violations or such as rape, defilement or incest. Publication of content that positively identifies the victims or their relatives is prohibited (Media Council of Kenya Code of Conduct for Journalists, 2013; IPSO Editors' Code of Practice, 2019).

Concerning intrusion on victims of sexual assault, a majority of the FGD participants admitted that invasion of privacy of people involved in sexual violations is prevalent on the convergent networks. The FGD participants observed that they frequently witnessed content that could lead to the identification of the sexually assaulted persons. The participants noted that the content is published and circulated freely on Internet social sites. For instance, some of the identifiable content include pictures and names of the victims, relatives, age, or place of residence. In some cases, images of injuries on victims, scenes of assault, pictures of the victims and their perpetrators are posted on the networked platforms. The participants noted that people download and share such pictures and video

clips through their networked platforms and keep forwarding them to their friends or group of friends in, for instance, WhatsApp and Facebook.

In the cases of sexual assaults, participants also argued that content that identifies the perpetrators affects other people such as family. Many of the respondents concurred that this kind of exposure is detrimental because it leads to invasion of privacy of innocent persons. Findings indicated that such exposure is stigmatizing because the content may keep reappearing on social sites for a long time. One of the participants observed that:

> Content that provides victims' identities is offensive because it causes serious intrusion into concerned peoples' privacy…some of the materials commonly posted involve vulnerable persons…If videos are recorded or published, they keep reappearing on social media hence compromising the protection of privacy of the victims.

Some of the vulnerable persons mentioned include women, girls and children. From the conversations, when victims of sexual assault are exposed, it leads to re-victimization. As one participant noted, the victims who are identified are affected:

> We can also talk about the victims themselves…the ones who undergo the action can face shame…

According to the FGD participants, the content they mostly witnessed had been recorded and circulated in form of videos. The following conversations indicated that videos with identifying materials are often posted on the platforms:

FG01: There was a video of a man raping a baby.

FG 01 (*continued)*…and also a video of a house-help, a female one, defiling a one-year-old boy.

FG02: There was a case where a girl was raped and it was recorded…it was posted on a pornographic site…

FG03: ...also, this time when women were being…just undressed by men in the street, it became a trend…that's why they came up with 'my dress my choice'…it was happening here in Kenya.

FG04: I have seen videos of half-naked girls, undressed… crying, in public.

Some participants also commented on use of photos. One of the participants indicated that nude photos with identifiable content are posted on social platforms. Others said that nude photos are not always real but are edited through photoshop:

FG05: Some people post nude photos… some are photoshops

Another FGD participant observed that:

> People use other people's images and make memes with sexual content and post them.

Most of the participants in the FGDs indicated that Internet users who created or publish content that facilitates identification of victims of sexual assaults overstepped the privacy rights of the concerned persons. The nature of the content was considered to jeopardize the privacy of victims of sexual assault.

Universally, media ethos is against the disclosure of personally identifiable information in cases involving sexual assault. Providing names and pictures that might identify the victim is discouraged. For instance, the Bhutan Information Communications and Media Act (2006) provide that media should not identify victims of sexual assaults or publish materials likely to facilitate such identifications. The Reuters Handbook of Journalism (2008) states that, occasionally, journalists may encounter, witness or record scenes of a sexually graphic nature. In such cases, the reporters have the obligation of accurately relaying the reality, yet it is also their duty to care about the content that can cause distress, damage the dignity of the individuals concerned or even so overpower the audiences so

that the rational understanding of the facts is impaired. In a nutshell, journalists should not sanitize violence, bowdlerize speech or euphemize sex or publish graphic images and details or obscene language gratuitously or with an intention to titillate or to shock. Graphic material may not be suitable for general audiences just as sexually explicit photographs may be more acceptable in one part of the world than another.

The theory of media convergence by Henry Jenkins (2006) depicts media convergence as a media arena represented by technological shift with a new audience and transmedia storytelling. The theorist proposes that media convergence represents a postmodern communication pattern that indicates a participative process. This aspect of media convergence is demonstrated in this study as the findings indicate that the study participants witnessed, created or shared content on news of shock, acts of crimes and sexual assault. The conceptual framework of this study presented hypertextuality as one of the indicators of media convergence. It was presupposed that hypertextuality permits the production of huge content that may intrude on privacy. This was confirmed by the online activities and the content witnessed on the Internet social sites. The availability of digital devices affords Internet users opportunities to produce and share materials that intrude the privacy. As Kun et al. (2012) observe, social networks enable interpersonal connections between users, increasing the speed for news information to travel across the social groups permeating society in vast scope and depth.

4.5 Interactivity and Intrusion on Grief

This section addressed the third objective of the study that focused on role of Internet users' interactivity in intrusion of bereavement and personal grief.

In this section, the study sought to answer the following research question:

What is the role of Internet users' interactivity in intrusion of bereavement and personal grief?

4.5.1 Nature of the Cyberspace that Supports Real-time Interactivity

Internet connectivity refers to the inter-linking or accessibility of network communication servers over the World Wide Web (WWW). According to Cowles (2009), the early pioneers of the Internet envisioned a world without states in which abundant "free" information would equalize social relations. This communication environment has intensified the production of huge data by Internet users. The content is extensively transmitted on the current virtual networks instantaneously in real-time.

4.5.1.1 Virtuality and Internet User Connectivity

The focus group discussions demonstrated Internet users extensively connect on the virtual platforms through various applications. They also use other Internet tools such as web browsers to search for information. The participants noted that the Internet social networks and search engines are responsible for easy faster interaction among Internet users. For instance, as indicated earlier, all the participants in the FGDs had their mobile phones already connected to the Internet.

Many of the participants indicated that they were registered in various social networks such as Twitter, Facebook, Instagram, WhatsApp, Imo, WhatsApp or telegram. The participants were using interactive platforms and applications to send and receive messages. One of the participants explained that it is easy to access and post content because the Internet is available and accessible. The participant noted:

> The Internet is easily accessible and available…if I have a smartphone... I just go to the Internet and post videos.

Another FGD participant described the activities that can be carried out by a mobile device that is connected to the social networks:

> With a smart mobile phone, I find it easy to capture information by recording audio, filming or photographing. I

> can share…with friends…My mobile phone is also connected to Internet with browsers and Internet explorers that help me to navigate the Internet when searching for information.

As Kalamar (2016) notes, with the introduction of 2.0 Internet, the reorganization of network and the new media podium and services convergence, the audiences have transformed by being integrated into modern digital infrastructures with numerous interactive possibilities.

From the FGD discussions, intrusion of privacy of people in bereavement and grief is attributed to the connectivity of communication systems, smart devices, transmission techniques, speed, and applications used in online media environments. One of the participants stated that it becomes easy to send information due to the speed of Internet communication. The participant, for instance, observed that it is easier and faster to communicate and, hence; many people were communicating on the sites by posting, reposting and tagging:

> …the fact that Information spreads very fast because there many people using the Internet. So, when somebody posts, they will post, repost and tag…

The respondent also commented that such kind of information spreads fast and also, becomes hard to withdraw content once posted:

> …so, in a minute the information is spread...when something is posted on the Internet, it becomes so hard to pull it down.

As indicated before, some FGD participants also mentioned some applications that connect devices and share information within their vicinities such as Bluetooth, Xender and Flashshare. These applications are used to pair and transfer data from one device to another. The moment people get the content, they also upload it and send it to their friends. The

findings from the FGDs, therefore, illustrate that it has become easy and fast to engage in communication on the convergent platforms. The social networks have become openings for sharing content that would often build distress, especially in transmitting sensitive death messages and images of deceased people and their families. This finding is supported by Kun *et al.* (2012) who assert that people easily access, make comments, produce content, and publish news on the Internet protocol. Tran (2015) also concurs by elaborating that:

> The proliferation of smart technology…are culminating in a technological phenomenon encompassing networks of Internet communication. The Internet has now ended the monopoly of news institutions and weakened the government's ability to censor information. With the help of digital devices such as PCs, cell phones, cameras and digital video, Internet users and journalists have made an abundant contribution to news on the Internet. However, this vast amount of linking, republishing and sharing leads to explicit sensationalizing of incidents involving private content.

In this study, connectivity of Internet users was associated with unrestricted production and spreading of information related to bereavement. The findings are consistent with the assertions of Henry Jenkins, in the theory of Media convergence, that media convergence is characterized by changing media, changing audiences, participatory communication cultures and collective intelligence that enable production and consumption of large amounts of data on the Internet. James Moor's theory of privacy also proposes that media convergence represents a postmodern communication pattern that indicates a participative process. In this study, this fact was qualified by the evidence of proliferation of user-generated content on the IP. As Moor argues, individuals or groups have privacy, only if, in a situation where the information related to them is protected from intrusion, observation and surveillance by others. AMWIK (2014) and the Media Council of Kenya Act (2013) generally advise sensitivity in information sourcing and publications of content with identifiable materials such as pictures of deceased persons or when covering scenes of disasters.

Table: 4.3: News of Shock, Acts of Violence, Crime and Sexual Assault

	Activities	Identifiable Content
News of shock:	Texting, taking photos, audio recording and uploading of videos.	Images/ photos Videos Names
Acts of violence and crime:	Filming scenes of violence. Posting live scenes and acts of violence and crimes such as terrorism, war, murder, police brutality, shootings, robberies, mob justice.	Names and images of Victims of Violence, Perpetrators of crime Relatives Eyewitnesses
Sexual assault:	Filming videos posting and reposting of content Commenting/ texting Publication of embarrassing content Photoshop Creating memes	Names Videos on rape and defilement Pictures of victims Nude photos

4.5.2 Internet Activities Intruding on Bereavement and Grief

The majority of the FGD participants admitted having had regular encounter materials concerning matters of bereavement and grief being circulated by Internet users. Some of the content mentioned consistently by the participants in the FGDs included online stories about the cause of death or comments on kinds of ailments resulting in the death of individuals, messages of murder, suicide, mourning and publication of funeral functions. The study by Kammer (2013) supports Jenkins's (2002; 2006) concept of media convergence that, digital convergence has prompted transformation roles in journalism to

embrace inclusivity and participation of audiences. With the new convergent networks, it is now apparent that skilled reporters are no longer the only creators of news content. Internet audiences have been making and disseminating huge media content. This has promoted audience involvement. Communication has become more interactive and more prevalent on various social networks and convergent spaces.

4.5.2.1 Production of Multimedia Elements

The data from FGDs illustrated the availability of smart devices with a variety of functions that enable users to conduct different tasks. As noted earlier, the devices can record or capture content in various formats such as videos, photos and audio content, thus, increasing publications. Some of the materials published include situations where individuals are undergoing personal grief.

The following is a conversation concerning the production of content on bereavement:

Question: What activities commonly intrude on bereavement and personal grief on the Internet?

FG01: They start making funny memes from the images.

Follow-up question: Memes about who?

FG01: About the person who is bereaved… the one who is crying.

Question: What else do people do to intrude on privacy?

FG02: They record videos of the burial sessions.

Follow-up question: Is a burial session private?

FG02: Yes (*In a chorus*)

Question: What makes you think the habit is intrusive?

FG03: Immediately the video gets out there, …people are different, some will criticize. People even go to an extent of even looking at how people were dressed…who reacted badly, and then they start commenting.

Question: Is that the only thing that people do?

FG04: They start talking about the peoples' (*the bereaved family*) background.

As Hanrahan (2004) remarks, the convergence has incorporated the multi-service features where a device or facility supports multiple services or a network of services:

> ….embraces multi-function features where multiple services are supported on a single terminal. The convergence also permits extended functionality features where different infrastructures are inter-worked and also adopt the versatile feature, where a service or content delivered through different infrastructures or different media diverse equipment, works in a single standard interface of mechanism.

One FGD participant explained that such news of bereavement, sometimes, is important to the public but the motive and the impact must also be considered. The participant elaborated that:

> It is one thing to keep the audiences informed and it is another to protect the privacy rights of the bereaved families...some people publish such content because they want to make and sell news. Such news attracts public attention and is viewed the most in social networks, such as Facebook or Twitter…People use mobile phones to take pictures or record videos of the scenes of crime or accidents and forward to others, exposing the dead to their families and to the general public.

As Yualabi (2014) asserts, media convergence does not only afford users opportunities but threats as well, as the technologically developed societies have ushered in the digital phase, and media businesses are contending with new opportunities and threats occasioned by what is called 'convergence'. Calvert (2006) expounds that:

> …autopsy photographs, death-scene, images of suicides, pictures of the dead in both open and closed caskets, tapes and transcripts of emergency telephone calls that contain victims' dying words are frequently found at the center of privacy of death controversies. The issue frequently boils down to the question of how to strike a proper legal balance between the publics' right to newsworthy information about the dead and concerns for the family's privacy rights, emotional tranquility, solemn respect and dignity. This right should therefore focus on the ability of the person(s) to gain a substantial control of publication regarding postmortem reports, images or messages concerning the death of their departed family members or relatives.

The Reuters Handbook of Journalism (2008) requires the reporters to treat victims with sensitivity and to avoid causing needless pain and offense. According to AMWIK Journalist Handbook (2014), the public's right to know shall be weighed against the privacy rights of people in the news, intrusion and inquiries into an individual's private life without the person's consent are generally not acceptable unless public interest is involved. Public interest shall itself be legitimate and not merely prurient or morbid curiosity. The Universal Declaration of Human Rights reaffirms the right to privacy where no one may be subjected to arbitrary or unlawful interference with his/her privacy (UNHR, 1948). Protection of personal privacy is also underscored by the Vienna Declaration and Programme of Action (1993), the Media Council of Kenya Act (2013), and the Kenyan constitution (2010). Kun *et al.* (2012) also assert that publication of content about the

departed family members alienates the legitimate privacy entitlements that the concerned person(s) should be afforded.

The FGD participants also indicated that the urge for information is a cause for searching for information on surprising occurrences and happenings such as tragedies involving grief. Participants mentioned some of the practices they considered intrusive including taking photos of the dead filming, downloading, uploading, texting, commenting, publishing of speculations and posting of memorial and burial services without the knowledge or the consent of the concerned persons. One FGD participant explained that:

> When people hear of rumours and bad news concerning death…news concerning murder, suicide or accident, out of curiosity, people quickly use their smartphones to browse the Internet for the breaking news and then download such content. The chain of sharing continues because they also share the content with other people they are connected with and the messages are forwarded on and on through Instagram, WhatsApp, Telegram or text messages...

In the conversations of one FGD, on publications of messages of death, there was an argument as to whether it would be considered intrusive in cases involving public figures. For instance, one participant argued that:

> Although everyone deserves privacy protection during grief, if such news involves public a figure, it should be treated as a necessary source of information for the public because people are interested in information concerning prominent persons; because what affects public figures, affects the society.

The participants demonstrated that Internet users are always looking for new information. An FGD participant explained that it is difficult to assure the bereaved families of protection from privacy violations as people yearn for more and more information:

> …eyewitnesses of such disasters take and post pictures and videos…others are searching, downloading, commenting and re-posting further to other people.

It was noted that in such times, the Internet is usually awash with graphic images identifying the dead by pictures or names. The participants have been involved not only in searching for content but also in its creation and publication on social sites.

From the FGD conversations, the personal privacy of bereaved persons and families is being invaded particularly when consent is not obtained before such publications. This finding from the conversation above is supported by Sumartias and Hafizni (2017) who observe that innovation and multimodal convergence is being experienced where content convergence is evident:

> News is being presented in the form of multimedia formats combining text, images, podcasts, audio, video, slideshows and blogs. Internet users, therefore, are endlessly transmitting multimedia concerning global happenings.

The FGD participants, therefore, agreed that people seeking breaking news on bereavement and grief search the information online to satisfy the urge for information, especially, in cases involving popular personalities. From the discussions, media convergence has supported unrestricted authoring of content on bereavement by Internet users leading to little control over the flow of data traffic in the online spaces. Kalamar (2016) argues that:

> We cannot just study convergence without consequently paying close attention to the audience and its transformation.

> The basic tenet is that audiences are active and make media do things to serve their purpose.

A Report on privacy and media intrusion by the Law Reform Commission of Hong Kong (2004), records the results of a poll where 89% of the respondents interviewed indicated that:

> It was improper to publish pictures of the uncovered bodies of deceased persons. The publication of such photographs was considered disrespectful to the deceased persons and an affront to the dignity of the deceased.

In the same tone, in a report produced by MCK and the International Media in 2014 dubbed '*Images that Stay Forever'*, journalists are advised to avoid violating peoples in their grief by recording photos of emotions at public scenes. Journalists are also discouraged from intruding upon private property or causing disturbance to the victims in their grieving process.

As the theory of privacy by James Moor (1997, 2004) proposes, an individual has privacy only in a situation where one can exercise control over personal information. As Moor argues, personal privacy should be maintained through non-intrusion, non-interference and restricted access to personal information. On the contrary, findings from the FGDs illustrate that Internet users were involved in production of a wide range of data concerning bereavement. Findings further indicate that a lot of content was shared through the social interactive sites, hence, intrusion of the privacy of bereaved persons on the social platforms was common. As illustrated in the conceptual framework of this study, findings portrayed that interactivity of media convergence plays a substantial role in infringement of privacy of bereaved people in their moments of grief.

Table 4.4: Aspects of Media Convergence that Support Interactivity

A**spects**	**Activities**	**Identifiable content**
Internet user connectivity/virtuality.	Filming/Video Photographing Uploading Downloading	Videos with graphic content- lifeless bodies Messages of murder News stories on suicide Mourning messages Videos- funeral, ceremonies
Production of multimedia elements.	Publishing Sharing/Circulating Commenting.	Commenting Memes.

4. 6 Conclusion

This chapter focused on the analysis of the data from the FGDs concerning multimediality of media convergence and its role in the proliferation of user-created content on private information. The chapter also analyzed the data on the influence of hypertextuality on publication of news of shock, violence, crime, sexual assault and intrusion into private grief on the media convergent platforms.

From the FGD discussions, findings indicated that multimediality allows the production and distribution of private information in form of different media formats including videos, texts and photo images. Participants used their smart devices to share the multimedia contents without restrictions, therefore, intensifying activities associated with intrusion on personal privacy.

The participants identified the devices used for online communication and the functions conducted using multimedia devices, applications and software. Internet users' practices that aggravate intrusion of privacy and the private content witnessed on the convergent

social platforms were also analyzed. It was noted that, although the majority of the participants admitted that privacy intrusion was high, most of them did not demonstrate keenness in preserving their privacy. Most of the participants divulged identifying information such as names, ID numbers, location, age, places of residence, phone numbers or photos on the Internet social sites. This fact points to the need for creation of awareness concerning the privacy risks posed by the exhibited Internet habit.

The materials witnessed by the participants illustrated that hypertextuality of media convergence has supported Internet-user activities that infringe on the privacy of other users on the Internet platforms. This suggests, as advanced by Henry Jenkin, that hypertextuality of media convergence has altered audiences where the audiences assumed a more participative role in creation and distribution of information. Findings showed that the participants witnessed, created or shared content on news to shock, violence, crime and sexual assault. Findings further illustrated that the content was circulated across the Internet social platforms with no restrictions.

On intrusion of personal grief, findings demonstrated that the virtual nature of the Internet, user-connectivity, production of multimedia elements and seeking for information were associated with production and distribution of data which often involved real-time circulation of news of bereavement and grief. Accessibility of easy-to-use Internet tools was deemed to aggravate access and dissemination of intrusive content on social sites. From the aspects of media convergence examined in this chapter, such as multimediality, hypertextuality and interactivity, findings generally demonstrate that intrusion of personal privacy on the Internet social sites was being experienced.

The next chapter presents data analysis from the key expert respondents from government institutions related to communication. The chapter focused on data analysis on the strategies of mitigating online privacy infringements.

CHAPTER FIVE: STRATEGIES FOR MITIGATING PRIVACY INFRINGEMENTS

5.1 Introduction

This chapter focused on the fourth objective of the study. The objective sought to explore the strategies for mitigating infringement of intrusion of online privacy. The chapter presents a qualitative analysis of the responses from the eight key experts sampled for the study. The data analyzed in this chapter was obtained through face-to-face interviews by use of the interview guide prepared for the study. These respondents provided expert opinions and specific insights that helped to explore mitigation strategies for guarding against online infringements of privacy.

In this chapter, the study sought to answer the following research question:

What are the strategies for mitigating infringements of online privacy on media convergent platforms?

Table 5.1: Interview Response Rate

Institution	Proposed Sample	Actual Sample
The Media Council of Kenya (MCK)	4	3
Communications Authority of Kenya (CA)	3	3
ICT Authority of Kenya (ICTA)	2	2
TOTAL	9	8

This study identified highly skilled staff in terms of expertise. The respondents were drawn from government institutions related to communication. The areas of the eight key

respondents included: i) Media Council of Kenya- Media Analyst and Monitoring, Media/ICT and Accreditation and Compliance; ii) ICT Authority- Programmes and Standards and, ICT and; iii) Communication Authority of Kenya- Multimedia Services, Legal Services and Cybersecurity. The response rate was eight out of the proposed nine respondents. The media monitoring and Media Analyst at MCK is under one department and not two as anticipated. Therefore, one respondent was interviewed from the department.

The key respondents in this study were represented by specific individual codes assigned by the researcher. The individual codes were used to represent the identities of the respondents to maintain the confidentiality of the participants. This is consistent with Mugenda and Mugenda (2003) who recommend that, in research where anonymity is required, the real identities of participants are represented by an individual code. Individual codes for research respondents may be in form of numbers or a pseudonym generated to link the respondent with the data provided. In the data analysis throughout Chapter Five, respondents were therefore referred according to the respective codes. The following table presents the identity codes assigned to the Key respondents.

Table 5.2: Respondents' Identity Codes

Expertise / Area	**Identity code**
Cybersecurity	01CS
Multimedia Services	02MS
Legal Services	03LS
Media Monitoring and Analyst	04MM
Media/ICT	05MT

Accreditation and Compliance	06AC
Programmes and Standards	07PS
ICT	08CT

The data in this chapter was thematically analyzed based on the responses of the key respondents to the questions in the interview guide. This approach to data analysis is consistent with Kumar (2011) who observes that, in qualitative research, findings are mostly communicated in descriptive discourses or narrative format written around the major themes. As previously indicated in Chapter Four, the researcher has also provided summary tables of the responses in various segments of this chapter.

The data was analyzed according to respective themes in alignment with the interview guide. To explore strategies of mitigating online infringements, the researcher had to establish the prevalent privacy invasion issues related to Internet usage, the factors that escalate infringements of online privacy, the nature of the Internet that limits protection of privacy of Internet users, and the aspects of the Internet undermining regulation of online communication on the convergent platforms. The data on mitigation of infringements of online privacy was also analyzed.

5.2 Prevalent Privacy Issues Arising from Internet Usage

The key respondents identified the prevalent privacy issues occasioned by Internet usage. The issues that emerged from the interviews included harvesting personal data, disclosure of confidential information, susceptibility of social sites and fake news.

5.2.1 Harvesting of Personal Data

Data harvesting involves retrieving, extracting or collecting information from an online resource. Some of the key respondents concurred that, in some cases, private data is

accessed raising various threats to online privacy. Data harvesting was linked to various privacy infringements including data breach, data theft, impersonation, identity theft and cyberbullying.

Respondent 02MS explained that there is access to a lot of private data leading to data breach and theft. The respondent explained:

> One is the aspect of data breach. Data breach is one of the things many people are experiencing. A lot of data which was not supposed to go out there to everybody is being seen by everybody.

02MS further stated that data theft is another concern that arises from harvested data:

> The last one which is the big thing is the issue of data theft where people can hack into your Facebook, get details about you…get details about your children…

Follow-up question: So, you can confirm that people are harvesting data?

02MS: What we can say is that the way the Internet is structured, it is possible for people to harvest a lot of data.

In the FGDs, participants indicated that Internet users access private informant through downloads and screenshots. Respondent 01CS noted that identity theft is a cybercrime where personally distinctive data, such as names, telephone numbers or banking details are accessed by unauthorized parties. The respondent noted that such data may be used for personal benefits including financial gain. The respondent explained that persons may use the unique details to impersonate others by masquerading as the real owners. Respondent 05MT and 02MS also agreed that fraudsters normally claim to offer valuable services to their target victims. Respondent 05MT, for instance, explained that clients are mostly invited to click on the provided web links or to make payments. The respondent further indicated that there are people who go online purposely to collect information. The data

collected may be used for fraudulent dealings through impersonation. This is replicated in the FGDs, where findings indicated that personal details including names and photos can be stolen and used to create new social accounts. The respondent 05MT noted that:

> …one is impersonation. If persons manage to collect your information and impersonate you online, they can easily convince other people that they are actually dealing with you.

Respondent 01CS commented Internet users use multimedia devices that are versatile in connectivity and web navigation capacities. The respondent also noted that there are incidences where people have been swindled in fake charities after their private data is harvested. For instance, the respondent indicated that there are widespread fake schemes involving in peddling attractive stunts claiming miracles cures or awards in fake betting games.

From the above responses, data harvesting has led to the proliferation of fraudulent activities. As Singleton (2013) explains, identity theft happens when a cybercriminal successfully steals an individual's personally identifiable information. Identity theft, therefore, serves as a major gateway to other cybercrimes including credit-card fraud, loan fraud and other similar crimes. The costs to victims of this type of cybercrime can involve both damages of public image and financial costs in form of loss of business, legal expenses and avoidable cost of installing security structures.

01CS also explained that personally identifiable data may be cross-shared by Application developers. The respondent explained that there are incidences when a user intends to sign into a certain platform and the pop-up message request the user to sign in either through email or through another App. This means that different Application developers can cross-share details of their subscribers. According to the respondent, this practice raises privacy concerns because a third party has accessed the data of the user.

Respondent 02MS attributed data harvesting to the way society is socialized. The respondent also indicated that personal data can be accessed through hacking. The respondent indicated that:

> Also, the way we are socialized…we are socialized in a way that we are not so much security-aware...we go to Facebook comment on where we are, what we are doing. It looks like just a social interaction, but we are not aware that the information is not only private but is also somewhere and some other person can hack into that information and get it.

The above response represents the activities of the FGDs participants. The participants were involved in extensive interactions in their online activities that included sharing of personal content. Respondent 01CS also added that personal data can be used in cyberbullying. The respondent noted that:

> People will only attack what they know…because the owners have shared it with others.

Respondent 05MT and 01CS commented that user-generated information often leads to privacy violations. For instance, 05MT explained that most Internet users are generally oblivious of the privacy risks involved:

> …most users don't know…some of the information they are putting online…they are exposing their own privacy. This information can later be used. Users have no control of what happens to that information, like…is it retained? is it stored? is it destroyed?

Respondent 08CT noted that, sometimes, employers require potential employees to submit substantial personally identifiable data. Hence, employers are able to access, collect and store private information concerning their employees. In the theory of privacy, James Moor

(2004) argues that, as private information is stored in computer databases, people have no control over the usage of the stored information. Bijone (2016) observes that personal data should be protected by reasonable enhancement of security safeguards against risks such as data loss or access by unauthorized parties, destruction, usage, modifications or even disclosures over the complex networks.

Respondent 07PS noted that there has been duplication of data sets that entail individuals' personal information in various institutional systems. The respondent, however, noted that the government intends to minimize the data created on individuals. The respondent commented that:

> The government is planning to develop a standard data set…the minimum information that can be collected from an individual…one source of data…what I would call, 'one source of truth'.

The International Labour Organization (ILO) (1997) emphasizes the principle of protection of workers' data. The principle, in part, requires that:

> External communication of data should respect the principle that workers' data be processed only for purposes connected with the specific employment relationship…an equally important restriction follows from a principle stressed by national and international regulations on data protection, namely that the collection of personal data does not entitle the employer to make free and unlimited use of the information gathered. When indicating the specific purposes for which the data are collected, all future uses must also be indicated.

As James Moor argues, in the theory of privacy, the contemporary electronic age is a communication environment that has presented uncertainty about the protection of

communication protonorms. Moor notes that the merging communication media platforms enable users to extract information from many discreet and unrelated databases and incorporate it into composite information files. This concept supports Henry Jenkins' notion of media convergence that the convergent platforms permit extensive access to varied information.

5.2.2 Disclosure of Confidential Information

Disclosure of confidential data was identified by several of the key respondents as a prevalent privacy threat. Respondent 02MS observed that private data has been, in some instances, shared for commercial purposes by Internet Application developers without the consent and the knowledge of the Internet users. The respondent indicated that this kind of information disclosure is a major concern. The respondent stated:

> …the aspect of unauthorized disclosure of information basically by the big giants (*Apps developers)*...and selling the same to advertisers so that advertisers can use that intelligence to give specific advertisements to specific people depending on how much data they have gathered from the social media platforms. That is the elephant in the room.

Respondent 01CA commented that information disclosure occurs by revealing private data to unauthorized persons and therefore jeopardizing the privacy of the data subjects. The respondent explained that information disclosure may occur through unpremeditated leakage in the process of undertaking regular tasks. Respondent 07PS also concurred that information disclosure can happen through accidental loss of data storage devices. Both 01CS and 07PS indicated that employees, in some instances, may release information entrusted to them. Respondent 01CS commented that, in some incidences, forensic investigations may be conducted.

As Gordon (2007) asserts, organizations are at risk of deliberate unauthorized disclosure of data by internal users within the organization. Motivations for such disclosures are

varied including corporate espionage or surveillance, financial rewards, or grievances with their employers. The latter reason appears to be the most common and the most probable. The methods by which insiders leak data could be one or many, including mediums such as remote access, instant messaging, emails or webmails leading to serious breach of privacy.

Some key respondents noted that information disclosure, sometimes, is due to the amount of personal content that the Internet users keep on uploading on the social sites. Respondent 03LS indicated that, for users to access some applications and services on the IP, they are requested to provide specific details of personal nature. Respondent 03LS noted that a user may be given a pop-up message with *allow* or *deny* options. Some other applications request permissions to access the users' private data. In the cases where one needs to use the application or services, the individual finds it inevitable not to give out their details. The respondent explained that:

> When you are using social media platforms, the requirement is that you register so that you can be able to use the platform. I think the intrusion comes in when these social media applications require that they need to have access to your locational data, access to your contact information, access to your message, access to your transactional information…a major search engine will request access to your information. In most instances, you will find that, if you do not choose the allow option, chances are that you will not be allowed to use that service or application.

Respondent 03LS continued to explain that, in case a user chooses the allow option and proceeds to search for an item, later on, the user receives related advertisements. The respondent noted that:

> If you allow access to your locational or transactional data, chances are, in three to four hours down the line…when you are browsing, you will notice several advertisements that are coming back to you in form of pop messages recommending this, recommending this…so, I think that intrudes. I think that will be considered as an intrusion to privacy because, in as much as it is recommending, there is the risk of free will…the option of choice is lost.

The findings are in agreement with Moran and Weinroth (2008) who found out that the Internet has enabled online marketing institutions to collect data without the immediate knowledge or consent of their consumers. The same study also indicated that marketers gather new types of information to target customers and profiles concerning individual online buyers. This concept of data mining is also advanced by James Moor (2004).

Respondent 05MT also concurred with 03LS that the information requested from users when registering for online services is of personal nature. The respondent 05MT commented that such kind of information may lead to privacy infringements. The respondent indicated that:

> Sometimes you are doing registration, and the information that is being collected from you is of personal nature. You are being asked for your ID number, where do you live? next of kin…this information can later be used against you.

As the findings from the FGDs indicated, most the participants were registered in various social accounts such as Facebook, Instagram, Telegram or Twitter. The social platforms required the users to volunteer personal details in order to use the services. This illustrates that more and more information is being divulged. The idea is supported by Tene *et al*. (2012) who assert that the tasks of ensuring data security and protecting privacy become harder, as information is multiplied and shared ever more widely around the world. Information regarding individuals' health, location, electricity use, and online activity is

exposed to scrutiny, raising concerns about profiling, discrimination, exclusion, and loss of control. Williams *et al*. (2011) observe that organizations similarly must defend against data exfiltration (of high impact) and therefore might be less willing to store customer data. Likewise, one of the findings of the study by Grinch (2015) indicates that:

> There are ethical and philosophical dilemmas arising from constant online data mining and harvesting of information and despite the existence of large numbers of programs with huge capacity to collect personal data, in the media convergent platforms, not everyone is aware of them.

The Privacy Technical Assistance Center also declares that at times, due to a lack of resources or qualified Information Technology (IT) staff, organizations' communication systems might be connected to the Internet directly, or is connected using out-of-the-box network appliances with default configurations attached, with no additional layer of protection. Respondent 07PS suggested that organizations need to train their staff on the current data handling and protection skills as complex ICT products are being deployed to users without training. Such training would contribute to minimizing the risks of unforeseen leaks of private data.

5.2.3 Susceptibility of Social Sites to Cyber Attacks

Respondent 01CS indicated that there is a considerable level of susceptibility of Internet users to cyber-attacks. The respondent noted that Internet users have been victims of malicious attacks on social platforms. The respondent identified, in particular, malware attacks as one of the issues that lead to compromise of personal privacy. Respondent 01CS, for instance, noted that Internet users should be discouraged from logging into strange web links:

> Internet users who receive spam mails must have had their email addresses disclosed or accessed by third parties. Spammers mostly request Internet users to open web links

> and register for services purportedly offered by the web service owners. The users who are successfully influenced into opening the links may have harmful software or viruses introduced into their systems or devices.

03LS noted that anything one puts on the Internet can be stolen:

> Anything you put online can be stolen…do not say 'Remember password'. Always log out of the devices. If you are dealing with something sensitive…if you are dealing with financial matters, your health…anything that you think should be confidential, that you wouldn't want to find going into the public domain.

Respondent 08CT stated that in case of successful attacks, the affected user may be unable to access their social accounts. The respondent attributed the loss of personal data to the susceptibility of social accounts to certain malware. The respondent explained that:

> Internet users ought to hesitate clicking on pop-up messages or logging into unfamiliar web links. This is because, in most cases, the web links prompt the victims to enter sensitive data while working online leading them to disclose confidential information. This information may be used to attack their social accounts.

The findings agree with Adams (2012) who asserts that it is important to note that, while some applications use permissions for the benefit of the users and do not intend to put their users' privacy in danger, some applications use permissions with unethical intentions and hence; distinguishing which application has good intent and the one that does not is up to the user. Internet users need to understand that downloading applications is a way taking a risk and putting personal privacy in the hands of other persons, including the developers of such applications.

5.2.4 Proliferation of Fake News

Some of the respondents concurred that publication of false or inaccurate news stories are prevalent on social sites across the Internet. According to Zimdars and McLeod (2020):

> Fake news is purposefully crafted, sensational, emotionally charged, misleading or totally fabricated information that mimics the form of mainstream news.

False news contains content that may lead to misinformation or disinformation. Respondent 04MM noted that fake news may inaccurate information concerning personal information. However, the respondent indicated that MCK is committed to addressing the issue of misinformation that arises from fake news. The respondent further noted that the Media Analyst and Monitoring department continually monitors the media including the content transmitted through electronic platforms. Respondent 05MT concurred with 04MM that the Council has constantly faced incidences related to false and unverified news on social sites. In the FGDs, one participant noted that people keep posting information they are not sure about. This would mean that there are times when people publish unverified information. Respondent 05MT explained that controlling the production of fake news is, sometimes, being challenged by Internet anonymity. The other challenge mentioned by the respondent is the fact that it has become cheap and easy for online players to create Internet sites:

> We actually have a desk that deals exclusively with fake news…fake news is a menace. Sometimes we don't know the sources…because of anonymity… Maybe the issues of cost and how easy it is to set up an Internet recourse or a website, is also a contributor.

The findings are in agreement with the assertion by Safieddine and Ibrahim (2020) that:

> Although fake news is not an online problem only, there is no previous time in human history that these tools were at the disposal of fake news generators.

From the prevalent issues isolated by the key respondents, Internet users are susceptible to privacy infringements. The findings are also supported by the research conducted by Pathak (2016) which found out that the paradigm shift in this digital age brings new ethical problems which are mainly related to issues of media laws such as the right of privacy which is threatened by the emphasis on the free flow of information. The literature reviewed in the study revealed a shift in communication paradigm arising from the convergence of media platforms. Henry Jenkins (2006), in the theory of media convergence, brings out the concept of communication shift where new digital technologies have been adopted in communication. James Moor (2006) in the theory of privacy, explains the aspect of privacy invasion in relation to sharing personal data across and between digital databases its potential to intrude on the privacy of others.

Table 5.3: Prevalent Privacy Issues Related to Internet Usage

Prevalent Issues	**Activities**
Harvesting of personal data	Data breach Identity theft Impersonation Cyber-bullying
Disclosure of confidential information	Disclosure of personal data, names, ID numbers, place of residence, locational data, transactional data, next of kin.
Susceptibility of social sites	Malware attacks Cyber-attacks

Fake news	Inaccurate content Misinformation Disinformation

5.3 Factors Escalating Infringement of Privacy

The key respondents highlighted some factors that aggravate violation of personal privacy on the IP. The respondents identified factors that included Internet tracking, online anonymity and unregulated user-generated productions such as uncontrolled blogging activities.

5.3.1 Tracking of Users on the Internet

The key respondents observed that user-ready Internet tools are emerging every day. Respondents indicated that there are Applications and software that may be used to monitor the activities of other online users. The tools have capabilities of tracking user online activities. Some of the tools mentioned included spyware, keylogging devices and cookies.

For instance, respondent 05MT noted that users can monitor or follow the Internet activities of other users. The respondent commented that personal data can also be stolen by cybercriminals. For instance, cybercriminals can use malware and hack information:

> …criminals spy everything that you do…they can also install spyware on your machine where the spies can monitor you. We have Keyloggers, Keyloggers collect every information...they can collect all the keystrokes.

Respondent 05MT also identified sim swap as a crime committed from private data accessed when users are trailed on the social sites:

> There are people who go online purposely to collect information. It doesn't have to take a day; they can even spend a month just collecting information about you. Once

> they have gathered enough information about you, they simply make a call to service provider. They tell them, 'I have lost my line'. They will be asked several questions… what is your name, what is your…so they give that information. They look so, so authentic, and after that you know what happens.

Respondent 08CT, for instance, noted that cookies carry personally identifying records from online shopping sites. The respondent stated that cookies can be used to track the shopping habits of online customers because when logging in for online shopping and making payments for goods or services, customers' details can be disclosed. As noted earlier by 03LS, such data may be used for marketing. In FGDs, online shopping was associated with disclosure of private information that risks personal privacy. The participants indicated that people volunteer details such as names, contact, location and place of residence. The observations are in agreement with the study by Moran and Weinroth (2008) conducted on ethics related to online invasion of privacy of customers by Internet marketing agencies. The survey indicated that tracking of online shopping habits most often than not leads to unwanted contact of customers by marketers and, perhaps, greatly infringes on the privacy rights of concerned customers. The concerns raised about Privacy matters are basically on whether the marketing agencies provide, to the concerned individuals, notices and choices in their information requests and disclosure statements. Similarly, the results of the research by Zhao *et al.* (2017) found out that telephone numbers have become the most common way of getting personal information and details of clients.

5.3.2 Online Anonymity

Respondents observed that some content creators conceal their real identities while working on Internet social sites. As the study by Kuss *et al.* (2013) found out, individuals disclose private information more readily due to the anonymity of the medium. Respondent 01CS explained that the Internet supports anonymity where a user may register a pseudo to conceal the real identity. Anonymous Internet users may therefore publish any content because identifying them is difficult. The respondent noted that:

> Internet anonymity undermines responsibility and accountability in online communication because anybody can publish invasive or fake content.

On the same issue of online anonymity, respondent 05MT asserted that:

> …there are so many people who exist in anonymous identity. Even the cybercriminals we have talked about, most of them are faceless. So, they go online, create something…it looks so, so original, something credible, and because there is no face behind it, what you trust is the content in there. That's how you end up giving out information.

From the findings, therefore, anonymity is a challenge in privacy protection. As Singleton (2013) notes, cybercriminals are rarely close in physical contact with or in geographic proximity to their targets. Nonetheless, their distance and anonymity do not diminish either the incidents of their crimes or the damage they can inflict. Quite to the contrary, it is their very remoteness that aids the commission of the crimes that are equal or greater in magnitude than traditional crimes. The anonymity of cyberspace and their remoteness hide their behavior and crimes from their victims and law enforcers, hence, finding and extraditing them becomes difficult. Previous research established that even ordinary Internet users operate under anonymous identities for different motives including the fear of being intruded. For instance, findings of a survey by the Social Research Centre of Australia (2011) indicate that many Internet users were wary about privacy intrusion and hence did not disclose their names in the social networks. Most of the participants in the survey observed that users remain incognito or use pseudonyms to sign in when working online.

Anonymity and pretense are regarded as unacceptable. Journalists are expected to positively identify themselves to their sources and audiences. For instance, the Code of

Conduct for the Practice of Journalism in Kenya (2013) requires reporters to identify themselves to their sources when conducting information gathering.

5.3.3 Proliferation of Unregulated Social Sites.

Some of the key respondents noted that there is great autonomy in online communication that allows Internet users to generate huge content on social sites. Jenkins (2006), in his description of media convergence, argues that authorship of online content is no longer done by specific persons such as media correspondents or journalists. Many Internet audiences have now become producers of online media content.

Respondent 07PS also commented that unregulated content creators are widespread. The autonomy makes it challenging to hold the creators responsible for publications. The respondent noted that some online players disguise their identity hence; it is difficult to identify them. The respondent stated that such content creators:

> … can be anywhere in the world…the same…know how to hide. They have different ways of hiding…even if they have a name, they mutate, so you can't get them.

As mentioned earlier by respondent 05MT, it has become easy and fast to set up an online resource. The respondent stated, because of the tools at their disposal, users find it easy and convenient to put up social sites. According to the respondent, a content creator does not need any approval to create an online site. The respondent explained:

> As we talked about the characteristics of the Internet, remember the Internet is not governed per se. If today, you as Nancy (*the researcher's name*), want to start a website, you will not need to pick a phone and call anyone, right now, you will create your domain registration using your phone…everything (*emphasizes*) including payment. Within three minutes, it will be up. There is, really, no one who

> polices...therefore, it creates a very good avenue for people to infringe on other people's privacy to do so without regulation or restrictions.

This fact demonstrates the autonomy that exists on the IP. Therefore, in the new media convergence environment, anyone can create content on the Internet without restrictions. The surge of uncontrolled social sites was identified as one of the contributors to publication of inaccurate content. Some of the sites were linked to the proliferation of fake news. The respondent 05MT noted that even when the sites are brought down, new ones are created:

> We flag them down…tomorrow they start another one.

Respondent 04MM observed that MCK accredits journalists who are trained in the media field. The respondent indicated that some of the people who are creating content are not necessarily trained journalists. Respondent 06AC also noted that only trained journalists are accredited by MCK. The respondent explained that:

> We ensure that journalists are registered and that they practice according to the code of conduct…we ensure that all accredited journalists are people who are trained in journalism field.

From the findings, it would follow that, media regulators may not comprehensively control the activities of non-accredited content creators. The Autonomy of the social media platforms was deemed to limit this realization. This aspect also emerged in the FGD discussions where the participants indicated that there is unrestricted production of content including filming, and taking of photos.

The findings are in agreement with Kun *et al.* (2012) who observe that there is a change in media content and media audiences:

> Traditional media audiences have slowly evolved from passive, isolated consumers into information creators and consumers…other amateur journalists are constantly involved in online authoring…However, these untrained news information producers often depend on emotion or sensationalism to judge the validity, credibility and worth of their news contents, resulting in highly variable information quality.

5.4. Factors Limiting Protection of Privacy on the IP

The key respondents highlighted certain factors that challenge the protection of privacy in the current media convergent environment. The factors identified included Internet user vulnerability, surveillance, data storage media and the public interest to receive information.

5.4.1 Internet User Vulnerability

The key respondents expressed concern about the high user vulnerability levels. For instance, respondent 05MT explained that media convergence communication networks are swiftly evolving hence, new applications and IT knowledge is emerging faster than the awareness of Internet users. The developments in information technologies constantly expose Internet users to undesirable intrusion. Respondent 03LS emphasized the need for Internet users to understand the capabilities of the current information technologies. The respondent explained:

> …because nowadays we are seeing the products that are coming into the market… telecommunication devices are coming with pre-installed applications. The control is in your hands, you may have a device that can access the Internet, but if you are well aware of the capabilities of your mobile phone…what you can consent to and what you

> cannot consent to, what you allow the applications to have access to and what you deny them to have access to. The control is basically in your hands.

Respondent 02MS cited inadequate user-awareness as a factor contributing to increased online vulnerability. The respondent emphasized the need to continuously develop skills in data handling and safety. Respondent 01CS also commented that:

> …individual Internet users need to have the knowledge in order to protect themselves from privacy breaches while working online.

The idea was supported by respondent 02MS who commented that Internet users risk disclosing important confidential data. Therefore, there is a need for users to exercise caution. The respondent explained that:

> You need to be cautious about the challenge you are exposing your identity to. There is some information that will be necessary that you only use secure network when you are communicating, for example, free WI-FI is really attractive to many people but, whenever you are using free WI-FI, somebody may be stealing your data. Those public hot spots are dangerous places to use your Internet device because they are not so much protected and hackers are able to scan around, and are able to track and get confidential information.

Respondents 01CS and 03LS cited access permissions that users grant during online communication as openings to user vulnerabilities. The permissions may lead to access to private information. Respondent 01CS, for instance, noted that:

> There are common pop-up prompts such as ‘allow’ or ‘deny’. When users click ‘allow’, they automatically grant access.

According to a study by Grinch (2015), one must not only look at the invasions of privacy but also at the potential areas for invasion. This concurs with Williams *et al.* (2016) who indicate that it is important to devise methods to predict the impact of sensitive data to enable individuals to understand the risk of such exposures. The research by Boyd and Hargittai (2010) found that users with low overall Internet skills are less likely to change their privacy settings on their online accounts such as Facebook and are less confident in doing so. These populations experience negative outcomes from their social sites use due to less optimal use of the available privacy and security settings. This scenario, therefore, poses a challenge limiting the protection of individual privacy in the wake of the convergent media environment. The U.S Technical Assistance Center points out that some organizations lack established security architecture, leaving their network systems vulnerable to exploitation and the loss of personally identifiable information.

5.4.2 Surveillance

Surveillance involves systematic collection and processing of information through electronic hardware or software of applications. Respondent 07PS observed that, although there are justified reasons for surveillance, the devices installed in public and private premises harvest information from members of the public. 01CS agreed with 07PS that surveillance devices may be installed but reasonable caution to be exercised, as personally identifying elements are recorded. Regarding tort law concerning privacy, Volokh (2014) notes that the increasing prevalence of private surveillance may subtly make people more willing to accept government surveillance. If private entities are, for instance, required to maintain surveillance cameras with face recognition software on private property, it will be much harder to argue that police departments should be prohibited from doing the same on government-owned streets. Yet this does not stem from a judgment that such video recording has no effect on tenant or visitor privacy, rather, it stems from a judgment that

the owner's property rights authorize him to do this notwithstanding tenant privacy interests. Thierer (2014) asserts that:

> …there is a valid reason for privacy and security concern as there is potential massive security threats and privacy violations in the world of always sensing devices. There is no way to achieve perfect safety, security or privacy in the 'Internet of Things' era. We cannot have the most open accessible and interactive network of networks that humanity has ever known without also having some serious security and safety issues creeping up. We will always face new challenges and will need to constantly work towards the improvement of data practices.

Surveillance on social media allows people to access private information including contents from varied social contexts. For instance, 01CS and 02MS indicated that the data people upload remains on social platforms. 01CS noted that there are abundant personal data traces left on the Internet social sites when users are not keen to apply data access protection and other security settings. Respondent 02MS explained that:

> Whatever you put on the Internet; you cannot delete. You may try to delete it from your end and it looks like deleted but, that information is somewhere and somebody can bring it up.

Respondent 07PS also commented on the creation of huge data. The respondent indicated that Internet users are uploading and sharing large volumes of personal information on various social platforms, and consequently risking their privacy. According to Gross and Acquisti (2005), potential employers sometimes conduct background searches to investigate candidates. This poses enormous threat to privacy of their employees, as this data is preserved in databases and can easily be retrieved. The assertion is in agreement with the findings of this study. For instance, as indicated earlier in the findings from the

FGDs, the concern about the implication of data uploaded emerged. For example, one participant argued that people may have challenges in getting jobs if employers found out that they had a history of crime. Respondent 02MS commented on the permanence of the information that people divulge on social sites while working online. The respondent observed that someone can trace the activities of other Internet users from their content:

> Internet is *"unforgetful"*, hence, it is possible to track a range of information including identities.

Unauthorized access to information is discouraged in various instruments. For instance, universally, privacy protection has been given considerable attention. In the USA, for example, the Electronic Communication Privacy Act of 1986 prohibits the bugging of any conversation made over cable or terrestrial devices when people are in their privacy. A similar observation was made by Clark and Roberts (2010) who assert that monitoring of employee's or applicant's social sites and profiles is a socially unacceptable practice because it allows the employer, without the knowledge of the employee to, undetectably, voyeur into private information.

5.4.3 Data Storage and Portable Media

Portable devices were associated with privacy violations such as disclosure of sensitive information. Some respondents noted that information disclosure sometimes occurs due to portable device and their usage. Content in portable storage devices may be accessed or copied by unauthorized parties in case of loss.

Respondents 01CS observed that:

> Data storage media are common sources of accidental leakage of confidential information…as you know data leakage is not always deliberate.

The respondent noted that confidential data need to be protected by applying passwords in portable devices to restrict access.

Respondent 05MT elaborated that:

> One of the biggest concerns when it comes to removable devices, is the fact that, it is very easy for information contained in them to land in wrong hands. First of all, there is sharing of these removable media. secondly, they are prone to loss. You could have confidential information lost when using removable media…they are also subject to rapid failure.

The devices were therefore identified as common sources of information leakage especially if they land in the wrong hands. The devices can copy and transfer data of large magnitude. Their loss or access may lead to the risk of disclosure of information. The literature reviewed indicated that data storage devices were potential sources of data leakage. This is consistent with Singleton (2013) who asserts that among the major cybercrimes, is the copying of private data by an unauthorized party. This crime occurs when a cybercriminal gains access to sensitive data and steals it. The crime can be as simple as copying an entity's customer data files onto a flash drive and selling it to a competitor, or using confidential or proprietary information to compete with the entity's business.

Respondent 08CT explained that sometimes faults may occur from time to time, affecting the process of transfer of information leading to unanticipated data disclosure. The respondent also noted that frequently repeated passwords can also be hacked leading to unwanted access or loss of data. A study by Bijone (2016) found that attackers gain unauthorized control of various systems, and can modify or alter system states, read files, etc. Generally, such attacks exploit certain flaws in the software. Attackers as well exploit the vulnerability in operating systems or application software.

5.4.4 The Need to Access Information

Respondent 04MM observed that the need to provide information to the public is the essence of communication. Respondents 07PS and 05MT shared the same view that the

need to provide news affects the speed at which news is transmitted. For instance, 07PS noted that publishers want to be the first to disseminate certain information as they make revenue from news making. Respondent 04MM also concurred that the challenge arises from the need to transmit news as fast as it emerges and the pressure to meet routines.

As indicated in the Report on ICT and Privacy in Europe (2006), the new communication developments are challenging privacy protection:

> In recent years, protection of privacy as a pillar of open societies has been challenged by different developments leading to erosion of some safeguards of privacy.

As 04MM further noted that the right to access information is entrenched in the Bill of Rights of the Constitution of Kenya (2010). Therefore, newsmakers may not be restrained from creating and transmitting information unless there is a prevailing reason that may hinder the reportage of certain kinds of news. The findings from the FGDs indicate that people widely search the Internet when they hear about shocking occurrences, download and later repost to other people. This indicates that large amounts of online data are accessed. However, 04MM stated that MCK analyzes the media contents including the news disseminated across the Internet networks. Similarly, 05MT and 06AC indicated that the practice of journalism in Kenya is regulated by enforcing the professional ethics outlined in the Media Council of Kenya Act (2013). This is an effort that could reduce harm arising from uncontrolled production of information.

The respondent 06AC, for instance, expounded that:

> We enforcing professional practice …the practice is guided by the Media Council of Kenya Act (2013) …we call it our blueprint.

The Media Council of Kenya Act (2013) empowers the Council to carry out the functions of developing and regulating ethical and disciplinary standards for journalists, media

practitioners and media enterprises in the country. One of the elements protected by the Act is the aspect of personal privacy. The Act states that:

> The public's right to know should be weighed against the privacy rights of people in the News…Intrusion and inquiries into an individual's private life without the person's consent are not generally acceptable unless public interest is involved. Public interest should itself be legitimate and not merely prurient or morbid curiosity.

5.5 The Aspects of the Internet Undermining Control of the IP

./c convergent platforms. Some of the aspects identified included searchability of the Internet platforms and Internet penetration and access.

5.5.1 Searchability of Virtual Networks

Virtuality signifies the intangible nature of cyberspace characterized by immediacy, temporal closeness, boundlessness and limitlessness. Tomlinson (2007) refers to the situation as ‘spatial proximity. Searchability of the Internet was associated with unlimited access to information. Respondent 07PS explained that Internet users are consuming and distributing online content in real time. 01CS noted that Internet has come with great convenience for assessing and sharing information. Respondent 05MT observed that:

> Internet search applications and Web browsers are fast and easy-to-use tools in navigating cyberspace to access the desired content. Internet users are constantly on the Web searching for information. This practice enables Internet users to access large amounts of data of any kind and nature, available on the social sites they usually visit.

According to Gilmor (2008), this is only a start as people will pick up many kinds of newer media forms. Internet users can subscribe to others users' sites and links and make comments on pages. Through trackback mechanism, they can as well see when other users link to their pages and can respond with either a reciprocal link or by adding a comment.

Respondent 02MS explained that the Internet is an open virtual resource that is accessible to any user that has a device connected to the platform. The respondent noted that users need to consider that the information shared on the Internet may be accessed and therefore, should be cautious when posting. The respondent explained that:

> The nature of the Internet is open…Internet was created for data exchange. By design, the Internet was created to be a sharing platform whereby different servers can talk to each other. You need to be careful. Whatever you put on the Internet, somebody can access it in one way or another. This knowledge is important. If people are aware, they will be a little bit careful when posting.

As indicated in the findings from FGDs, the participants were connected to the Internet platforms conducting various communication activities on the sites (Table 4.2). This means that the participants were involved in constant online communication. The findings are supported by Cowles (2009) who observes that the media convergent environment is a virtual world, with the capability to contain infinite spaces accessible by virtual locators. Even in the language, we use to describe the Internet experience, we talk about having *'visited'* the websites. This is evidence that we do not consider the Internet plateau as simply a communications medium. The ability to experience and change the virtual world makes the Internet potentially different from previous technologies. Privacy concern around sharing information in a public cyberspace is amplified by converging structural characteristics of the new media landscape. This may obfuscate the true audiences of these disclosures due to their technical properties e.g., persistence, searchability and dynamics

of use; including invisible audiences **(**Boyd, 2008b). This implies that privacy protection is at stake if regulations are not efficiently reviewed and enforced.

5.5.2 Internet Penetration and Access

The rate of Internet penetration and access may be revealed by the Internet data subscription trends. Respondent 03LS indicated that Kenya's Internet absorption rate was, then, the highest in the region.

Based on the First Quarter Sector Statistics Report for the Financial Year 2020/2021 (July - September 2020) by CA, Internet/data subscription was marked by a remarkable rise:

> As at the end of the first quarter of 2020/21 financial year, the Internet/data market experienced positive growth…The total data/Internet subscriptions rose by 4.8 percent to 43.5 million, from 41.5 million subscriptions reported last quarter with mobile data subscriptions accounting for 98.5 per cent of the total subscriptions.

As Gilmor (2008) asserts, there is a free and uncontrolled flow of information in the virtual space as media use is becoming democratized.

Respondent 05MT argued that, with the high rate of Internet access, there is the possibility of uncontrolled activities on the social platforms. The respondent indicated there is a need to create more capacity as Internet consumption rises.

> With the high level of Internet penetration, there is need for some sort of control... the explosion and the rate at which the Internet usage is growing, maybe, we need more capacity to be able to deal with that.

The finding is replicated by the findings from the FGDs which indicate that all the students were connected to the internet. The participants used the phones to conduct various functions in the summary Table 4.2. As 02MS expounded, the new Internet paradigm has

altered communication and consequently affected the checks and controls that previously ensured protection of personal privacy during the times of analogue communication. The respondent explained that:

> We normally talk about the Internet cloud…when you are connected to the Internet, you will be connected with servers that are in different places in the world. So, it is not a physical connection…unlike previous voice communication during the times of analogue communication, whenever transmitting voice communication, we had checks and controls on it which kept the privacy of that communication. But now, when using Internet communication that is basically on IP, that aspect of privacy is not catered for on the Internet platform.

The respondent further pointed out that, fundamentally, the new developments in communication have increased data creation, circulation, and consumption of a range of social media products. The findings are consistent with the study by Kammer (2013) which indicate that media convergence has altered the nature of the media consumers from passive audiences to vibrant participants in information creation and distribution. Kun *et al.* (2012) also note that the expansion of new channels of communications has important implications for the dissemination of knowledge and ideas in a society. According to the survey by Mendel *et al.* (2012), the abilities of the new communication environment have posed privacy challenges as it enables the users to possess tools for collection and location of new types of personal data which in the past would have been impossible or unfeasible. Computers, mobile phones or other devices are attached to the Internet have unique IP addresses, which provide unique identifiers for every device and which means that they can be traced. The ability to locate any device creates significant new privacy challenges.

As observed by respondent 08CT, Kenya has witnessed substantial growth in Internet access and usage as demonstrated by the rising number of Internet Service Providers and

Internet users. This has posed a great concern that may call for legislative attention. The respondent noted that ICTA has therefore intensified minoring of standards and conformity of government ICT programmes. Similarly, respondent 05MT commented that media convergence has supported the growth of new media creators that never existed before. The respondent commented that media convergence has supported new media players that never existed before. The mainstream media companies have tried to expand and are now embracing online productions and interactions with audiences. The respondent also indicated that, since there is an undeniable drift from traditional communication processes to new online methods, MCK is constantly monitoring the new trends.

Findings from the key respondents show that Internet users have been actively involved in production and sharing of data on social sites, therefore, risking their privacy and that of others. The study findings are supported by Henry Jenkin (2006) who, in the theory of media convergence, proposes that the new media environment has increased the creation of unlimited data. The theorist states that media convergence embraces three Cs that include Computing, Communication and Content. The convergence of media has created an environment that supports proliferation of production of huge amounts of data on social platforms. This also in agreement with James Moor who proposes that privacy is threatened because interactivity and data transmission techniques are used to transfer and share personal data across and between digital databases. As preconceived in the conceptual framework of this study, the Internet user-generated productions have a role in escalating intrusion of privacy of users on the convergent platforms.

Table 5.4: Control and Regulation of Online Platforms

Factors escalating intrusion	User-trailing applications and tools
	Online anonymity
	Proliferation of unregulated social sites

Factors limiting control of the convergent platforms	Internet user vulnerability Surveillance Portable/ removable storage media Public interest to access news
Aspects of the Internet undermining regulation of online communication	Searchability of the Internet platforms Internet penetration and access

5. 6 Mitigation: Guarding Against Online Privacy Infringement

This section presents the analysis of the data from key experts on strategies for guarding against intrusion of online privacy. The key respondents provided fundamental insights on the strategies of addressing privacy violations on the media convergent platforms. The strategies highlighted included legislation, self-regulation, enforcement of compliance and conformity to regulation and policy, media monitoring and analysis, accreditation and registration, information access restriction and security settings, and user skills and education.

5.6.1 Legislation and Policy Making

Legislation and policy-making are critical processes in regulating and setting standards of any practice. During the interviews, almost all the key respondents consistently agreed that protection of online privacy has faced a considerable challenge in the face of the rapidly changing media convergent landscape. However, the respondents highlighted some of the developments made through legislation and policy-making.

For instance, concerning cyber regulation, respondents 01CS and 03LS identified some of the Bills that had been formulated. Both respondents indicated that the Computer Misuse and Cybercrimes Bill (2018) had been drafted and passed. The Bill focused strongly on cybercrimes and the protection of online privacy. However, 03LS noted that soon after,

there was a petition that led to suspension of some sections of the Act. The parties that petitioned the Bill cited inconsistency of some sections of the Bill in respect to various fundamental freedoms such as media freedom. Similarly, 07PS noted that the Information Communication Technology Practitioners Bill was formulated in 2016. Although it was not implemented, the Bill was intended to enforce registration of ICT practitioners. The Information and Communications Technology-ICT Policy was formulated in 2006, reviewed in 2016, and later, in 2020. The policy was reviewed to embrace the emerging changes in information communication technologies.

Respondent 03LS commented on the formulation of the Data Protection Bill (2018). The respondent noted that the Bill is a major step towards the protection of personal data. The Data Protection Bill proposes crucial regulatory guidelines relating to protection of private data. For instance, the Bill spells out the grounds for processing private data including obtaining consent from subjects whose data is processed, sharing of sensitive personal data, retention, data erasure and destruction, and the penalties for infringements defined under the Act.

Respondent 03LS commented about the then ongoing debate concerning the operations of Over-The-Top Technologies and Services (OTTs). According to Kenyan National ICT Policy (2016), OTT applications operate by using public Networks. OTTs services and products are usually streamed directly to audiences and customers. The services include video services, music, advertisements, money transfer or mobile banking services. Audiences access OTT media services through PCs, smartphones or smart TV applications over other Networks. The OTTs are considered to benefit by making revenue, although they are not being subjected to regulations as compared to other regulated services.

However, respondent 07PS commented that the establishment of the regulatory environment of Internet services is still in its initial stages. The respondent pointed out that there is a need to explore greater possibilities of continuous amendments of the current communication policies due to the rapid changes experienced on the IP platforms. Respondent 03LS also noted that the Internet is still not fully understood. The respondent

further indicated that an early regulation might adversely affect the innovation aspect of ICT. The respondent elaborated that:

> People will still argue that we are still understanding the Internet and how it works…it is interesting because the Internet has been around for quite some time but, it is still new, we are still learning. People say, what we see is just the tip of the iceberg. The main argument you get, from the proponents out there, is that if you seek to regulate technology quite early…you might end up stifling it. We don't want to stifle the innovation aspect. It's more of trying to balance.

The innovation aspect of technology is also underscored by the National Information and Communications Technology (ICT) Policy of Kenya (2006). This Policy emphasizes ensuring that relevant education and training programmes are initiated towards helping people to maximize the opportunities afforded by ICT technologies in improving the quality of their lives and in enhancing their work prospects. This is important in stimulating investments and innovations in ICT, and achieving universal access based on internationally accepted standards and best practices. The ICT policy (2006), as noted earlier, has undergone review in 2016 and later in 2020, to embrace the emerging changes in the ICT field.

The Media Council of Kenya also advocates for privacy protection. Respondents 04MM and 06AC also indicated that the Media Council of Kenya Act (2013) provides for the protection of privacy rights.

As stated in the Act, the Media Council of Kenya should ensure that:

> The freedom and independence of media is exercised in a manner that respects the rights and reputations of others. …Things concerning a person's home, family, religion, tribe,

> health, sexuality, personal life and private affairs are covered by the concept of privacy except where these impinge upon the public.

The right to privacy is also provided for in the Bill of rights of the National constitution of Kenya (2010). The constitution provides that every person has the right to privacy, which includes the right not to have the privacy of their communication infringed. On the other hand, the same Bill of rights protects other fundamental freedoms such as media freedom, freedom of expression and the right to access information.

From the foregoing, there has been considerable focus on media regulation and policymaking. However, the process seems to be faced with the need to balance amongst several factors ranging from the need to regulate online communication, promoting the interests of ICT innovation, to the need to safeguard various fundamental freedoms such as media freedom, freedom of expression and the right to access information. For instance, the implementation of the Computer Misuse and Cybersecurity Bill (2018), which was anticipated to be a major milestone towards the control of Cybercrimes and Internet privacy protection, is yet to be determined. The Bill focused on protecting a range of Internet-related infringements such as unauthorized access of information, child pornography, cyber-stalking, computer fraud and cyberbullying. As Li (2011) asserts, there is a need to accelerate the formulation of laws and regulations on the protection of the privacy of citizens and make the violation of privacy clear.

5.6.2 Enforcement of Compliance to Regulation and Policy

The key respondents upheld compliance and conformity to communication standards and policies in safeguarding the privacy of communication from Internet infringements. The respondents highlighted various strategies including self-regulation, media monitoring and analysis, accreditation and registration, training, licensing, inspection, complaints handling and computer incident response.

5.6.2.1 Self-regulation

One of the approaches that may promote compliance and conformity is self-regulation. In media practice, self-regulation of practitioners is regarded as ordinarily admissible for observation of communication standards. As Haraszti (2008) asserts:

> Media self-regulation is a joint endeavour by media professionals to set up voluntary editorial guidelines and abide by them in a learning process open to the public. By doing so, the independent media accept their share of responsibility for the quality of public discourse in the nation, while fully preserving their editorial autonomy in shaping it.

Although self-regulation is upheld in encouraging conformity in media practice, some respondents indicate that the process may not comprehensively realize the protection against the privacy vulnerabilities occasioned by Internet usage in the prevailing media convergent ecosystem. Respondent 04MM indicated that self-regulation has been applied in the industry amid challenges. The respondent noted that although self-regulation is advised for regulating practice in the industry, it has not fully addressed privacy violations on the Internet platforms because there are non-journalists, who are involved in creating content on the Internet social sites. The respondent noted that online content creators need to understand the consequences of breach of ethics. The respondent emphasized that Internet users and communication practitioners need to understand when their online practices conflict with communication quality and standards, and how it amounts to legal offense. The respondent felt that enforcement should be applied. The same idea was supported by respondent 07PS who noted that self-regulation may not always work as expected. The respondent asserted that, for the sake of compliance, enforcement is important. The respondent stated that if people are aware of the consequences, the knowledge can also be deterrent. The respondent stated that:

> Self-regulation is very hard, because if you want to regulate somebody… there must be a penalty. So that they can fear… the fear of what if? (*laughing*) that fear of what if, …will compel them to comply.

Follow-up question: so, do you mean we need a law?

07PS: Yes, we need a law… we need a law for them to comply.

The above responses indicate that self-regulation alone may not be adequate to ensure complete adherence to best practices in cyberspaces. It was noted that there is the presence of other non-journalist players creating content on the social platforms who may not adhere to self-regulation. This assertion is consistent with the findings of the survey by Zhao et al. (2017) that, more legislation is needed for better control of Internet space.

5.6.2.2 Media Monitoring and Analysis

Some of the key respondents indicated that routine monitoring of media activities is key in keeping track of cyber activities on Internet platforms. As Singleton (2013) observes, it is important to initiate monitoring systems, technologies and access, such as logs created by technologies leading detection strategy

Respondent 04MM observed that monitoring and analysis of media activities help in identifying incidents of infringements on the convergent networks. Both 04MM and 05MT indicated that MCK conducts routine monitoring and analysis of media activities including electronic media platforms. 05MT explained that MCK has a weekly magazine that monitors media activities:

> One of the milestones…is the launch of a weekly magazine known as the "*The Media Observer*". This is a tool used by the Council for monitoring and analyzing media communications. Through this document, we do weekly

> analyses of unverified or fake news content. It is also used to inform audiences what News is fake.

However, the respondent also noted that there are some setbacks in controlling communication activities on the Internet platform. One of the reasons is the open nature of the IP. The respondent indicated that:

> …considering it (*The Internet Protocol)* is an open area, the amount of policing on the Internet is not what you would expect compared with other physical spaces.

From the response above, the open nature of the IP has permit free flow of information hence, challenging the control the online communication. This finding is consistent with Kuss (2013), who asserts that:

> …there is great autonomy in online publishing where users are actively posting huge data instantaneously.

Respondent 02MS indicated that, sometimes, there are enforcement constrictions in terms of jurisdiction. The respondent noted that the content regarded to cause infringement is often limited to the country that considers it privacy invasion. For instance, the respondent explained:

> What I mean is this…what might be illegal in Kenya might be very legal in another country…In Kenya we might be having laws that say it is not right but other countries may not see anything wrong with that. So, what we consider private here, may not be private in another country. So, that poses the challenge of enforcement. If you want another country to enforce in terms of what you consider that privacy has been infringed, that country might say, 'we don't see any problem here'

On the issue of protection of copyright, 02MS observed that:

> The issue of copyright is there...but the issues of copyrights are limited to jurisdiction. So, if somebody hacks into my information in *country x (Country's name withheld)*, the laws of Kenya cannot be able to arrest that person…because you cannot come up with laws and expect another government to implement.

From the responses, media monitoring and analysis were upheld by many respondents. However, it was apparent that enforcement of privacy protection on the IP is practical only within certain jurisdiction limits. The fact that the IP is a virtual spectrum, has challenged the realization of enforcement because infringements may be committed anywhere in the globe. As the survey by Mendel *et al*. (2012) established, there are new challenges for regulation given the transnational nature of the Internet:

> Despite the emergence of international best practice standards for data protection, there is still much progress to be made towards the harmonization of national laws as online companies still find it hard to navigate the complex patchwork.

The findings are corroborated by a study by Williams *et al.* (2011)who argue that the importance of cyber-resilience emphasizes the ubiquitous personal risk from data breaches; organizations would invest in costly technological protection, but still, fall victim to high-impact advanced persistent threats.

5.6.2.3 Accreditation and Registration Policy

Accreditation involves certification of an establishment, an entity or an individual who meets the requirements or the set standards in a particular field. Some respondents indicated that, as a matter of policy, individuals or enterprises are affiliated through registration or accreditation. For instance, respondent 06AC noted that the MCK accredits

practitioners in the media field as provided by The Media Council of Kenya Act (2013). The respondent noted that accreditation is meant to encourage ethical practice in the field:

> Accreditation of media practitioners by the Council focuses on encouraging adherence to media professional values and observation of communication standards. For this reason, the Council has set guidelines for accreditation.

The MCK has specific accreditation categories that include media enterprises, local journalists, foreign journalists, journalists in freelance practice, students of mass communication training, media trainers, advertising firms and public relations practitioners. 07PS noted that through ICTA, the government strives to enhance standards and conformity through accreditation of ICT suppliers for the government.

07PS also noted that ICT practitioners are being registered:

> We have created standards for ICT practitioners and ICT suppliers. We are now registering them. We have categorized them into different categories. The intention of ICTA is to ensure that we bring everybody on board… we have incorporated all the ICT professionals in the field…. like…ICT technicians, ICT graduates, ICT practitioner…depending on where they fall, they are registered by ICTA… to make sure we bring ethics and values…in terms of usage of information technology because everybody uses this technology.

The above findings demonstrated progress in the application of policies relating to accreditation of media players and registration of ICT practitioners. Considering that ICT technologies and cellular devices are normally connected to Internet networks, accreditation and registration of respective players is a key step towards promoting best practices that would minimize online infringements. In the FGDs, findings indicated that

the participants were avid consumers of Internet services and ICT products. It becomes important also to determine how the consumers interact with these products.

5.6.2.4 Incidents Response and Complaints Handling

Respondents 01CS, 02MS and 05MT mentioned that the government has a response team known as Kenya Computer Incidents Response Team (KE-CIRT). 01CS observed that KE-CIRT coordinates responses to cyber violations once detected or reported. Respondent 02MS suggested that Computer Incidents Response teams would work better if governments collaborate internationally:

> If they collaborate, it will make it easier…Kenya has KE-CIRT…different countries have formed their CIRTs (*Computer Incidents Response Teams*). so, when there are international collaborations, they can talk with different Response Teams and…can help address some of the issues raised such as cybercrimes, hacking…

01CS also stated that the Directorate of Criminal Investigation (DCI) and the National Intelligence Service (NIS) are involved in investigations of infringements. The respondent was in agreement with 07CT who explained that ICTA has highly skilled experts, but the police are involved in criminal investigations, where the need arises:

> ICTA is highly skilled in terms of expertise. But sometimes we team up… we team up for forensic investigations with the police…if the case is criminal in nature and is spreading across. So…we team up.

On complaints handling, respondents 02MS and 03LS commented that the Department of Licensing, Compliance and Standards at CA issues licenses and also monitors compliance by the licensees. Respondent 01CS and 03LS further explained that the Authority has consumer and public affairs services that protect customers against breaches committed by

licensed service providers. Respondent 03LS also observed that complaint handling minimizes the effect of infringements. Similarly, respondents 04MM, 05MT and 06AC mentioned that MCK offers a platform for individuals or organizations to make complaints to the Complaints Commission of the Council. Respondent 04MM commented that the Complaints Commission is charged with the roles of receiving complaints and arbitration of disputes presented to the Council.

5.6.3 Access Restriction

Respondents recommended the use of security settings in preventing unauthorized access to private information. Respondents encouraged restriction of access to personal data through various methods. Some of the methods identified included biometrics identification, encryption and password settings. In this study, some respondents indicated that biometric identification methods are essential in establishing authenticity and preventing unauthorized access to sensitive information.

5.6.3.1 Biometric Identification

Some respondents felt that biometrics are more secure in preventing unauthorized access than using passwords alone. For instance, respondent 01CS noted that institutions have adopted biometric software, majorly, as a complementary means of identity recognitions. The respondent mentioned fingerprint, facial and voice identification as the most common biometric identification methods. About voice recognition, respondent 01CS indicated that some mobile network service providers have adopted voice identification in mobile phone communication. The respondent observed that:

> Biometric technology is being adopted to complement passwords and pin codes. Sometimes even passwords considered strong can be lost, forgotten or stolen.

However, 01CA also argued that the use of biometrics could be another means of data harvesting. The respondent stated that privacy concerns may arise from the fact that it is

not clear how the biometric data is stored or who can access it. The respondent further stated that biometric information is personally identifiable data and may be used for malicious purposes.

On the same issue, 07SP stated that the use of biometrics adds strength to passwords:

> The strength of a password can combine both the biometrics and the password… that one can be a very strong password.

The respondent also argued that it is not a good idea to totally replace passwords with biometrics:

> If we fully replace the password with biometrics…there will be a challenge because of physical change, even age…biometrics may be affected by physical change (*laughing*)…and you are not identified. The best is to combine the two.

This is in agreement with the study by Galterio *et al.* (2018) who explain that biometrics play an avid role in today's mobile security realm. Organizations consider that:

> By using biometrics, their system would be strongly secured…the most relevant, popular, and realistic use case is security. Buildings, border checkpoints, airports, and seaports all require authentication for access. ATM machines, banking applications, computer and network security, and email logins are some examples where authentication is also absolutely necessary for access…Governments have put in a significant amount of resources in order to develop facial biometrics and have begun to implement them for day-to-day use. Biometrics have had a positive impact on border crossing at airports,

> identifying fugitives and criminals, and with the right development, can also be implemented in banks, shops, and many other offices.

In the research conducted on biometric identifiers, Babich (2012) elaborates that biometrics technology has its own functionalities that include universality, uniqueness, permanence, measurability, collectability, performance and acceptability.

5.6.3.2 Security Settings

Respondent 01CS, for instance, explained that communication devices come with various default tools and applications that users may apply in preventing unauthorized access to private information. The tools enable users to control can view their activities by applying restriction settings as desired. The idea was supported by respondent 02MS who indicated that encryption enables users to substantially control access to personal information. The respondent stated that:

> Encryption mechanism can also be used to secure communication. There are simple encryption keys one can use to secure communication so that it can be difficult for someone to hack into private communication.

It was observed that access protection can be compromised when Internet users grant access permissions to unknown applications or users. For instance, respondent 05MT indicated that Internet users should not, as a general rule, divulge personal details or to strange callers purporting to be working for certain banks, companies or service providers; especially if they are requesting for a password reset. The respondent noted that divulging confidential information may result in cyber-attacks. 05MT further stated that if a user finds a link requesting access permissions, one should think first before opening the link:

> There is a rule that says: *stop, think and click*. If you find a link, you should stop and think first and, when you are sure it is safe, you click.

As noted by 05MT, data theft can be avoided if Internet users fortify and strengthen the password by creating unique pin codes. The respondent noted that there are very basic settings but their absence may cost a user data loss or disclosure. 05MT agreed with 08CT that usage of similar passwords for different social accounts owned by the same individual should be avoided. According to the survey by Bijone (2016), attackers start with access to a normal users' account on the system by sniffing passwords and can exploit certain vulnerabilities to gain and access important personal data.

The research study by Devi and Roy indicates that privacy security settings would limit other users from accessing or viewing social network profiles of other users. Adams (2012) further observe that privacy since settings may vary depending on the platforms, Internet users should read and understand the settings and should not approve of any settings that expose their private information to the public. If the users find a setting that makes all of their content available to the public or that shares personal information with Internet actors such as advertisers, users should be apprehensive or consider the consequences emerging from exposure of private content.

5.6.4 Data Minimization

Some respondents recommended data minimization as a way of protecting online privacy. As respondent 02MS previously noted, the Internet does not '*forget'.* Even after the deletion of any data, the information that was created previously will always be available on the IP and can be accessed in one way or another.

On the same note, respondent 07PS emphasized that people should refrain from sharing confidential information if they wish to maintain privacy. The respondent explained that once confidential information is shared, the owner may no longer have control over it:

> I normally tell people; the only safe data is the one you have…and is with you alone. The moment it leaves you…(*laughs*), you cannot control…and whatever is confidential is no longer confidential. It is everywhere in the public domain.

Respondent 05MT recommended that users should avoid giving away information by responding to random pop-up messages on social sites. As noted earlier, the respondent explained that opening such links can be hazardous, especially, when a user decides to follow instructions, grant permissions and act as prompted. The findings are in agreement with Adams (2012) who argues, some of these permissions could be used without malicious intent, but Internet users should approach the requests with caution. Respondent 05MT continued to elaborate that:

> Internet users should not trust strange web links but instead should decline when they experience such advances. One should also be wary of suspicious and anonymous callers especially if the callers are soliciting for sensitive personal data.

Respondents 01CS and 08CT indicated that taking caution in online privacy matters has become necessary as many people have turned to Internet usage almost on daily basis. 01CS for instance explained that some risky spots include those that offer free or public Internet services:

> Internet users need to be aware of the need to logging out after using the Internet, especially if they have been using public hotspots and Cybercafes.

The respondent explained that some Internet users may not be aware that their private content can be visible to other users on social sites when they fail to log out of the

platforms. In such a case, private information is available to whoever uses the same devices after them. The findings are supported by Moran and Weinroth (2008) who state:

> Internet users leave a trail of digital footsteps from birth to death, which multiplies by orders of magnitude with online banking, e-commerce and m-commerce using mobile phones.

The study findings are in tandem with previous studies that revealed that, despite the potential privacy risk, Internet users continue to share private information. For instance, the survey conducted by the Social Research Centre in Australia (2011) indicates that most Internet users are providing too much data in the networks. The survey found out that users are either assuming that their privacy is being protected, without taking the time to review the information themselves, or they are not worried about the privacy of the information they provide online. The study by Zhao *et al.* (2017) also found out that privacy awareness relating to Internet records is insufficient and that most people lack privacy protection skills.

Respondent 01CS further commented on the *right to be forgotten*. The respondent stated that, in some nations, individuals may demand the erasure of personal data from virtual databases. This would be a step towards data minimization.

5.6.5 Internet User-skills and Awareness

During the interviews, the need to equip Internet users with knowledge was the most mentioned strategy for preventing online privacy infringements. Most of the key respondents concurred that user awareness, concerning privacy and online security threats, should be created. The respondents generally agreed that knowledge would help Internet users to develop skills necessary for minimizing vulnerabilities posed by Internet communication. Respondents, therefore, emphasized the need for Internet users to safeguard their right to personal privacy while working online. Respondents 01CS, 2MS and 05MT noted that the Internet is largely an open and a free resource, therefore, Internet

users divulge abundant amounts of information. Respondent 02MS added that some Internet users are oblivious of the fact that their Internet activities can be accessed by other users leading to a breach of privacy. The respondent explained that user education is critical in safeguarding the privacy of communication on the Internet platforms. The respondent explained that:

> The simplest and or the most effective way is creating awareness because, if we cannot control what people do with the Internet…educate users to know the capabilities that come with which devices, which application or which Internet platform. Some of the applications used for voice or private communication come with features that…basically enable the person to have a little bit of privacy on it.

A study by Adams (2012) found out that Internet users who openly provide their personal information are becoming targets for privacy invasion. Before users can download applications, they are required to first accept permissions created by the application's developer. Users should, therefore, research the permissions each of the applications requests before accepting the service terms.

It was observed that Internet awareness should include building capacity on privacy security in online interactive applications. Respondents at MCK stated that the Council conducts regular training for journalists on matters of online ethics. Both 04MM and 06AC indicated that the training of journalists is conducted regularly in conjunction with the training department of the Media Council. For instance, 06AC stated:

> …together with the training department…we conduct training to remind them…and also to ensure that they practice according to the code of conduct of the practice of journalism.

Respondent 07PS also indicated that ICTA is working on capacity building in matters of ICT usage across the country:

> What we are doing is building capacity for citizens when it comes to technology, because, we have realized that we are deploying complex technology to common *mwananchi (ordinary citizen)* without training. There is a department coming up with a capacity-building Programme and we are planning to buy some vehicles...We will be going across the country and training common users, common *mwananchi (ordinary citizens)* on the utilization of this ICT. I think this will help.

According to the study by Boyd and Hargittai (2010, there is need to understand how digital media works:

> This kind of knowledge, and the self-efficacy that accompanies it, will enable users to maximize the potential social capital benefits from these sites while minimizing the harms that can accompany sharing some kinds of disclosures with some audiences. Hence, relevant communications techniques are going to be critically essential skills for participation.

Respondent 03LS indicated that creating user awareness would be far better than enforcement. The respondent explained that:

> The approach now would be more of creating awareness…enforcement in the event of computer crime is after the event has happened. So, the person has already suffered a loss…a wrong has already been done. so, chances are that people will be going in to rectify the wrong; but you

> can avoid that wrong if the players or users are aware of what is happening.

Respondent 03LS explained that CA has Consumer Education and Outreach Programmes to empower consumers to make informed decisions on the communication products and ICT services. The respondent elaborated that CA has a programme that focuses on consumer education known as *'Kikao Kikuu*'. The respondent indicated that the programme is a progarmme under the Consumer Protection and Public Affairs Department. Under the programme, CA conducts consumer empowerment meetings at County levels to raise awareness of ICT issues and service quality. 03LS explained that the programme targets the communities at the grassroots levels:

> It involves going to various Counties creating awareness to the consumers of ICT services. It is quite an intensive exercise because it is engaging with *watu wa kawaida, mwananchi wa kawaida* (the ordinary people, the ordinary citizen)…creating awareness on how you can use ICT services and if you have a complaint where you can report.

The commitment to consumer education is also to the programmes is popularized through the campaign dubbed "*Chukua hatua: pata huduma ya mawasiliano unayostahili" (This is a call on consumers to take action*). Clients are empowered to understand their rights, identify infringements including cybercrimes and, if violated, take necessary action.

03LS indicated that the Authority also initiated a Child Online Protection Policy (COP). This service has become necessary as children have become active consumers of the Internet and social media products. The respondent explained that the child online protection policy aims at safeguarding the privacy of children on the Internet. The COP programme ensures that children working online are not violated. The respondent further observed that, since children have now become active consumers of the Internet and social

media products, CA has focused on children's online protection by initiating the child protection awareness Programme. The respondent stated the following about the COP:

> …It is of keen interest because we have the whole Programme of COP running online…so, the key aim here is to raise awareness. When children go online to carry out any form of activity, be it studying, be it entertainment, be it education, as the parent or the guardian or as the person who is overseeing the activities of this child, awareness is very crucial

From the respondents, Internet user-awareness was emphasized as a key strategy for minimizing privacy infringement of Internet users. This is in agreement with the assertion made in the research by Williams *et al.* (2016). The researchers observe that:

> Education will be central in affording Internet users the knowledge and skills to maintain control of privacy of their information. The development of disclosure metrics for individuals and organizations will help technology users perceive the risks of their decisions, and assist regulators in detecting abuse.

Similarly, the research by Adams (2012) indicates that by becoming more aware of privacy issues, users can urge changes to be made to the way social media is approached. The findings concur with Li (2011) who indicates that users' skills and knowledge can minimize Internet users' vulnerability to online privacy disclosures. Personal knowledge and experience are important sources of information about privacy issues. These include general knowledge about Internet use and specific knowledge about privacy invasions.

Table 5.5: Strategies for Mitigating Violation of Online Privacy

Legislation and Policy	The National Information and Communications Technology- ICT Policy (2006) The Kenya Information and Communications (Registration of SIM-Card) Regulation(2015) The National Information and Communications Technology- ICT Policy (Reviewed in 2016) The Computer Misuse and Cybercrimes Act (2018) Data Protection Bill (2018) The National Information and Communications Technology- ICT Policy (Reviewed in 2020). The national constitution of Kenya (2010) The Media Council of Kenya Act (2013)
Enforcements of Compliance and Policy	Self- Regulation Media monitoring and analysis Licensing and inspection Accreditation and registration practitioners Training of journalist- MCK Computer Incidents response Complaint handling
Access Restrictions	Access restriction and security settings Strong passwords Encryption
Biometric Identification	Fingerprints Facial Voice recognition Combining of passwords and biometrics

Data Minimization	Minimize divulging private information
	Avoid logging into unknown weblinks and public hotspots
User-skills and Consumer Awareness	Dealing with pop-ups messages
	Internet and ICT Capacity Building
	Consumer Education Progarmmes
	Child online protection programme (COP)

5.7 Conclusion

The chapter focused on data analysis, discussion and interpretation of findings from interviews with the key experts selected for the study. Some major areas of privacy invasion on convergent platforms were revealed in the analysis of data from the respondents. The prevalent privacy issues identified included harvesting of personal data, disclosure of confidential information, susceptibility of social sites to cyber-attacks and fake news. Findings of the study also indicate that the availability of trailing applications, online anonymity, and unregulated social sites escalated infringement of privacy. Internet user vulnerability, surveillance, data storage media, and the need to access information were some of the factors considered to limit privacy protection on the IP, while the aspects of the Internet that undermine regulation of communication included searchability of virtual networks and Internet penetration and access. From the analyzed data, findings indicated that infringement of privacy on the Internet Protocol is an issue of concern.

The chapter also presented the analysis and discussion of the findings on the strategies for guarding against violation of online privacy. The strategies highlighted by the key respondents included legislation and policymaking. The respondent indicated that some Bills and Policies have been formulated including the Computer Misuse and Cybercrimes Act (2018), the Kenya Information and Communications (Registration of SIM-Card) Regulations (2015), the Data Protection Bill (2018), and the National Information Communication Technology-ICT Policy (2006, 2016, 2020). The Media Council also enforces professional practice through the Code of Conduct for the Practice of Journalism

in Kenya entrenched in the Media Council of Kenya Act (2013). One of the aspects protected by the Media Act is the privacy rights of people in news. The Bill of rights in the Constitution of Kenya (2010) also safeguards the privacy of communication.

The respondents cited other strategies such as enforcement of compliance and conformity, media monitoring and analysis, registration and accreditation of practitioners, licensing, inspection, incident response, and handling of complaints, user awareness and COP. The other strategies proposed by the respondents included data minimization, access restriction settings such as strong passwords and encryption. Biometric identification was also identified as means of protection from unauthorized information access. Some of the biometric identification methods identified included fingerprints, facial and voice recognition. However, one of the respondents noted that collection of biometric data might be another means of harvesting personal data that may expose individuals to privacy infringements. The findings indicate that most of the key respondents concurred that user-awareness is key in guarding against privacy infringements on the convergent platforms.

This chapter presented the strategies for mitigation of privacy invasion. The next chapter presents the summary of the study findings, conclusions and recommendations.

CHAPTER SIX: SUMMARY, CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

This chapter provides a summary of the findings from both the FGDs and the expert respondents. This chapter also provides the study conclusions and recommendations.

6.2 Summary of the Research Findings

The findings from FGD participants depicted a proliferation of Internet user publications and consumption of private information on the Internet spectrum. For instance, the participants regularly witnessed data of personal nature circulating on social sites. This chapter also presents the summary of the findings from the key respondents on strategies for mitigating online privacy infringements.

6.2.1 The Role of Multimediality and proliferation of Private Information

From the data analyzed, multimediality of media convergence emerged as a key element attributed to infringements of privacy of Internet users. It emerged that Internet users have adopted sophisticated multimedia smart devices, Internet user-tools, software and applications with various functionalities that enable production, access and unrestricted sharing of information of the convergent social sites. As respondent 07PS noted, there is deployment complex technology to common *mwananchi (ordinary citizen)* without training, and consequently the need for capacity building.

From the content gathered through the FGDs, there is a proliferation of uncontrolled user-generated Internet activities on social sites where information of personal nature is shared. Internet users are constantly working online in creating, receiving or disseminating information by the use of interactive applications and smart devices. The study identified aspects of multimediality of media convergence that permit users to invade the privacy of others. From the data analyzed from the FGDs, information is often accessed and shared by reposting to other users. The content was mostly in form of multimedia elements and

formats such as videos, audio clips, texts, photos and screenshots. Respondent 05MT noted that it has become easy, cheap and convenient to set up online resources, hence, the rise of uncontrolled social sites. Most of the key respondents observed that the emergence of versatile devices used to communicate on the Internet spaces has aggravated the production of unregulated user-generated content.

From the experiences of the FGD participants, creation and transmission of content were constantly conducted through social networks and platforms such as Facebook, Twitter, Instagram, WhatsApp, Imo or Telegram. Findings revealed that Internet users were, without any form of restriction, divulging information of personal nature on the social platforms. The findings are supported by the key respondents who noted that Kenya has the highest Internet absorption rate in the region. The high rate of Internet access has stimulated online activities.

6.2.2 Hypertexuality and Shocking News, Violence, Crime and Sexual Assault

Findings of FGD participants showed that Internet users published and circulated shocking content on acts of violence, crimes and sexual assault. Some of the materials witnessed on the Internet by the participants included live scenes of violence such as terrorism, war, murder, police brutality, domestic violence and mob justice. Identifiable materials were published and circulated in form of videos and pictures. The activities linked to intrusion of privacy included filming, posting and reposting of content.

The identifiable content on issues of sexual assault, witnessed by the FGD participants on the social sites included names, pictures and videos. Whenever such kind of personally identifiable content was produced and shared, it amounts to invasion of privacy. Such exposures are deemed to intrude on the person(s) that should otherwise be protected. The Media Council Act (2013) discourages disclosures of identifiable materials such as pictures and names:

> The media shall not identify victims of sexual assault or publish material likely to contribute to such identification.

> As a general rule, the media shall apply caution in the use of pictures and names and shall avoid publication. when there is a possibility of harming the persons concerned.

On the same note, findings from the key respondents such as 04MM and 06AC indicated there are various media creators, who are not trained journalists, producing and distributing media content on the convergent networks. Hence, enforcing the best practices stipulated by the Media Council of Kenya Act (2013) and other communication policies, including self-regulation, has become a challenge. The key respondents also observed that the anonymity and the autonomy that exist on the convergent media platforms, constrained the effort to control the activities of the social sites.

6.2.3 Interactivity and Intrusion on Bereavement and Grief

The findings of the study attributed the interactivity of the Internet platforms to easy and speedy dissemination of content concerning bereavement and private grief. Some of the participants confirmed that they frequently witnessed disturbing personally identifiable content involving grief on social sites. The FGD participants observed that intrusion of privacy of people in bereavement is escalated by the nature of the Internet in terms of virtual connectivity, searchability and accessibility. Findings indicate that users have easy access to Internet navigation tools such as search engines and web browsers. Almost all the participants across the FGDs indicated that intrusion on bereavement and grief on the social sites was high. The findings are validated by the responses from the key respondents interviewed in the study. As noted by the key respondents 07PS and 05MT, audiences have assumed the role of creating and sharing news. One of the challenges faced in enforcing compliance is the rise of unregulated social sites that produce unverified news. Secondly, the news is transmitted speedily and is equally accessed on the platforms.

6.2.4 Strategies for Mitigating Infringements of Privacy

Findings from the key respondents, harvesting of personal data, disclosure of confidential information, susceptibility of social sites and publication of fake news were some of the

issues considered to be prevalent in regarded to intrusion of privacy on the Internet. The respondents indicated that Internet trailing tools, online anonymity and the proliferation of unregulated social sites were responsible for escalating infringements of privacy of Internet users. The factors considered to limit privacy protection on the Internet convergent platforms included Internet user vulnerability, surveillance, data storage media and the public interest to receive news. The key respondents also identified the aspects of the Internet considered to undermine the regulation of online communication on the convergent platforms including searchability, and Internet penetration rate and access.

The findings of the FGDs, presented in Tables 4.1 and 4.2, demonstrated that the participants owned smart devices with great capabilities. Internet users used smart devices to create, access, store or distribute information; hence, risking their privacy. The FGDs participants indicated that they are registered in various social platforms including Facebook, Instagram, Telegram and Imo. Some participants indicated that some of the information requested when registering the social media accounts was of personal nature. The findings of the FGDs also demonstrated that the participants regularly witnessed various materials that would be considered private on social sites. This means that people were sharing private content on the Internet platforms without deeply reflecting on the vulnerabilities involved.

On mitigation strategies, the key respondents advocated for enforcement of compliance and conformity to standards. From the findings, various strategies were adopted including legislation, media monitoring and analysis, incident response, forensic investigations, accreditation and registration of practitioners, training of journalists, and licensing and inspection of service providers and ICT suppliers. The other strategies highlighted include data access restrictions, data minimization, Internet user and consumer education, and complaint handling. Findings indicated that self-regulation is encouraged but may not compressively address the aspect of Internet infringements of privacy on the cyberspaces, as communication in these spaces is often conducted by other online players other than trained journalists. This aspect of Internet authorship was manifested by FGDs participants' activities and the materials they constantly witnessed on the social sites.

Legislation and policymaking effort were demonstrated in the formulation of various Bills and the review of some policies such as The National Information and Communications Technology-ICT Policy (2006). The Policy was reviewed in 2016 and, later, in 2020. It is also anticipated that the implementation of the disputed Computer Misuse and Cybercrimes Bill (2018) would be key in cyber regulation and protection of privacy. Formulation of the Data Protection Bill (2018) is a crucial development in data protection. Under the Bill, processing of personal data is restricted unless under the conditions specified in the Bill. The Media Council of Kenya Act (2013) requires journalists to respect the right of privacy of people in news. The National Constitution (2010) also provides for the protection of privacy of communication from infringement.

However, this research found out that the regulatory effort is faced with competing factors. For instance, national jurisdiction limits were considered to constrain the control and the enforcement of protection against infringements of privacy of Internet users. The findings also indicated that the media convergence environment is steadily evolving; hence, the regulatory framework and the enforcement effort are continually being challenged by the changes that stir the new communication ecosystem. From the data analyzed in this study, it is apparent that protection of online privacy has not been sufficiently realized. Findings revealed that infringement was being witnessed on social sites. This indicates that privacy vulnerability exists on the convergent platforms.

Despite the privacy concerns depicted by the findings of this study, it is worth considering that media convergence has a profound benefit to the overall global populace in terms of socio-economic headways. As respondent noted 03LS asserted, regulating the IP at an early stage might stifle the innovation aspect of technology. Some authors have also looked at the brighter side of the media convergence, for instance, Chung and Paynter (2002) assert that:

> Perhaps, there is no other external object quite like these digital tools, hardware and software, capable of usurping more capacity as moral agent in collaboration with “human-

> ware". Today authors do not perceive a dystopian future like the one that some sociologists wished to avoid. The Internet is a great tool being widely used in interactive communication. With only a few mouse-clicks, people can follow the news, buy goods and order for services, and communicate with each other in real-time around the global cyberspace.

According to Yualabi (2014) the adoption of high-performance computers, shift to digital platforms, and creation of high-speed computer networks have brought us new ways of doing things. Old barriers of time and space are practically eliminated. You can view, hear, or read virtually anything, anywhere, anytime. Media people tend to get very excited about convergence because it holds so much promise. The melding together of different media, incorporating new personalized services is both impressive and overwhelming.

6.3 Study Conclusions

The research explored role of media convergence in intrusion of online privacy. From the findings of the study, the following conclusions were made:

1. The Internet users in the FGDs demonstrated adequate knowledge of the content that entails private information but, apparently, did not seem to refrain from divulging content of private nature on the social sites. Participants witnessed various personally identifiable materials relating to news of shock, acts of violence, crime, sexual assault and grief on the networked sites. This is an indication that privacy infringements were constantly being experienced. The key experts also indicated that Internet users are exposed to considerable vulnerabilities while working online.
2. The emergence of new communication technologies such as multimedia communication devices, tools and applications, and the accessibility of the Internet aggravated the proliferation of uncontrolled social sites, unrestricted production and sharing of information.

3. An array of mitigation strategies had been adopted ranging from legislation and policy-making effort, enforcement of compliance, accreditation and registration, regular training of journalists, to licensing and inspection. MCK had a media monitoring tool, *The Media Observer*, that analyzes media content including electronic communication. Infringement complaints are handled by the complaint commissions in both MCK and CA. The KE-CIRT, the DCI and the NIS were engaged in coordination of incident responses and forensic investigations.
4. User-education, consumer-awareness and outreach programmes, ICT capacity building and the child online protection Programme (COP) were some of the strategies adopted to empower users of ICT products and services.

6.4 Recommendations of the Study

This research focused on role of media convergence in intrusion of online privacy in the media convergent platforms. The study makes recommendations in the following areas:

6.4.1 Recommendations for Policy

1. Communication regulation and policy-making need to constantly focus on the evolving IP platforms and the emerging technologies in order to continually review the regulatory environment.
2. To consider the possibility of making a comprehensive privacy law that would, primarily, protect the aspect of privacy of online communication. The findings of this study indicated that, despite the existing regulations and policies, privacy violations were being experienced on the Internet social platforms.
3. Since the Internet Protocol is an open virtual resource, there is a need to explore the possibility of strengthening collaborations among nations in dealing with Internet privacy infringements, as jurisdiction limits were deemed to challenge the control of infringements on the IP spectrum.

6.4.2 Recommendations for Practice

1. To encourage minimization of data volumes, as findings indicated that unrestricted production, harvesting, retention, and distribution of personal data were linked to

various privacy infringements such as hacking, data breach, data theft, impersonation and identity theft.

2. As the findings from FGDs demonstrated that university students are not only constant users of online social sites but also active consumers of ICT products and services. Therefore, it would be essential to consider the possibility of extending Consumer Education and Outreach Programmes to this population. Findings from the key experts strongly indicated that Internet user-awareness is a critical strategy in mitigation privacy infringements.

6.4.3 Recommendations for Research

This study recommends the following areas for further research:

1. Investigating implications of privacy infringements on the cyberspaces.
2. Exploring Internet user-awareness of cyber privacy risks.

REFERENCES

Adams, B. I. (2012). *Social Media and its Effect on Privacy*. A Research Thesis. University of Central Florida, Orlando. http//www.etd.fcla.edu. Retrieved on 8/8/2018.

American Civil Liberties Union: *https://www.aclu.org/.../privacy.../internet.../* Retrieved on 5/9/2017.

American Society of Newspaper Editors Code of Ethics (1996, 2002). *ASNE Statement of Principles.* http://www.asne.org/kiosk/archive/principl.htm. Retrieved on 13/10/2018.

Ani, O. E. (2010). Internet access and use: A study of undergraduate students in three Nigerian universities. *The Electronic Library, 28*(4), 555-567. Retrieved on 8/1/2016.

Anwar, S., Zain, J. M., Zolkipli, M.F., Inayat, Z., Khan. S., Anthony, B. & Chang, V. (2017). From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions: *Algorithms*: http://creativecommons.org. Retrieved 25/11/2017.

Appelgren, E. (2007). *Media Convergence Strategies and Digital News Services*. A Doctoral Thesis: Retrieved on 10/8/2018.

Australian Press Council: www. presscouncil.org.au: Retrieved on 12/4/2016.

Babich, A. (2012). *Biometric Authentication: Types of biometric identifiers*. A Thesis. Haaga-Helia University of Applied Sciences. Retrieved 21/4/2018.

Baker, T. L. (1994). *Doing Social Research*. 2nd Edition. McGraw Hill, New York.

Banning, S. & Sweetser, K. (2007). How Much Do They Think It Affects Them and Whom Do They Believe? Comparing the Third-Person Effect and Credibility of Blogs and Traditional Media. *Communication Quarterly, 55*(4), 451-466. Retrieved on 30 /3/2016.

Baran, S. (2002). *Introduction to Mass Communication*. McGraw Hill, New York.

Baran, S. J. & Davis, D.K (2010). *Mass Communication Theory: Foundations, Ferment, and Future.* Sixth Edition, Wadsworth, Cengage, Boston.

Baxter, P. & Jack, S (2008). *Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers.* McMaster University, West Milton, Ontario.

Bhutan Code of Ethics for Journalists (2006). *Bhutan Information, Communications and Media Act. Bhutan Information and Media Authority*. Royal Government of Bhutan. Thimphu. http://pubs.sciepub.com/ajis/4/3/2.dio:10.12691/ajis-4-3-2. Retrieved on 25/11/2017

Bijone, M. (2016). A Survey on Secure Network: Intrusion Detection & Prevention Approach. *American Journal of Information Systems, Vol. 4, No. 3, 69-88.*

Borgmann, L. (2012). Universal Principles of Media Ethics: South African and German Perspectives. *Global Media Journal,* German Edition Vol. 2, No.2. Retrieved on 10/4 /2016.

Boyd, D. & Hargittai, E. (2010). *Facebook privacy settings: Who cares? First Monday*,15 (8). *journals@UIC.* Retrieved on 16/2/2020.

Boyd, D. (2008b). *Taken out of context: American teen sociality in networked publics*. A PhD Dissertation, University of California Berkeley. www.dana.org.retetrieved on 16/2/2020.

Burgess, J. & Green, J. (2009). *YouTube – Online Video and Participatory Culture. Digital Media & Society* Series, Polity Press, Cambridge.

Calvert, C. (2006). *The Privacy of Death: An Emergent Jurisprudence and Legal Rebuke to Media Exploitation and a Voyeuristic Culture*. http:pdf. semantic scholar.org. Retrieved on 16/2/2020.

Carpenter, E. & McLuhan, M. (1960). *Explorations in Communication: An Anthology*. Beacon Press, Boston.

Chung, W. & Paynter, J. (2002). *Privacy Issues on the Internet*. A Conference paper. Retrieved on 8/10/2016.

Clark, L. A. & Roberts, S. J. (2010). Employer's use of Social Networking Sites: A Socially Irresponsible Practice. *Journal of Business Ethics,* 95 (4), 507–525. www.homepages.se.edu. Retrieved on 16/2/2020.

Code of Ethics for Journalists (2006): *Bhutan Information, Communications and Media Act*: Retrieved on 10/4/2016.

Communications Authority of Kenya (CA). https://ca.go.ke/wp-content/uploads/2021/01/Sector-Statistics-Report-30th-December-2020.pdf. Accessed on 27/4/2021

Cowles, J. (2009). The Internet as Utopia: Reality, Virtuality, and Politics. University of Wisconsin Oshkosh. *Oshkosh Scholar*. Volume IV, pp. 81-89. Retrieved on 9/10/2016.

Crabtree, A. & Mortier, R. (2017). *Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control*. https://ssrn.com/abstract=2874312. Retrieved on 21/4/2018.

Creswell, J. (2009). *Qualitative and Quantitative and Mixed Method Approaches*. Thousand Oaks Sage, California.

Culnan, M. (1993). "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes towards Secondary Information Use." *MIS Quarterly*, 17(3), 341. Retrieved on 26/6/2016.

Cummings, N.M. (2008). *The Uses and Gratifications of Communication in Virtual Spaces: Media Depictions of Second Life*. A Thesis. University of Oregon.

Cybercrime Convention of the Council of Europe (2001). *Centre for Communication Governance*. ccgnludelhi.wordpress.com. Retrieved on 12/7/17.

Davis, W. S. & Eldridge, S. (2012). Privacy, Confidentiality, and Data Security in the Age of Electronic Records and the Internet: Implications for "Human Subjects Review" in the Social Sciences: *Western Political Science Association (WPSA) Conference, Portland*. Retrieved on 25/11/2017.

Deuze, M. (2007). *Media Work*. Cambridge.htt://oda.hio.no/jspui- /51264.post.pdf. Polity Press. Retrieved on 1/5/2016.

Devi, B. B. & Roy, R. N. (2012). Internet Use among University Students: A case study of Assan University. *A Journal of Humanities and Social Sciences*. hptt://WWW.thecho.in/…/ pg.182-202. Retrieved on 8/1/2017.

Dwyer, T. & Martin, F. (2012). *Convergence: Operational Legal and Ethical Trends in Online and Cross Media News Production*.www.presscouncil.org.au/…/Retrieved on 11/7/2017.

Editors Code of Practice. (2011*)* http://www.preewise.org.uk. Retrieved on 12/4/2016

Erdal, I. J. (2007). Media Convergence and Cross media News Production. Mapping the Field. *Nordicom review, 28* (2007) 2, pp. 51-61. Retrieved on 10/8/2018.

European Union Charter of fundamental Human Rights (2000). *M.Dw.com.* Retrieved on 20/7/2017.

Flanagin, A. J. & Metzger, M. J. (2008). Digital Media and Youth: Unparalleled Opportunity and Unprecedented Responsibility. *MacArthur Foundation Series on Digital Media and Learning.* 5–28. doi: 10.1162/dmal.9780262562324.005. Cambridge, MA: The MIT Press. Retrieved on 16/4/2016.

Fleury, A. (2012). *Near-future Trends in Interactive Media Convergence using Quantitative and qualitative Approaches:* A PhD Thesis. Lars Bo Larsen Aalborg University. Retrieved on 7/8/2018.

Foly, B. (2018). Purposive Sampling. www.surveygizmo.com. Retrieved on 17/2/2018.

Frik, A., Nurgalieva, L., Bernd, J., Lee, J ., Schaub, F., Egelman, S. ((2019*). Privacy and Security Threat Models and Mitigation Strategies of Older Adults*. https://www.usenix.org/conference/soups2019/presentation/frik. Retrieved on 28/3/2021.

Fuchs, C. (2013b). *Political economy and surveillance theory: Critical Sociology*. 39(5), 671–687.www. fuchs.uti.at.>marxsurveillance. Retrieved on 16/2/2020.

Galterio, M. G., Shavit, S.A., & Hayajneh, T. (2018). A Review of Facial Biometrics Security for Smart Devices. *Computers.* Retrieved on 10/10/2018

Gillmor, D. (2008). *Principles for New Media Literacy.* Berkman Center for Internet and Society at Harvard University. Boston.

Gómez-Diaz, R. & Arroyo-Almaraz, I. (2015). *The Undesired Effects of Digital Communication on Moral Respons*e. http://dx.doi.org.| Pages: 149-158.hptts://revistacommunocar.com/veered. Retrieved on 7/4/2016.

Goodman, P. (2019). Disadvantages of Digital Technology: hptt/: www turbofuture.COM. Retrieved on 11/9/2019.

Gordon, P. (2007). *Data Leakage - Threats and Mitigation*: SANS Institute. Retrieved on 18/1/2018.

Grant, A. E & Wilkinson, J. S. (2009). *Understanding Media Convergence: The State of the Field*. Oxford University Press, New York. Retrieved on 10/8/2018.

Grinch, J. L. R. (2015). *Personal Perceptions of Privacy and Security. Thesis. Georgia SouthernUniversity*.http://digitalcommons.georgiasouthern.edu/honors-theses. Retrieved on 7/8/2018.

Gross, R. & Acquisti, A. (2005). *Information revelation and privacy in online social networks: ACM -Workshop on Privacy in the Electronic Society*. PDF. www.heinz.cmu.ed.papers. Retrieved on 16/2/2020.

Grubbs, A. (2011). *Privacy Law and the Internet using Facebook.com as a Case Study: Thesis Project.* Retrieved on 23/4/2018.

Hanrahan, H. (2004). *Modeling Convergence: Technology Layering for Horizontal Regulation:* http://www.ee.wits.ac.za/comms/Telecomms.output/output/satnac./hanrahan.pdf. Retrieved 16/2/2020.

Haraszti, M, Baydar, Y., Gore , W., Zlatev, O., & Maurus, V. (2008). *The Media Self-Regulation Guidebook*. Miklós Haraszti, The OSCE Representative on Freedom of the Media. Vienna.

Hazzi, O. A. & Maldaon, I. (2015). *A Pilot Study: Vital Methodological Issues*. http://www.btp.vgtu.lt. Accessed on 11/2/2020.

Heale, R. & Forbes, D. (2013) *Understanding Triangulation in Research Studies That Use Triangulation.* https://ebn.bmj.com/content/ebnurs/full.pdf

Ibrahim, F., Pawanteh, L., Peng Kee, C., Basri, F.K., Hassan, B. R. & Mahmud, W.A. (2011). *Implications of Professionalism in War Reporting.* Retrieved on 26/12/2018.

ICT and Privacy in Europe (2006). A Report. Retrieved 2/1/2017.

Independent Press Standards Organization (IPSO) Editors' code (2019). WWW.ipso.co.ku. Accessed 10/2/2020.

International Labour Organization-ILO (1997). *Protection of Workers' Personal Data.* https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf. Retrieved on 21/3/2021

Jenkins, H. (2002). *Interactive Audiences? The ''Collective Intelligence'' of Media Fans.* Retrieved on 1/5/2016.

Jenkins, H. (2004). The Cultural Logic of Media Convergence. *International Journal of Cultural Studies*. SAGE Publications London, Thousand Oaks, CA and New Delhi. www.sagepublications.com Volume 7(1): 33–43. Accessed on 10/2/2020.

Jenkins, H. (2006*). Convergence Culture: Where Old and New Media Collide*. New York University. Presswww.nyupress.org Accessed on 26/6/2016.

Jenkins, H. (2006*). What Happened Before You Tube? You Tube – Online Video and Participatory Culture.* Digital Media & Society Series. Polity Press, Cambridge.

Jhally, S. (1982). Probing the Blind spot: The Audience Commodity. *Canadian Journal of Political and Social Theory/Revue Canadienne de theorie politique et sociale,* Vol. 6, Nos. 1-2 (Hives/Printemps. Retrieved on 3/3/2016.

Kalamar, D. (2016). C*onvergence of Media and Transformation of Audience. Feri, Institute of Media Communications*. University of Maribor, Slovenia. https://hrcak.srce.hr>file. Retrieved 7/8/2018.

Kalan, M. (2011). *Expressions of Grief on Facebook: Navigating Discomfort, Persistent Identity, and Public Memorialization*: Master Thesis in Media Studies, Syracuse University.

Kammer, A. (2013). *News on the Web: Instantaneity, Multimodality, Interactivity, and Hypertextuality on Danish News Websites.* A PhD Dissertation, University of Copenhagen. Retrieved on 6/7/2016.

Kenjebaev, N. (2008). *Protection of Privacy and the Personal Data in the Information Age*: Malaysian Approach. International Islamic University, Malaysia.

Kenya Information and Communications Act (2010): *National Council for Law Reporting*: www.kenyalaw.org. Retrieved on 12/9/2016.

Kenya Internet Users: www.allafrica.com . Retrieved on 20/4/2018.

Kenya Media Council Act (2013). *Kenya Gazette Supplement No. 180 (Acts No. 44).* Government Printer, Nairobi.

The National Information and Communications Technology (ICT) Policy (2006). www.information.go.ke. Retrieved on 22/1/2017.

KHRC (2014). *The Internet Legislative and Policy Environment in Kenya*. Website: www.khrc.org.ke . KHRC. Retrieved on 10/2/2020.

Khumalo, S. L. (2013). *News as Commodity vs. Public Good. Adaptation Strategies of South Africa Newspapers in Digital Era*. A Dissertation. University of Pretoria. Retrieved on 16/2/2019.

Knowledge@Wharton, (2007), *Matching Technology to Consumers Demand*. http://www.upenn.edu/researchatpenn/article.php?1166&tch. Retrieved on 10/4/2016.

Kothari, C. (2004). *Research Methodology; Methods and Techniques*. New age International, New Delhi.

Kroker, A. (1984). *Technology and the Canadian Mind.* New World Perspectives. Montréal.

Kruger, F. (2004). *Black, White and Grey: Ethics in South African Journalism*. Cape Town: Double.

Kugler, L. (2015). Online Privacy: Regional Differences. *Communications of the ACM*, vol. 58 (2). pp. 18-20. http://dx.doi.org/10.1145/2693474. Retrieved on 7/8/2018.

Kumar, R. (2011). *Research Methodology: A step-by-Step Guide for Beginners*. Sage Publications. Los Angeles.

Kun, F., Yang, K., Ha, I., Yuping, Z., Mengyao, W. & Nute, K. (2012). Mapping Digital Media: China. Country Report; *Open Society Foundations*. Retrieved on 3/12/2017.

Kuss, D. J., Griffiths, M. D., & Binder, J. F. (2013). Internet addiction in students: Prevalence and risk factors. *Computers in Human Behavior*, 29(3), 959–966. Retrieved on 30/9/2018.

Latzer, M. (2013). *Media Convergence – Media Change and Innovation*. University of zurich, Switzerland. www.mediachange.ch>pdf>publication.l…Retrieved on 8/8/2018.

Law Reform Commission of Hong Kong Report: Privacy and Media Intrusion (2004). http://www.hkreform.gov.hk. Accessed 12/4/2016.

Laws Governing Media Practice in Kenya (2014). *A Journalists' Handbook: Association of Media Women in Kenya*- AMWIK: www.amwik.org. Retrieved on 21/5/2016.

Leadbeater, C. & Miller, P. (2004). *The Pro-Am Revolution: How Enthusiasts Are Changing Our Economy and Societ*y.www.demos.co.uk. Retrieved on 27/4/2018.

Leslie, A., Ingrid, M. & Brandley, E. (2009). *Qualitative and Mixed Methods provide Unique Contributions to Outcomes Research.* Yale University, New Haven

Li, Y. (2011). *Empirical Studies on Online Information Privacy Concerns: Literature Review and Integrative Framework. Communications of the Association for Information Systems:* Columbia College, http://aisel.aisnet.org/cais. Retrieved on 8/8/2018.

Liu, E. & Pak-Kwan, C. (1999). *Regulation of media intrusion. The experiences of Taiwan, the United Kingdom and United States.* https://legco.govt.hk-. Retrieved on 19/7/17.

Marchione, R. C. (2009). *Participatory Culture and Commodification in The Age of the "Digital Revolution*". A Thesis. Georgetown University. Retrieved on 16/2/2019.

McCombes, S. (2019). *An introduction to sampling methods.* https://www.scribbr.com/methodology/sampling-methods/. Retrieved on 27/2/2021.

McMillan, S. J. (2002). *Exploring Models of Interactivity from Multiple Research Traditions: Users, Documents, and Systems.* www.utk.edu. Retrieved on 11/2/2020.

Medel, T., Hawtin, D., Wagner, B. & Torres, N. (2012). Global Survey on the Internet Privacy and Freedom of Expression: *UNESCO Series on the Internet Freedom.* UNESCO, Paris. Accessed on 25/11/2017.

Media Council of Kenya & International Media (MCK/IMS (2014). Trauma Book for Journalists: Images That Stay Forever: Special Edition, Kenya: *International Media Suppor*t.www.mediacouncil.or.ke. Retrieved on 4/3/2018.

Media Council of Kenya Handbook (2016) *Anatomy of Conflict: A Conflict Analysis Handbook for Journalist: Towards Conflict Sensitive Reporting:* www.mediasupport.org. Retrieved on 2/ 9/2018.

Media Law Handbook for Southern Africa (2013), Vol. 2: Konrad-Adenauer-Stiftung- Regional Media Programme. Johannesburg.

Medium. freecodecamp.org. Retrieved on 19/4/2018.

Metzger, J. & Flanagin, A. (2008). *Digital Media, Youth and Credibility*. The MIT Press, Cambridge. Pg5–28. Retrieved on 10/4/2016.

Moor, J. H. (1991). *The Ethics of Privacy Protection:* Horton Hall, Dartmouth College, Hanover. Retrieved on 19/4/2017.

Moor, J. H. (1997). Towards a Theory of Privacy in the Information Age: *Computers and Society*, Vol. 27, No. 3, pp. 27-32. Retrieved on 19/4/2017.

Moran, T. J. & Weinroth, J. (2008). Invasion of Privacy on the Internet: Information Capturing without Consent: An Ethical Background as It Pertains to Business Marketing. *Journal of Business & Economics Research – July 2008 Volume 6, Number 7 pg. 43-48*

Morgan, D.L (1997). *Focus Groups and Qualitative Research*. 2nd ed. 16th series. Thousand Oaks, Sage. California.

Mugenda, A. & Mugenda, O. (2003). *Research Methods: Qualitative and Quantitative Approaches*. Acts press. Nairobi.

Muniandy, B. (2010). Academic Use of Internet among Undergraduate Students: A Preliminary Case Study in a Malaysian University. *International Journal of Cyber Society and Education*. Pages 171-178, Vol. 3, No. 2. Accessed 16/1/2017

National Information Communication and Technology-ICT Policy- Kenya (2006). Retrieved 25/10/2016.

Newman, D. (2014). There is no Privacy in the Internet of Things :The Little Black Book of Billionaire Secrets: *Forbes*: Wwww.forbes.com. Retrieved on 19/7/2017

Nosko, A.; Wood. E. & Molema, S. (2010), '*All about me. Disclosure in online social networking profiles. The case of Facebook', Computers in Human Behavior*, 26 (3), 406–418.

O'Reilly, T. (2005). *What is Web 2.0? Design Patterns and Business Models for the Next a Generation of Software* http://oreilly.com/web2/archive/what-is-web-20.html. Retrieved on 12/9/2016.

Orodho, J. (2009). *Elements of Education and Social Sciences Research methods*. Knezja Publishers, Kenya.

Parliament Assembly Council of Europe (2011). www. assembly.coe.int/…/xref-xml2html-e…Retrieved on 12/7/17.

Pathak, (2016). Digital Age 2.0 and its challenges on media ethics. *IOSR Journal of Humanities and Social Science (IOSR-JHSS),* Volume 21, Issue 1, Ver. I (Jan. 2016) PP 18-24. Retrieved on 3/12/ 2017.

Patton, M. (1990). *Qualitative Evaluation and Research Methods*. Beverly Hills, CA: Sage.

Phelps, J. G, Nowak & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information: *Journal of Public Policy and Marketing* 19(1). Retrieved on 12/7/2017.

Polit, D. G., Beck, C. T & Hungler, B. P (2001). *Essentials of Nursing Research: Methods, Appraisal and Utilization*. 5th Ed. William & Wilkins. Lippincott, Philadelphia.

Porta, M. (2008). A dictionary of Epidemiology. *Journal of American Epistemology*. 5th Edition. Oxford: Oxford University Press. 320 P.Www.Academia.Dk. Retrieved on 21/2/2020.

Powell, D. (1990). *Media Intrusion into Grief*. www.journals.sagepub. com. Retrieved on 12/7/2017.

PressWise (2003). Suicide Sensitive Journalism Handbook (Sri Lanka). *Centre for Policy Alternatives (CPA)* http://www.preewise.org.uk. Retrieved on 25/4/2016.

Privacy Technical Assistance Center: http://nces.ed.gov/ptac)htts://nces.edgov/ptac. Retrieved on 11/7/2017.

Prosser, W. (1960). The Torts of Privacy, *California Law Review* 383(48), 392-398. Retrieved on 3/7/2017.

Pryor, L. (2001). Who Gives a Damn about Privacy? *Online Journal Review*.

Reuters Hand Book of Journalism (2008*).* www.trust.org. Retrieved on 5/2/2015.

Rider, K. (2016). *The Privacy Paradox: Privacy, Surveillance, and Encryption*. A Thesis: University of Washington. Retrieved on 7/8/2018.

Ruggiero, T. (2000). Uses and Gratification in the 20th Century. *Mass Communication and Society. 3* (1), pg. 3–37.\. Retrieved on 21/4/2016.

Safieddine, F & Ibrahim, Y. (2020). *Fake News in an Era of Social Media: Tracking Viral Contagion*
https://books.google.co.ke/books?id=sb89dwaaqbaj&dq=fake+news&hl=en&sa=x&ved=2ahukewi6k7u_4b7vahvlshuihtkldrgq6aewbnoecauqag.
Retrieved on 20/3/2021

Saltzis, K. (2015). *Media Convergence in News Organizations. How Digital Technologies affect Journalists & the Management of News Production*. A PhD Thesis. University of Leicester. ProQuest llc. Retrieved on 7/8/2018.

Schafer, R. (2007). The "*Acoustic Space*": http://id.erudit.org/iderudit/017594ar.vol.17, pg. 83-86. Retrieved on 1/4/2016.

Schafer, R. (2011). *Bastard Culture! How User Participation Transforms Cultural Production.* Amsterdam University Press, Amsterdam.

Schreiber, J. & Kimberly, A. (2011). *Educational Research*. John Wiley and sons. Hoboken

Serem, D., Boit, J. & Wanyama, M. (2013). *Understanding Research: A simplified Form*. Utafiti Foundation, Kenya.

Shaw, M. & Black, D. (2008). *Internet Addiction: Definition, Assessment, Epidemiology and Clinical Management.* University of Iowa Roy J. and Lucille, A. Carver College of Medicine. Iowa, USA. Retrieved on 30/9/2018.

Shilton, K. & Sayles, S. (2016). "We Aren't All Going to Be on the Same Page About Ethics:" Ethical Practices and Challenges in Research on Digital and Social Media. *49th Hawaii International Conference on System Sciences.* Retrieved on 3/12/2017.

Showkat, N. & Parveen, H. (2017). *Non-Probability and Probability Sampling*: https://www.researchgate.net/publication/319066480. Retrieved 12/2/2021.

Singleton, T. (2013). The Top 5 cybercrimes: *American Institute of CPAs*. Retrieved on 19/4/2018.

Social Research Centre Report - Australia (2011). *Internet Privacy Research*. University of Queensland Centre for Critical and Cultural Studies: www.srcentre.com.au. Retrieved on 25/11/2017.

Stockwell, A. (2018). *Cyber Attack Bots Lead to the Charge in Online Security Crime*. www.cliqueapi.com. Retrieved 18/4/2018.

Sullivan, B. (2013). *Online Privacy Fears are Real*: www.nbcnews.com. Accessed on 16/10/2017.

Sumartias, S. & Hafizni, M. (2017). *Convergence Trends in the Television Media Industry: A Case Study on the Implementation of Media Convergence in Metro TV*. (2017) Retrieved on 7/8/2018.

Sundar, S. S. & Nass, C. (2001). Conceptualizing Sources in Online News. *Journal of Communication, 51*(1), 52. Retrieved on 3/7/17.

Sundar, S. S. (2008). The Main Model: A Heuristic Approach to Understanding Technology Effects on Credibility. *The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning*, 73-100. Retrieved on 3/7/17.

Taddicken, M. (2014). The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*:https://academic.oup.com/jcmc/article.abstract/19/2/248/4067550 doi:10.1111/jcc4.12052. Retrieved on 8/8/2018.

Tene, O., Polonetsky, J. & Stan, L. (2012). *Privacy in the Age of Big Data: A Time for Big Decisions*: Retrieved on 8/8/2018.

The Kenyan constitution, (2010). Government Printer, Nairobi.

The Media Council of Kenya Act (2013). http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/MediaCouncilAct2013.pdf. Retrieved on 6/3/2021.

The National Press Council of the People's Republic of China (1974). www.accountablejournalism,org> Taiwan. Retrieved on 17/7/2018.

The Research Advisors (2006). http://research-advisors.com) retrieved on 15/2/2017

Thierer, A. (2014). *Putting Privacy Concerns about the Internet of Things in Perspective*. iapp.org 8/8/18.

Thoene, S. (2012). *The Impact of Social Networking Sites on College Students' consumption patterns:* Master Thesis in Communication Studies, Marshall University. hptt://. marshall.edu//…/viewcontent.cgi Retrieved on 11/7/2017.

Tomlinson, J. (2007). *The Culture of Speed: The Coming of Immediacy*. Sage Publications. Los Angeles.

Tongco, C. (2007). Ethnobotany Research and Application. *Journal of Plants and People and Applied Research*. http:/hdl.handle. Retrieved on 19/4/2016.

Tran, A. H. (2015). The Internet of Things and Potential Remedies in Privacy Tort Law. *Columbia Journal of Law and Social Problems.* Retrieved on 23/4/2018.

Tulloch, J. (2004). Ethical Space: *The International Journal of Communication Ethics*. Vol1 No3. hptt://eprints.lincoln.ac.uk./uoa66jt05…Retrieved on 12/7/2017.

Turner, F. (2006). *From Counterculture to Cyber Culture: In Stewart, B, the Whole Earth Network and the Rise of Digital Utopianism.* Chicago University Press. Chicago.

UNICEF (1924). *Declaration of the Rights of the Child; Save the Children's Fund.* hptt://www.unicef.irc.org/…/ii-…Retrieved on 12/7/2017.

Vickers, R. (2012). Convergence, Media, Participation Culture and the Digital Vernacular: Towards the Democratization of Documentary. *International Conference on Communication Media, Technology and Design.* Istanbul, Turkey. comeindoc.com/…/resources.2-6-selected…Retrieved on 12/7/2017.

Vienna Declaration and Programme of Action (1993). Retrieved on 18/4/2018.

Volokh, E. (2014). *Tort Law Vs. Privacy*. Retrieved on 23/4/2018.

Walker, J.T & Maddan, S. (2019). Statistics in Criminology and Criminal Justice: Analysis and Interpretation. Fifth Edition. https://books.google.co.ke/books?id=cRaIDwAAQBAJ&dq=. Retrieved on 18/3/2021

Walsh, J. (2018). *Firewall Security: Best Practices for Firewall Rules*. https://www.liquidweb.com. Retrieved on 16/2/2019.

Ward, S. 2005. "Philosophical Foundations for Global Journalism Ethics." *Journal of Mass Media Ethics: Exploring Questions of Media Morality* 20(1): 3-21: https//ethics.jounalism.wisc.edu/…global Retrieved on 19/7/17.

White-Team Cybercrime: http://sysnet.ucsd.edu/~cfleizac/*WhiteTeam-CyberCrime*.pdf. Retrieved on 18/4/2018.

WHO (1998). Guidelines for Media Professionals; *Moscow Convention*. Moscow. http://www.presswise.org.uk. Retrieved on12/7/2017.

Williams, M., Axon, L., Nurse, J.C. & Creese, S. (2016). Future Scenarios and Challenges for Security and Privacy. *International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow* (RTSI). Retrieved on 3/12/2017.

Wimmer. R. & Dominick, J. (2011). *Mass Media Research: An Introduction*. 9th Ed. Wadsworth, Cengage. Boston.

Yualabi, O. (2014). *Concept of Media Convergence* (Article): https://ololadeganiyualabi. Retrieve on 11/9/2019.

Zeller, R. (1993). *Focus Group Research on sensitive Topics; setting the Agenda without Setting the Agenda. In Morgan L, Successful focus groups; advancing the state of the Art*. Newbury Park, Sage, California.

Zhao, H., Dong, Z., Hui, Z. & Dong, H.X. (2017). Personal Privacy Protection of China in the Era of Big Data. *Open Journal of Social Sciences*.5 139 145.https://doi.org/10.4236/jss.2017.56012. Retrieved on 8/8/2018.

Zimdars, M. & McLeod, K. (2020). *Fake News: Understanding Media and Misinformation in the Digital Age https://books.google.co.ke/books?id=8WPMDwAAQBAJ&printsec*. Retrieved on 20/3/2021

APPENDICES

APPENDIX I: Letter of Introduction

Kungu Nancy. W

Department of Communication, Media, Film and Theatre Studies

Kenyatta University

Dear Respondent,

RE: DATA COLLECTION FOR ACADEMIC RESEARCH

I am a postgraduate student undertaking a Doctor of Philosophy in Communication and Media studies at Kenyatta University. I am conducting an academic research for my Ph.D. Thesis. The research title is: *Exploring role of Media Convergence in Intrusion of Privacy: Experiences of Regular Internet Users in Nairobi City County, Kenya*. You have been identified as a resourceful respondent for this study. I am requesting your assistance to obtain the required data for the study. Your responses will be treated with confidentiality and your identity will remain anonymous. The findings of this study will be used for academic purpose only. Your participation is highly appreciated.

Thank you.

Yours faithfully,

Nancy Kungu

APPENDIX II: Discussion Guide for Focus Groups

This discussion guide was prepared and used for data collection from the conducted in the FGDs participants. The participants responded to the questions during the discussions concerning the concepts of multimediality, hypertextuality and interactivity and intrusion of privacy.

1. Multimediality and Proliferation of User-Created Content on Private Information

i. Provide a list of the devices commonly used by university students in communication on the Internet?

ii. Identify the functions/tasks that can be performed by the devices you have provided in (i) above

iii. What Internet tools and applications permit Internet users to access and share information that could intrude on privacy?

iv. Identify Internet activities performed by Internet users that, in your view, escalate invasion of privacy of others.

v. What type of private information do you often encounter on the Internet?

2. Hypertexuality Influence Real-Time Streaming of News on Victims of Violence, Sexual Assault and Crime

i) What is the nature of media content created by Internet users concerning the following?

a) News of shock

b) Acts of violence

c) Crime

d) Sexual assault

ii) In which ways does the content identified in (i) above jeopardize personal privacy?

3. Interactivity and Intrusion of Bereavement and Private Grief

i. What is the nature of cyberspace that supports the real-time circulation of news of grief?

ii. What user activities intrude on bereavement and personal grief on the Internet?

iii. In your opinion, how do you rate the level of invasion on personal grief through interactions on the Internet?

APPENDIX III: Interview Guide for Key Respondents

This interview guide was used to collect data on strategies for mitigating infringement of online privacy. The key respondents drawn from government institutions related to communication responded to the following questions in the guide:

1. What are the prevalent privacy invasion issues in relation to Internet usage?

2. What factors escalate infringements of online privacy of Internet users?

3. In your opinion, what are the factors that limit protection of privacy of Internet users?

4. What aspects of the Internet undermine regulation of online communication on media convergent platforms?

5. Suggest strategies for mitigating/guarding against violation of online privacy.

APPENDIX IV: Transcripts from Participants

The following are some transcripts from FGD conversations and Interview responses.

Some Transcripts from FGDs

Question. From the activities, we have mentioned. Which ones escalate privacy intrusion

FG 01: Screenshots

Question: What do screenshots do?

FG 02: Leaking conversations

Question: What other activities do people do?

FG03: Tagging photos

Question: What do you fill when people tag you?

GD 03: Bad. *Laughs…*yes bad.

Question: Why

FG03: There was no consent…People did not ask for permission.

FG 04:

…harassment…students are notorious for this…when you post something nice…like okay, 'am having a good day', Then guys come out there, then start abusing you by how you look…women especially, here in Kenya, they talk ill about your face…about how you look. Then people photoshop your face and put your profile some graphics.

FG05:

> Sometimes people take some pictures of people and put them on memes (*laughter*).

So, do you agree that this is an intrusion?

Yes! (*in a chorus*)

Question: What materials related to crime do you see?

FG06:

> During. okay…generally say...the al-Shabaab, we don't have a good relationship, when they kidnap like chiefs in North-eastern, then we see a video of them saying they will kill that chief if Kenya doesn't do what….so those are the threatening…going on currently.

FG 07

> Sometimes back there was a video of a person being robbed, but okay…the good thing is, the people stopped.

Question: What aspect of the Internet makes it simple for people to intrude others?

FG08: It is not very hard to have an account. People make multiple accounts.

Follow-up question: So, what do people do?

GF 09: People take videos and they upload.

Follow-up question: What else?

FG010: Photos. People take photos and upload them.

FG 011: Audio recording.

Some Transcripts from Interviews

Question: What are the areas of intrusion in relation to Internet usage?

> …if you are using a money lending application, people have reported cases…let's say I am your employee. I have taken a loan over a money lending application and I have defaulted on payment…bosses have reported having been called by operators of these mobile money lending applications and being requested to tell their employees to pay the loans they have defaulted on… I think that is a breach of privacy… so much exposure

Follow-up question: Does that affect the relationship with your boss?

> Yes, obvious, when a person chose to do that, there so many rights about this person that have been affected.

Question: What is digitization?

> Digitization…eeh, making digital? (*Laughter*), you see once upon a time, before digitization, we used to talk about analogue signals…that is how we used to transmit information but now we are changing everything into *ones* and *zeros*. when we are talking about digitization, we are changing everything from physical or from analogue into *ones* and *zeros*…we transmit it in *ones* and *zeros*…now technology has allowed us to change our communication…voice communication into data, we have digitized it as we have said.

Question. What about monitoring?

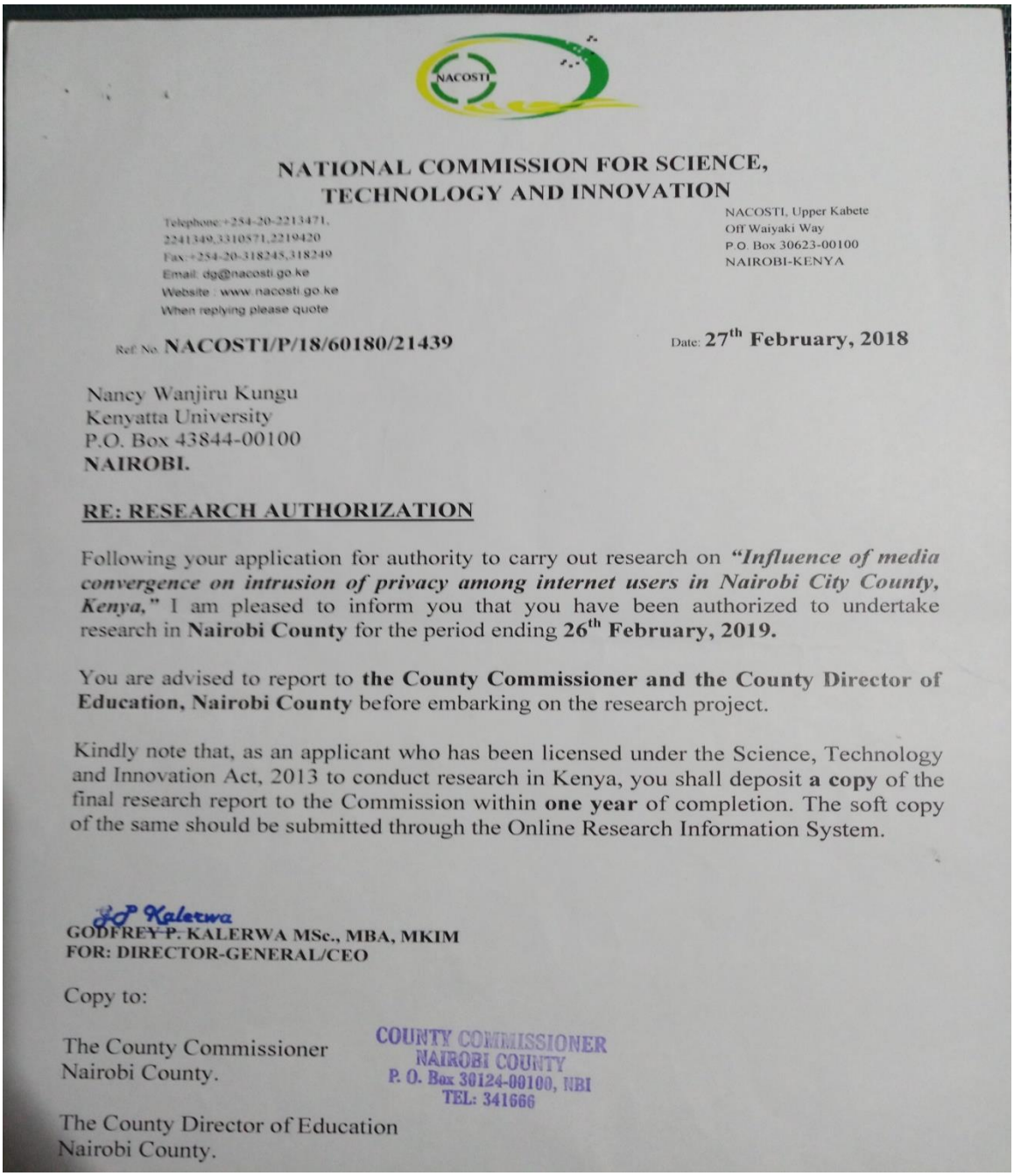
> What KE-CIRT does is to monitor specific areas. Especially when you are protection the national infrastructure. However, you cannot monitor everything about the Internet. It is too much. You just monitor what is important to you as a country and see how best you can address, for

example, cybercrime, viruses being sent into your nation…that kind of thing, hackings and all that.

Question: What are the prevalent privacy intrusion issues?

One is the security of the networks…about growing technologies whereby we have so many…groups who are ready to hack the network. We call them Internet hackers. Normally they look for ways of making a case. You know, when you hack a very tough network, then you have a case to say, 'I have seen, I can do this'.

APPENDIX V: Research Authorization Documents



NATIONAL COMMISSION FOR SCIENCE,
TECHNOLOGY AND INNOVATION

Telephone: +254-20-2213471,
2241349,3310571,2219420
Fax: +254-20-318245,318249
Email: dg@nacosti.go.ke
Website : www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref: No. **NACOSTI/P/18/60180/21439**

Date: **27th February, 2018**

Nancy Wanjiru Kungu
Kenyatta University
P.O. Box 43844-00100
NAIROBI.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"Influence of media convergence on intrusion of privacy among internet users in Nairobi City County, Kenya,"*** I am pleased to inform you that you have been authorized to undertake research in **Nairobi County** for the period ending **26th February, 2019.**

You are advised to report to **the County Commissioner and the County Director of Education, Nairobi County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

GP Kalerwa
GODFREY P. KALERWA MSc., MBA, MKIM
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The County Commissioner
Nairobi County.

COUNTY COMMISSIONER
NAIROBI COUNTY
P. O. Box 30124-00100, NBI
TEL: 341666

The County Director of Education
Nairobi County.

Republic of Kenya
MINISTY OF EDUCATION
STATE DEPARTMENT OF BASIC EDUCATION

Telegrams: "SCHOOLING", Nairobi
Telephone; Nairobi 020 2453699
Email: rcenairobi@gmail.com
cdenairobi@gmail.com

REGIONAL COORDINATOR OF EDUCATION
NAIROBI REGION
NYAYO HOUSE
P.O. Box 74629 – 00200
NAIROBI

When replying please quote

Ref: RCE/NRB/1/14/(29)

DATE: 28th February, 2017

Nancy Wanjiru Kungu
Kenyatta University
P O Box 43844-00100
NAIROBI

RE: RESEARCH AUTHORIZATION

We are in receipt of a letter from the National Commission for Science, Technology and Innovation regarding research authorization on **"influence of media convergence on intrusion of privacy among internet users in Nairobi City County, Kenya".**

This office has no objection and authority is hereby granted for a period ending 26th February, 2019 as indicated in the request letter.

Kindly inform the Sub County Director of Education of the Sub County you intend to visit.

28 FEB 2018

JAMES KIMOTHO
FOR: REGIONAL COORDINATOR OF EDUCATION
NAIROBI

Cc:

Director General/CEO
National Commission for Science, Technology and Innovation
NAIROBI

KENYATTA UNIVERSITY
GRADUATE SCHOOL

E-mail: kubps@yahoo.com
dean-graduate@ku.ac.ke
Website: www.ku.ac.ke

P.O. Box 43844, 00100
NAIROBI, KENYA
Tel. 8710901 Ext. 57530

Our Ref: M88/28111/14

Date: 3rd October, 2017

The Director General,
National Commission for Science, Technology & Innovation,
P.O. Box 30623-00100,
NAIROBI

Dear Sir/Madam,

RE: RESEARCH AUTHORIZATION FOR MS. NANCY W. KUNGU REG. NO. M88/28111/14

I write to introduce Ms. Kungu who is a Postgraduate Student of this University. She is registered for a Ph.D. degree programme in the **Department of Communication & Media Studies in the School of Creative Arts, Film & Media Studies.**

Ms. Kungu intends to conduct research for Ph.D. thesis entitled **"Influence of Media Convergence on Intrusion of Privacy among Internet used in Nairobi City County, Kenya"**

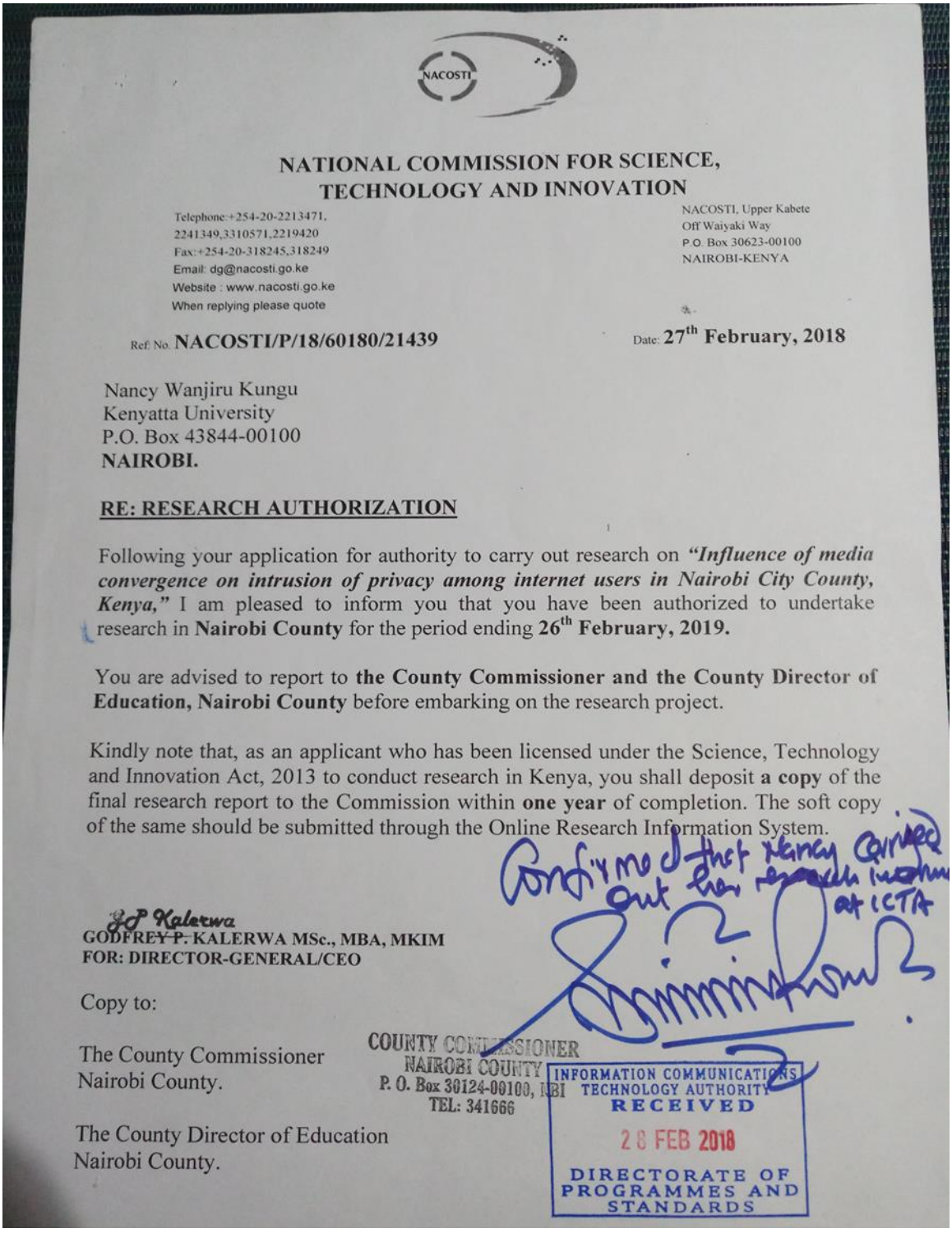
Any assistance given will be highly appreciated.

Yours faithfully,

KENYATTA UNIVERSITY
OFFICE OF DEAN
17 OCT 2017
GRADUATE SCHOOL
P.O. BOX 43844-00100 NAIROBI

MRS. LUCY N. MBAABU
FOR: DEAN, GRADUATE SCHOOL

RM/cao



NACOSTI

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone:+254-20-2213471,
2241349,3310571,2219420
Fax:+254-20-318245,318249
Email: dg@nacosti.go.ke
Website : www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref: No. **NACOSTI/P/18/60180/21439**

Date: **27th February, 2018**

Nancy Wanjiru Kungu
Kenyatta University
P.O. Box 43844-00100
NAIROBI.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"Influence of media convergence on intrusion of privacy among internet users in Nairobi City County, Kenya,"*** I am pleased to inform you that you have been authorized to undertake research in **Nairobi County** for the period ending **26th February, 2019.**

You are advised to report to **the County Commissioner and the County Director of Education, Nairobi County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

Confirmed that Nancy Carried out her research in the at ICTA

G P Kalerwa
GODFREY P. KALERWA MSc., MBA, MKIM
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The County Commissioner
Nairobi County.

COUNTY COMMISSIONER
NAIROBI COUNTY
P. O. Box 30124-00100, NBI
TEL: 341666

INFORMATION COMMUNICATIONS TECHNOLOGY AUTHORITY
RECEIVED
28 FEB 2018
DIRECTORATE OF PROGRAMMES AND STANDARDS

The County Director of Education
Nairobi County.

NACOSTI

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone:+254-20-2213471,
2241349,3310571,2219420
Fax:+254-20-318245,318249
Email: dg@nacosti.go.ke
Website : www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref. No. **NACOSTI/P/18/60180/21439**

Date: **27th February, 2018**

Nancy Wanjiru Kungu
Kenyatta University
P.O. Box 43844-00100
NAIROBI.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"Influence of media convergence on intrusion of privacy among internet users in Nairobi City County, Kenya,"*** I am pleased to inform you that you have been authorized to undertake research in **Nairobi County** for the period ending **26th February, 2019.**

You are advised to report to **the County Commissioner and the County Director of Education, Nairobi County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

Permission granted

GP Kalerwa
GODFREY P. KALERWA MSc., MBA, MKIM
FOR: DIRECTOR-GENERAL/CEO

2ND MARCH 2018

Copy to:

The County Commissioner
Nairobi County.

COUNTY COMMISSIONER
NAIROBI COUNTY
P. O. Box 30124-00100, NBI
TEL: 341666

MEDIA COUNCIL OF KENYA
P. O. Box 43132 - 00100, NAIROBI
TEL: 2725032/2737058
MOB: 0727 - 735252
info@mediacouncil.or.ke

The County Director of Education
Nairobi County.

COMMUNICATIONS AUTHORITY OF KENYA

CA/HCA/326

3rd April 2019

Nancy Kungu
PhD-Kenyatta University

0722493451

Dear Madam,

RE: AUTHORIZATION TO CONDUCT AN ACADEMIC RESEARCH

The above captioned refers.

We wish to confirm that the Authority has given an approval for your request to conduct an academic research on "influence of media convergence on intrusion of privacy of internet users in Nairobi city county, Kenya".

Please note that the information and data you intend to collect is for academic purposes only and should be treated in strict Confidence. You shall be required to provide the results of the information and data collected to the Authority upon completion of the data collection exercise.

Yours Faithfully,
Communications Authority of Kenya

P. J. Kemei (Mrs.)
For: Director/HCA

KENYATTA UNIVERSITY
GRADUATE SCHOOL

E-mail: kubps@yahoo.com
dean-graduate@ku.ac.ke
Website: www.ku.ac.ke

P.O. Box 43844, 00100
NAIROBI, KENYA
Tel. 8710901 Ext. 57530

Our Ref: M88/28111/14

Date: 3rd October, 2017

The Director General,
National Commission for Science, Technology & Innovation,
P.O. Box 30623-00100,
NAIROBI

Dear Sir/Madam,

RE: RESEARCH AUTHORIZATION FOR MS. NANCY W. KUNGU REG. NO. M88/28111/14

I write to introduce Ms. Kungu who is a Postgraduate Student of this University. She is registered for a Ph.D. degree programme in the Department of Communication & Media Studies in the School of Creative Arts, Film & Media Studies.

Ms. Kungu intends to conduct research for Ph.D. thesis entitled **"Influence of Media Convergence on Intrusion of Privacy among Internet used in Nairobi City County, Kenya"**

Any assistance given will be highly appreciated.

Yours faithfully,

MRS. LUCY N. MBAABU
FOR: DEAN, GRADUATE SCHOOL

RM/cao

KENYA METHODIST UNIVERSITY
PRINCIPAL
06 DEC 2017
Nairobi Campus
P.O. Box 45240-00100 NAIROBI

Asst. Dean of Students
for your assistance

Authority granted to engage students in the research subject to adherence to proper Ethical conduct.

6/12/17

AFRICA NAZARENE
UNIVERSITY

28th August 2018

Dear Sir /Madam,

RE: RESEARCH AUTHORIZATION FOR: MS.NANCY W.KUNGU

Ms.Kungu is a postgraduate student in Kenyatta University; she has been given permission to conduct research at our institution for her PHD thesis.

In Order to complete her program, Ms.Kungu is conducting a research entitled: "**Influence on Media Convergence on Intrusion of Privacy among Internet used in Nairobi City County, Kenya**"

Any assistance offered to her in collecting data will be highly appreciated.

Yours Faithfully,

AFRICA NAZARENE UNIVERSITY
PRINCIPAL, NAIROBI CBD CAMPUS
29 AUG 2018
Sig
P. O. - 53067 - 00200, NAIROBI

PROF.ORPHA ONGITI
PRINCIPAL NARIOBI CBD CAMPUS

MULTIMEDIA UNIVERSITY OF KENYA
P .O. BOX 15653 - 00503, NAIROBI, KENYA.
(MMU is ISO 9001:2008 Certified)

OFFICE OF THE DEPUTY VICE CHANCELLOR (AA, R&I)

REF: MMU/DVC AA R&I/RESEARCH/VOL.1

26th June, 2018

Nancy W. Kungu
Kenyatta University
P.O Box 43844
NAIROBI.

allowed.
Director CBD
9.7.18.

Director CBD
Kindly allow the bearer
to undertake Data Collection
9/7/2018

RE: REQUEST FOR COLLECTION OF DATA IN THE UNIVERSITY

Reference is made to the above subject matter pursuant to your letter dated 20th June, 2018 vide which you sought permission for data collection from the University.

We are pleased to inform you that your request has been granted and permission approved for collection of data within Multimedia University of Kenya, CBD Campus.

You are required to report to the Registrar Administration before you commence your data collection. You will be required to observe the University Rules and Regulations. Please ensure that you submit a copy of your study report to Multimedia University of Kenya.

We hope that our support will contribute to the success of your career development.

Yours faithfully,

PROF. PAUL N. MBATIA PhD.
Deputy Vice-Chancellor (AA, R&I)

C.c. Vice Chancellor
Deputy Vice Chancellor – AF&P
Reg. Administration
Chief Security Officer

MULTIMEDIA UNIVERSITY OF KENYA
MBAGATHI/ MAGADI ROAD,
P. O. Box 30305 - 00100
NAIROBI

Magadi Road, off Bomas of Kenya
P.O. Box 15653-00503, Nairobi, Kenya
Tel: +254 20 207 1391
Riding on Technology, Inspiring Innovation
Email: vc@mmu.ac.ke
website: www.mmu.ac.ke
Fax: +254 20 2071247

KENYATTA UNIVERSITY

OFFICE OF DEPUTY VICE-CHANCELLOR, RESEARCH, INNOVATION AND OUTREACH

P. O. Box 43844 - 00100
Nairobi. Kenya
Tel. 254-20-810901 Ext. 026
E-mail: dvc-rio@ku.ac.ke

Ref: KU/DVCR/RCR/VOL.3/245

Nancy Wanjiru Kungu,
School of Creative Arts, Film & Media Studies
KENYATTA UNIVERSITY

25th April, 2018

Dear Ms. Kungu,

RE: **REQUEST TO COLLECT RESEARCH DATA AT KENYATTA UNIVERSITY**

This is in reference to your letter dated 9th April, 2018 requesting for authorization to collect research data at Kenyatta University on the topic "I*Determinants Influence of Media Convergence in Intrusion of Privacy among Internet Users in Nairobi City County, Kenya"* towards a PhD degree of Kenyatta University.

I am happy to inform you that the Vice-Chancellor has approved your request to collect data. It has been noted that you wish to collect data from students aged 19 – 26.

Yours Sincerely,

Prof. F. O. Gravenir
Deputy Vice-Chancellor
Research, Innovation & Outreach
cc. Vice-Chancellor
DVC, Academic