IMPACT OF DIGITAL PROMOTIONS ON CONSUMER PRIVACY: A CASE STUDY OF UNITED STATES INTERNATIONAL UNIVERSITY - AFRICA

BY

SOPHIE SANAIEPI ODUPOY

UNITED STATES INTERNATIONAL UNIVERSITY-AFRICA

SUMMER 2017
IMPACT OF DIGITAL PROMOTIONS ON CONSUMER PRIVACY: A CASE STUDY OF UNITED STATES INTERNATIONAL UNIVERSITY - AFRICA

BY

SOPHIE SANAIEPI ODUPOY

A Research Project Report Submitted to the Chandaria School of Business in Partial Fulfillment of the Requirement for the Degree of Master of Business Administration (MBA)

UNITED STATES INTERNATIONAL UNIVERSITY-AFRICA

SUMMER 2017
STUDENT’S DECLARATION

I, the undersigned declare that this is my original work and that it has not been submitted to any other College, Institution or University other than the United States International University – Africa for academic purposes.

Signed: __________________________  Date: __________________________

Sophie Sanaipei Odupoy (ID 225796)

This project has been presented for examination with my approval as the appointed supervisor.

Signed: __________________________  Date: __________________________

Dr Kefah Njenga,

Signed: __________________________  Date: __________________________

Dean, Chandaria School of Business
COPYRIGHT

Under no circumstances will any part of this research project report be reproduced or transmitted in any form, or by any means such as electronically, by magnetic tape or mechanically, including photocopying, recording, on any information storage and retrieval system without prior authorization in writing from the author.

ABSTRACT

The general objective of the study was to determine how digital promotions infringe on consumer privacy. The study was guided by the following three specific research objectives; to determine ways in which social media marketing has affected consumer privacy, to evaluate the impact of direct internet marketing on consumer privacy and to determine the impact of mobile marketing on consumer privacy.

The research methodology, which was adopted was as follows. The study deployed a descriptive research design to explore or find out ‘how’ digital marketing has affected consumer privacy. The target population for the study comprised of United States International University – Africa (USIU-A) students of which 233 were sampled for the study. The study used stratified random sampling technique to ensure that students at every level education are given an equal chance of participation in the study. A structured questionnaire was used to collect the relevant information from the students. This study used the quantitative method of data analysis, as such both descriptive and inferential statistics were used. Microsoft Excel and Statistical Package for Social Sciences (SPSS) program version 21 were used to analyze and present the collected data.

The study established that “permitting Third-Party access of shared information” and “secondary use of shared information” were the most important privacy concern issues for respondents and that “collection of personal information” and “misuse of shared information” were the least important concerns of the respondents. The study found that “secondary use of shared data” and “intrusive marketing emails” were the most important privacy concerns for the respondents when using the internet and that “improper emails” and “cookies” were the least important. The study also found that “surveillance by marketers” and “inappropriate marketing news from mobile service providers” were the most important privacy concerns with regard to mobile marketing and that “intrusive texts messages from marketers” and “inappropriate calls from marketers” were of the least importance to respondents.

The study found that digital promotions and consumer privacy were positively associated. It found that Pearson correlation coefficient between social media marketing and consumer privacy and so was that between direct internet marketing (independent variable) and consumer privacy as well as that conducted between mobile marketing consumer privacy.
It found that the total variability of the models indicated by R Square was .050 suggesting that 5% of the variance (or change) in the model could be explained by social media marketing, direct internet marketing and mobile marketing. It established that the general equation for the consumer privacy was $= 2.428 + .132 \text{ Social Media Marketing} + .209 \text{ Direct Internet Marketing} - .142 \text{ Mobile Marketing}$.

In conclusion, the study contends that social networking sites including Foursquare, Facebook, LinkedIn, Google+ and Instagram do collect personal information with or without subscribers’ awareness. It also concludes that direct internet marketing is equally guilty of violating consumer privacy rights. That marketers have acquired consumers’ email addresses and communicated to them without their consent something which contravenes the idea of permission marketing, where marketing communication is based on consumers’ issuance of permission or consent to receive marketing information. It further concludes that the rapid advancement of mobile technologies has provided a more encompassing and powerful means of surveillance, which creates an open boundary structure with a high degree of information permeability.

The study recommends that; (i) the government of Kenya should strengthen existing laws on consumer protection (ii) The government of Kenya should enact policies to properly regulate the use of internet in Kenya (iii) The Kenyan Parliament should define new laws that address the issue of consumer privacy in mobile marketing (iv) Researchers and Academicians should conduct more research, and (v) Researchers should also study ways in which consumer privacy impacts on digital promotions.
ACKNOWLEDGEMENTS

The completion of this study would have been impossible without the material and moral support from various people. It is my obligation therefore to extend my gratitude to them. First of all, I thank the Almighty God for giving me good health, and guiding me through the entire course.

I am greatly indebted to Dr. Kefah Njeng’a who was my supervisor for his effective supervision, dedication, availability and professional advice. I extend my gratitude to my lecturers who taught me in the MBA programme, therefore enriching my research with knowledge. The Unites States International University classmates, with whom I weathered through the storms, giving each other encouragement and for their positive criticism.
TABLE OF CONTENTS

STUDENT’S DECLARATION ............................................................................................................... ii
COPYRIGHT ..................................................................................................................................... iii
ABSTRACT ....................................................................................................................................... iv
ACKNOWLEDGEMENTS .................................................................................................................. vi
LIST OF TABLES ........................................................................................................................... ix
LIST OF FIGURES .......................................................................................................................... x
LIST OF ABBREVIATIONS .............................................................................................................. xi

CHAPTER ONE .............................................................................................................................. 1

1.0 INTRODUCTION ..................................................................................................................... 1
1.1 Background of the Problem .................................................................................................... 1
1.2 Statement of the Problem ....................................................................................................... 5
1.3 General Objective .................................................................................................................. 6
1.4 Specific Objectives ................................................................................................................ 6
1.5 Significance of the Study ....................................................................................................... 6
1.6 Scope of the Study .................................................................................................................. 7
1.7 Definition of Terms ............................................................................................................... 8
1.8 Chapter Summary .................................................................................................................. 9

CHAPTER TWO ............................................................................................................................ 11

2.0 LITERATURE REVIEW ......................................................................................................... 11
2.1 Introduction .......................................................................................................................... 11
2.2 Effect of Social Media Marketing on Consumer Privacy ..................................................... 11
2.3 Impact of Direct Internet Marketing on Consumer Privacy .................................................. 16
2.4 Impact of Mobile Marketing on Consumer Privacy ............................................................... 18
2.5 Conceptual Framework ......................................................................................................... 23
2.6 Chapter Summary ................................................................................................................ 24

CHAPTER THREE ......................................................................................................................... 25

3.0 RESEARCH METHODOLOGY ................................................................................................. 25
3.1 Introduction .......................................................................................................................... 25
3.2 Research Design .................................................................................................................... 25
LIST OF TABLES

Table 3.1: Population Distribution..................................................................................................................26
Table 3.2: Sample Distribution..........................................................................................................................29
Table 4.1: Grouping of Respondents by Level of Study.....................................................................................27
Table 4.2: Frequency of Social Media Use..........................................................................................................28
Table 4.3: Grouping of Respondents by Age and Other Age-Related Facts.......................................................28
Table 4.4: Information Shared on Social Media...................................................................................................30
Table 4.5: Awareness of Use of Shared Information for Marketing.................................................................31
Table 4.6: Use of Shared Information for Target Marketing................................................................................32
Table 4.7: Marketers' Use of Personal Information Shared on Social Media....................................................33
Table 4.8: Sharing Personal Email for Receipt Marketing..................................................................................33
Table 4.9: Subscription to Newsletters for Marketing Information....................................................................36
Table 4.10: Frequency of Receipt of Marketing Information.............................................................................37
Table 4.11: Concern Sharing of Browsing History Information for Marketing................................................38
Table 4.12: Customers Personal Information Sharing by Mobile Service Providers........................................40
Table 4.13: Perception of Violation of Personal Trust by Service Providers......................................................42
Table 4.14: Appropriateness of Advertisements from Marketers' Received on Phones.....................................42
Table 4.15: Cross-tabulation of Information Shared and Awareness of Marketing Use.....................................43
Table 4.16: Cross-tabulation of Personal Information and Frequency of Marketing Email............................44
Table 4.17: Cross-tabulation of Mobile Service Sharing and Violation of Personal Trust..................44
Table 4.18: Cross-Tabulation of Mobile Service Sharing and Intrusiveness of Marketing..............................45
Table 4.19: Correlation of Consumer Privacy and Social Media Marketing....................................................45
Table 4.20: Correlation of Consumer Privacy and Direct Internet Marketing..................................................46
Table 4.21: Correlation of Consumer Privacy and Mobile (Phone) Marketing.................................................47
Table 4.22: Model Summary for Consumer Privacy..........................................................................................48
Table 4.23: ANOVA Analysis for Consumer Privacy..........................................................................................48
Table 4.24: Regression Coefficient Analysis for Consumer Privacy...............................................................48
LIST OF FIGURES

Figure 4.1: Grouping of Respondents by Gender .......................................................... 26
Figure 4.2: Frequency of Internet Use ............................................................................ 27
Figure 4.3: Most Important Consumer Privacy Concerns when Using Social Media .......... 29
Figure 4.4: Use of Information Shared in Social Media for Marketing ............................. 30
Figure 4.5: Most Important Personal Information Shared on Social Media ..................... 31
Figure 4.6: Perception about Intrusiveness of Social Media Advertisements .................... 32
Figure 4.7: Perception of Misuse of Shared Information on Social Media by Marketers .... 33
Figure 4.8: Concern on Customization of Information to Target Social Media Users ........ 34
Figure 4.9: Most Important Consumer Privacy Concerns for Internet Users .................. 35
Figure 4.10: Frequency of Receiving Marketing Information on Email .......................... 36
Figure 4.11: Perception of Intrusiveness of Internet Marketing ....................................... 36
Figure 4.12: Online Marketers Access of Internet-Users' Browsing History ..................... 37
Figure 4.13: Whether Browsers Prompted for Permission before Cookies’ Installation ....... 38
Figure 4.14: Most Important Privacy Concern Over Mobile Marketing ............................ 39
Figure 4.15: Appropriateness of Service Providers’ Sharing Customers Information ......... 41
Figure 4.16: Perception of Intrusive Marketing Messages from Service Providers .......... 42
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>Chartered Institute of Marketing</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>IMT</td>
<td>Information Management Technology</td>
</tr>
<tr>
<td>KDD</td>
<td>Knowledge Discovery in Data Bases</td>
</tr>
<tr>
<td>SNS</td>
<td>Social Network Service</td>
</tr>
</tbody>
</table>
CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Problem

In an increasingly digital world, corporations are using digital and online platforms to communicate their products and services to customers. The contemporary relationship marketing is mostly technology driven and relies almost exclusively on high-end reliable customer databases to obtain and configure information that depict customers’ need patterns and prospect population (Brown & Muchira, 2004). It follows, undoubtedly therefore, that the better the consumer information gathered, the better the company’s ability to communicate to and meet their customer’s needs.

In most instances, such digital promotions and advertisements disregard consumers’ privacy issues and laws, and increasingly, personal privacy is becoming an issue of great concern for most consumers (Al-Shakhouri & Mahmood, 2009). Kabanda, Brown, Nyamakura and Keshave (2010) observe that globally, 85% of internet users expect to see a privacy statement when browsing e-commerce websites and 66% reveal to feel more secure if they find such statements in company website. Nonetheless, firms have ignored these concerns and as Brown and Muchira (2004) observe there is a tendency for firms to misuse the consumer information and the digital platforms in a manner that leads to the violation of consumer privacy.

Globally, the conduct of corporations and organizations underscores the need for consumers to be concerned about their privacy and governments are moving in harmony to do just that. Papacharissi and Fernback (2005) observe that 27% of internet users in the United States of America (US) are concerned about online privacy violations and 54% find the tracking of personal information online, a harmful act and that 86% prefer an “opt-in” policy, which require websites to ask for permission before collecting and potentially using personal data. In the US, the Federal Trade Commission (FTC) approximates that about 85% of all websites collect the personal information of their consumers while failing to post their privacy policies, and estimates that only 14% of the corporations post their privacy policies (Al-Shakhouri & Mahmood, 2009).
In other cases, corporations have made the databases having the personal information of the consumers accessible to other firms. Still in the US, Equifax, a leading credit bureau in the country has made over 160 million customers credit records accessible to over 50,000 business (Brown & Muchira, 2004). Another survey conducted by the Business Week/Harris, found that privacy was the leading concern for internet users in the US. It proposed that a disclosure by firms of their privacy policies would result in a 78% increase in internet usage by those already using the internet and a 61% increase in internet use by non-internet users (Al-Shakhouri & Mahmood, 2009; Head & Yuan, 2001).

Another study found that 70% of American consumers were more likely to be from a firm that a third party had verified as having the greatest standards of data privacy (Conroy, Anupam, Milano & Singhal, 2014). In Canada, the need for consumer privacy protection led to the adoption in 2001 of the Personal Information Protection and Electronic Document Act (Bill C – 6) governing the collection and use of personal information.

In Europe, the General Data Protection Regulation (Directive 95/46/EC) and the ePrivacy Directive (a Directive on Privacy and Electronic communications) provide the principal legal framework for the protection of personal data (European Commission, 2017; Head & Yuan, 2001). Therefore, the issue of consumer digital privacy is accorded high importance within the European Union (EU). According to Singh and Hill (2003), companies in the EU that collect and transmit personal information are required by law to confirm the authenticity of the information gathered and to state that the information would not be used for other purposes than the ones for which it was collected.

Papacharissi and Ferback (2005) explain that these EU legal frameworks identify four critical issues that are vital to privacy. These are, (i) notice (that consumers should be notified of that kind of data being collected and intended use); (ii) consent (that the corporations and websites obtaining such data should obtain consumers informed consent); (iii) access (that users/consumers should have access to their own data upon request); and (iv) security (that the information should always be kept secure). The protection of privacy right is replicated everywhere in Europe including Germany, Denmark, Italy, United Kingdom, Switzerland, Spain, Sweden among others. However, this does not imply that there has not been violation of consumer privacy in the EU (European Commission, 2017; Papacharissi & Ferback, 2005; Head & Yuan, 2001).
Consumer privacy is also a major concern in Asia just like elsewhere in the world. In China, where it is estimated that some 420 million people are using the internet, the issue of online privacy has become a concern over the recent years (CNNIC, 2010; Wu, Lau, Atkin & Lin, 2011). China’s exponential expansion in internet use has increased made the internet less secure and raised privacy concerns among users. According to the *China Youth Daily* (cited in Wu, *et al.*, 2011), 55% of the interviewees thought that the protection of online privacy had become harder with 29.3% indicating that their personal information had been randomly released.

In Africa, the issue of online customer privacy is just beginning to take root. In fact, as internet and mobile phone usage continues to grow, privacy concern is also increasing among internet users. Kabanda, *et al.*, (2010) explain that the increasing use of internet, internet banking and mobile banking in South Africa has raised privacy concerns in the country. The country is currently the fourth (4th) largest internet user in the continent with 4.6 million internet users (InternetWorldStats.com, 2017). Schreuder and van Rensburg (2015) explain that according to a research conducted by Symantec in 2009, it was indicated that 1.6 million malicious signatures were recorded, 90% of which attempted to access confidential information from South African internet users and that phishing grew by 66% in that year.

In West Africa, Nigeria is the leading country in Africa in terms of internet usage with about 97 million internet users (InternetWorldStats.com, 2017). Nigerian constitution under articles 45 (1) (a) and (b) upholds citizens’ right to privacy in their homes, telephone communication and correspondence (Ademola, 2012). However, Adelola, Dawson and Batmaz (2015) observe that there is no privacy law concerning online communication in place making the public vulnerable to improper, uninformed and misuse of online personal information by firms. The same is the case for Ghana where there is no precise law addressing online privacy and corporations leaving the online corporations to exploit consumer information as they wish.

In North Africa, Egypt has provided an interesting case on the issue of privacy rights. In terms of internet usage, Egypt is ranked 15th (with 38.75 million internet users and a growth rate of 18.79% annually according to the country’s Ministry of Communication and Information Technology (MCIT) (2014). It by no doubt one of the leading countries if not
number one in terms of internet usage. Both the International Covenant on Civil and Political Rights (ICCPR) and the Egyptian 2014 Constitution uphold the right to privacy (Ezzart, 2014). However, despite the existence of legal basis for online privacy, both state agencies and corporations have circumvented the laws, the former in alleged pursuit of security and the latter by collecting, sharing and misusing personal data (Ezzart, 2014).

East African states and their citizens have also grappled with the issue of consumer privacy and this has led to some milestone progress amid violations of privacy rights by corporations. In Tanzania, Magala (2011) explains, the constitution is the source of privacy rights. The Tanzanian constitution was amended in 1984 to comply with international documents particularly the Universal Declaration of Human Rights (UDHR) to promote individual rights containing the right to privacy (Magala, 2011).

Kenya is East Africa’s leader in terms of internet use and mobile penetration, approximated at 31 million (68.4%) and 37.8 million (88.1%) respectively (InternetWorldStats.com, 2017; Communications Authority of Kenya, 2017). It is no doubt that, as is the case elsewhere in the world, consumer privacy has become an issue of great concern in Kenya as well. The right to privacy is enshrined in Kenya’s constitution. In the recently promulgated Constitution of Kenya, 2010, under article 31 it provides *inter alia*;

> “every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed and the privacy of their communication infringed” (Monyango, 2016, p.1)

The right to privacy was further indorsed by the Data Protection Bill of 2013 under Article 31 (c) and (d). It follows then that the collection of personal information without consent of the person, secondary use of the collected information, its monetization, storage by marketer is in violation of these rights (Schreuder & van Resenburg, 2010). Monyango (2016) notes that these laws do not expressly bar companies from collecting and using personal data. As such, it is still at the corporations’ discretion to commercialize the data such as in Targeted Online Advertising (Online Behavioral Advertising).

In such cases companies collect information on a person’s online activity such as the web pages one primarily visits and use the information to show contents and advertisements that they consider relevant to the user (Monyango, 2017). In most instances, the advertisements are invasive, inaccurate and indicate misuse of improperly collected personal information.
Some Kenyan companies have also shared personal information with other firms. For instance, Safaricom in their Terms and Conditions for the Okoa Stima Service, the company directs that in using the service the consumer gives permission to the service provider (Safaricom) to utilize, reveal and receive personal information relating to the use of the service (Monyango, 2016). Safaricom may share the personal information with Kenya Power and Lighting Company, the sole electricity provider in Kenya.

1.2 Statement of the Problem

In 2013 alone, the internet sector in Kenya was estimated to have contributed 2.9% of the country’s Gross Domestic Product (GDP) (McKinsey Global Institute, 2013). According to Privacy International (2017), 29.6 million people were using the Internet in 2015 in Kenya and 69% of the population had access to internet. About 36.1 million people had subscribed to mobile services and mobile penetration was put at around 83.9% (Privacy International, 2017). It is evident that Kenyan Internet and mobile phone sectors are growing exponentially and are robust. Web-based social media platforms such as Facebook, Twitter, Instagram, WeChat, WhatsApp, Blogs amongst others are in great use in Kenya. Privacy International (2017) notes that there were about 4 million and 700,000 Facebook and Twitter users in Kenya in 2015.

As such, marketers and business corporations are increasingly using the internet to market to consumers, create and sustain relationship with customers. This has led to concerted effort by marketers to obtain and use personal information to effectively reach consumers online. Nonetheless, the increasing use of internet by consumers and its use by marketers alike to reach more customers has raised concerns over the violation of consumers’ privacy. According to Mwencha, Muathe and Thuo (2014) consumers are increasingly concerned about how corporations and marketers obtain and use personal information. The personal information of concern includes names, telephone numbers, national identity card numbers, social, insurance and credit security numbers, employee numbers, personal of family medical information and personal or family financial information as well as other information they consider personal.

Gerlach, Widjajo and Bauxman (2015) observe that there has been a lack of studies on impact of online service-provider use of personal on consumer privacy. This study sought to conduct a survey on the impact of digital marketing on consumer privacy among USIU
students. In so doing, the study intends not only to bridge the literature gap on the subject but to add to the current literature more information on the subject matter.

1.3 General Objective
The general objective of the study was to determine how digital promotions infringe on consumer privacy;

1.4 Specific Objectives

1.4.1 To determine the ways in which social media marketing has affected consumer privacy;

1.4.2 To evaluate the impact of direct internet marketing on consumer privacy

1.4.3 To determine the impact of mobile marketing on consumer privacy;

1.5 Significance of the Study
The findings of this study will be important to a number of stakeholders in the education industry.

1.5.1 Students and Consumers
The current study intended to unearth important issues concerning consumer privacy and in so doing the study may be informative to consumers and alert them of their privacy rights especially when using smart devices such as computers, tablets and smartphones connected to the internet. Furthermore, the study may sensitize the consumers on how corporations and websites collect and utilize their personal data for marketing purposes. The study may facilitate consumer understanding and appreciation of how social media, e-mail and mobile marketing may and do infringe on their privacy rights. Therefore, the study may also sensitize the consumers on how they can help protect their privacy by exercising caution on the kind of personal information they make available online. Additionally, the study might also provide information that can help consumers whose privacy has been compromised through internet, social media or mobile marketing, on where to seek legal redress and on how to go about holding the privacy violators accountable.
1.5.2 Corporations

Corporations stand to benefit from the study by gaining an insight into the issues regarding consumer privacy. The study may therefore be of great significance to the corporation, as it might allow them to identify or recognize privacy concerns and rights of consumers, which may help them avoid costly legal procedures that could be launched against them. The study may also inform the management of organizations on the importance of stating privacy policies and on how to ensure that their promotions do not infringe on the privacy rights of their potential customers and members of the public.

1.5.3 Government of Kenya and Relevant Authorities

The study may provide information regarding the impact of digital promotions on consumer privacy; as such, it may be important to government and policymakers. It might contribute to further understanding of the effects of digital promotion on the consumers’ privacy. It may inform of the practices of marketers that violate privacy rights as well as the vulnerability of internet and mobile phone users to violation of their privacy. This may help the government to enact and implement privacy protection laws that protect the rights of consumers’ privacy some of which are enshrined in the constitution.

1.5.4 Other Researchers and Academicians

The study may be of great importance to other research and academicians in that it may contribute to the literature regarding digital privacy concerns. In addition, it may contribute to the literature review of future studies and help future researchers understand the subject matter and the underlying issues. The information the study provides may also kindle scholarly attention into the issue of privacy concerns in digital promotions.

1.6 Scope of the Study

The study examined the impact of digital promotions on consumer privacy. The study focused on how digital promotions conducted through the e-mails and through the internet on social media and other websites violate consumer privacy. The study comprised both primary and secondary research. The primary element involved the collection of primary data from a sampled number of students at United States University – Africa (USIU-A) located in Nairobi Kenya, off the Thika Superhighway. The primary data collection was
conducted over a one-week period in July 2017 using a structured questionnaire. The secondary facet involved the collection of information that exists in secondary sources.

1.7 Definition of Terms

Following are definitions and explication of some key terms and concepts that were used in the course of the study.

1.7.1 Digital Marketing

Digital marketing is similar to electronic marketing and is the management and execution of marketing through electronic media including mobile phones, emails, the web as well as the interactive TV devices in conjunction with digital data about the customer (Chaffey, 2009).

1.7.2 E-mail Marketing

Refers typically to outbound communications from a corporation to prospects or customers to encourage branding goals or purchase (Chaffey, 2009).

1.7.3 Marketing

Marketing refers to the process of recognizing and satisfying the needs of the customers with products manufactured, marketed or serviced by a company facilitating a mutual satisfaction (Nagapava, 2010).

1.7.3 Personal Information Privacy

Refers to a person’s ability or capacity to have and maintain control of all the information concerning him or her (Al-Shakhouri & Mahmood, 2009).

1.7.4 Privacy

This refers to the interests that individuals have in maintaining a personal space, free from any sort of interference by other organizations or individuals (Al-Shakhouri & Mahmood, 2009).
1.7.5 Social Media

Social media refers to internet-based interactive platforms through which people and communities can generate and share user-generated contents (Nagapavan, 2015).

1.7.6 Social Network

A social network refers to a site that allows or facilitates a peer-to-peer communication with a group or between a group of individuals by providing facilities to develop user-generated content and to exchange messages and comments between different users (Chaffey, 2009).

1.8 Chapter Summary

Chapter One has provided the introduction of the study. The chapter has provided the background of the problem contextualizing it in a global perspective before narrowing down to Kenya. The chapter has also gone ahead to state the problem for the study highlighting the problem, scholarly treatment of the issue and the need for conducting the study. The chapter has further highlighted the general objective of the study and the specific objectives, the significance of the study, the scope of the study and provided definitions of some of the key terms that were used in the study.

Chapter Two reviews existing literature on the impact of digital marketing on consumer privacy. The area of focus of the chapter is the assessment of the effects of social media marketing on consumer privacy, the impact of e-mail marketing on consumer privacy and the impact of mobile marketing on consumer privacy. The aim of Chapter Two is to provide an understanding of the research topic and to examine and present previous findings regarding the three specific research objectives.

Chapter Three discusses the research methodology for the study. The chapter highlights and describes the research design that the researcher utilized in the study, and also identifies, and describes the population of the study. The chapter further defines and explain the sampling design for the study and determine the sample size of the study. It further explains the data collection instrument for the study, research procedure and the data analysis methods used.
Chapter Four has presented the result and findings of the study using a variety of descriptive statistics including bar graphs, pie-charts and frequency tables. The chapter presents the findings regarding every question that the respondents were asked in the data collection instrument. The chapter also uses inferential statistics including cross-tabulations, correlation, analysis or variance (ANOVA) and regression to make inferences and further interpret the findings.

Chapter Five provides the summary of the study and the major findings of the study. The Chapter also details and discusses the major findings of the study in line with the three research objectives of the study. The chapter then provides the conclusion and the recommendations. Recommendations are provided both for improvement and for future research.
CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter reviews existing literature on the impact of digital marketing on consumer privacy. The area of focus of the chapter is the assessment of the effects of social media marketing on consumer privacy, the impact of e-mail marketing on consumer privacy and the impact of mobile marketing on consumer privacy. The review takes a two-pronged approach, it seeks to establish an understanding of the impact of digital marketing on consumer privacy, it also seeks to assess previous findings to determine if there is consensus among scholars on the effects of digital marketing on consumer privacy. The majority of the literature reviewed were academic material on the subject matter, published within the last decade and comprised mostly of books, press releases by organizations and peer reviewed journal articles.

2.2 Effect of Social Media Marketing on Consumer Privacy

2.2.1 Collection of Personal Data

Rogers (2017) observes that in recent years, there has been a crackdown by the Information Commissioner's Office (ICO) regarding corporations' use of personal data in their promotional communication. McFarland (2012) observes that firms collect personal data such as insurance and medical records, credit records, compensation claims and histories of consumers without informing the consumers. Such information is shared on with social networking sites proving a blatant violation of consumer privacy.

Social networking sites including Foursquare, Facebook, LinkedIn, Google + and Instagram do collect personal information with or without subscribers’ awareness (Gan & Jenkins, 2015). It is estimated that Twitter and Facebook currently have about 645.7 million and 1.86 billion subscribers respectively (Statistic Brain Research Institute, 2017; Zephoria Digital Marketing, 2017). This exponential use of social media makes it a platform through which the providers and other people or organizations can obtain a lot of personal information.
Changi (2006) observes that the rapid growth of information technology has resulted in an increase in internet use and that firms are now able to gather, retain and share consumer data, which can be used to conduct a more targeted marketing. Dholakia and Dholakia (2016) contend that firms such as internet-based companies including Amazon, Facebook, Google and Netflix collect colossal amounts of personal data as part of their business operations. However, most of the users of these sites are unaware that their personal data is being collected (Dholakia & Dholakia, 2016; Gan & Jenkins, 2015). According to Gan and Jenkins (2015) Twitter and Facebook users are often unaware of the perils connected with signing up to social media platforms, uploading a picture on Facebook, updating status, enabling the geo-location for tagging amongst other activities.

The fact that social media sites collect personal information on that scale often without the knowledge of the subscribers is in contravention of consumer rights (Nagapavan, 2010). The personal data collected by social media sites includes names, telephone numbers, national identity card numbers, social, insurance and credit security numbers, employee numbers, personal or family medical information and personal or family financial information, making it a treasure trove for marketers. Ghosh (2016) established that despite the fact that 71% of consumers are apprehensive of sharing information about their location, 20% of marketers gather this information anyway and that both social media companies and tech firms were publishing information regarding consumers’ location despite the existing privacy concerns over the same.

Empirical evidence exists that personal data obtained by the Social Network Service (SNS) providers have been used for marketing purposes. For instance, such information has been used, often without the subscribers’ knowledge in segmented marketing. In this case, the marketers segment the subscribers using the information they provide into social, demographic or economic categories and then serve targeted advertisements to groups of users (Spineli, 2010).

The users are placed into a group or a segment according to the information they provider then the SNS, acting as a broker provides the advertisements to them or marketing firms and marketers get access to subscribers’ personal information and advertise to the subscribers by themselves. According to Campaign (2016) a recent study revealed that 71% of consumers abhor sharing their location and yet marketing firms collect and share this
information. In fact, the same study revealed that 20% of marketers collect information about consumers’ location.

Spinelli (2010) contends that Facebook and MySpace often divulge or disclose personal profiles, videos, pictures and the ability to send messages to family, acquaintances, family and co-workers. This implies that the users are not always given the choice to say how the data that they provide is going to be used by the SNS especially with regards to marketing and promotions. In other words, marketers and SNS’s are often involved in the unauthorized collection of personal data.

2.2.2 Misuse of Shared Information

Spinelli (2010) and Gerlach, et al., (2015) observe that it is currently impossible for consumers or internet users to use the internet without disclosing some personal information. However, consumers are becoming concerned about how the data they provide is used even more that the content of the personal information they give out (Ademola, 2012). Research has established that marketers acquire and misuse personal information from and in social media sites. Ghosh (2016) found that up to 92% of the consumers are unaware of how social media firms and marketers use the personal data that they collect from them. A third of the consumers are also unaware as to where their personal data collected by the social media sites are used (Ghosh, 2016).

Chartered Institute of Marketing (CIM) (cited in Campaign, 2016) conducted a study involving some 25,000 consumers and marketing gurus and found that 9 in 10 consumers had zero idea of how social media sites use their information. Ghosh (2016) observes that there is a perturbing absence of transparency regarding brands scooping up, sharing and utilization of consumer information. The study also found that 51% of consumers indicated that they had received communication on social media from companies that they believed had misused their personal information with 17% of the surveyed indicating that “it happens a lot” (Campaign, 2016). Gerlach, et al., (2015) observes that the information that users of SNS provide is often misused by the providers and marketers. The CIM research established that 92% of the consumers have no idea how organizations and websites used their personal data. The same study further revealed that 81% of the marketers who were surveyed revealed that their firms shared consumer information through departments
without consulting consumers (Campaign, 2016). Ghosh (2016) found that about 81% of the marketers studied indicated that their firms shared data across departments and offices without obtaining explicit authorization from their consumers.

Gan and Jenkins (2015) contend that SNS’s disclose collected or acquired personal data to third parties especially marketers. Changi (2007) explains that in a study conducted to assess user perceptions about the use of information that they provide online, it was determined that up to 45% of those surveyed indicated that they worried about how companies used such information. Ghosh (2016) found that about 50% of the consumers are convinced that firms have misused their personal information for marketing and that 70% of consumers do not hold a positive perception about sharing personal information, believing that it does to add value to them. Other studies including that conducted by CIM revealed that if procedures aimed at protecting consumers’ personal information were strengthened, consumer trust in disclosing personal information would improve remarkably (Al-Shakhouri & Mahmood, 2009; Campaign, 2016).

Further complicating issues for consumer privacy is the lack of understanding of data protection laws by marketers. Ghosh (2016) found that about less than half of marketers who were surveyed understood that the applicable laws concerning data protection with a just a third of the surveyed firms indicating that they were transparent on how they collected the data. The illegal acquisition of personal data from consumers and the willingness to distribute such information is problematic as the study by Ghosh (2016) found that about 68% of the surveyed marketers were themselves reluctant in sharing their own data, knowing that such data would be used.

2.2.3 Data Mining

Marketers appetite for personal information is big and they employ techniques to interpret the personal information that they obtain (McForland, 2012). This practice of inferring information is conceived as data mining. According to Singh and Swaroop (2013) data mining, also known as Knowledge Discovery in Data Bases (KDD) refers to the nontrivial extraction or abstraction of implicit hitherto unfamiliar and potentially important information from data in databases. Betancourt (2010) explains that data mining is the transformation of raw data by firms into useful information for marketing purposes.
The process involves the use of sophisticated software to look for patterns in the raw data to help businesses to have a deeper understanding of their customers and to establish more effective marketing strategies (Betancourt, 2010). Betancourt (2010) contends that firms are mining social web to create dossiers on consumers. She contends that information that is publicly posted on social media sites and blogs as well as forums are fair game. McForland (2012) observes that without the knowledge of consumers, SNS’s and marketers obtain personal information provided by users of SNS sites and employ the use of sophisticated technologies and techniques as well as psychological models to infer sensitive personal information and make presumptions on consumer behavior including purchasing habits and trends. However, data mining is not only used by marketers, according to Singh and Swaroop (2013) the practice is also vital for internet security experts who use the information to detect intrusion. Its use in digital marketing especially in social media marketing has grown exponentially and at the peril of consumer privacy concerns.

Studies have found that marketers employ data mining to combine personal information they obtain with their marketing experience to attempt engaging and influencing consumer behavior including their purchasing patterns, social class, age, ethnicity, gender among others. Marketers, SNS sites and marketing companies obtain a spectrum of personal information including the more personal information such as health records, amount assets owned, shopping habits, and family situations from social media platforms such as Foursquare, Facebook, LinkedIn, Google + and Instagram (Gan & Jenkins, 2015). They can then segment people into groups and customize their advertisements to each group in what is termed as target marketing.

Singh and Swaroop (2013) contend that through data mining marketers can infer consumers likes and dislikes based on their age, gender, shopping habits and other characteristics and trick consumers into adopting certain purchasing behavior that they would otherwise not have made. Dholakia and Dholakia (2016) note that most internet-based companies including Amazon, Facebook, Google and Netflix have applied data mining techniques. Betancourt (2010) observes that Rapleaf Inc. mined social data of over 389 million consumers on social media where such information is publicly accessible. Rapleaf Inc. then sells such mined personal data mined from social networking sites to several firms including retailers, car companies, hotels, politicians, airlines, non-profits and banks.
2.3 Impact of Direct Internet Marketing on Consumer Privacy

2.3.1 SPAM

According to Grondcolas, Rettie and Payne (2007) email marketing has become one of the most cost effective online marketing tools. The *eMarketer* (2009) approximates that about 61% of all medium and large corporations in the US engage in email marketing regularly. It has been determined that email marketing is important for marketers because it has the ability to allow for real-time interaction and relationship building with customers. Peppers and Rodgers (2008) conducted a study concerning the importance of email marketing and concluded that due to associated low costs and high response rates, email was an invaluable tool for marketers.

However, the use of email has serious consequences for consumers in terms of their privacy rights. Research has established frustrating aspects of email marketing for consumer privacy. According to Grondcolas, *et al.*, (2007) marketers have acquired consumers email addresses and communicated to them without consumers’ consent. This is in contravention of permission marketing. Coined by Godin (1999), permission marketing implies a marketing approach that is based on consumers’ issuance of permission or consent to receive marketing information. Such permission means that marketing information is anticipated, relevant and personal to consumers rather than being irrelevant and intrusive (*eMarketer*, 2009).

Currently, collection of personal information online, often without consumers’ consent has enabled marketers to acquire consumers’ emails without their consent. Through further data mining marketers have tailored advertisements based on the inferences about consumers and often send emails to individuals. Research has established that these communications are often intrusive and irrelevant having been based on inconclusive information about the consumer (Gan & Jenkins, 2015). According to a survey by the Information Management and Technology (IMT) Strategies (cited in Grondcolas, *et al.*, 2007), it was found that permission emails were highly responded to by consumers than non-permission emails.

The fact that several web-based firms including social media have the tendency to share personal information with marketers for a profit or to use the information themselves; the issue of improper marketing emails is a major concern for consumers (Dholakia and
Dholakia, 2016). In a study conducted by Grondcolas, et al., (2007) to assess internet users’ perception of email marketing, it was found than more than half of the surveyed found email advertisements and promotions intrusive. It is apparent that marketers have acquired and used personal emails of consumers to promote and advertise their products and services online through emails without obtaining the permission of the consumers in the first place.

2.3.2 Secondary Use of Personal Data

Research has established that internet-based companies and e-marketers are acquiring personal information and using them without obtaining consent of the consumers. Spinelli (2010) and Gerlach, et al., (2015) have observed that online site and SNS require consumers to provide personal information sometimes without stating the reason as to why they need the information. For instance, Grondcolas, et al., (2007) notes that Facebook requires subscribers to provide real dates of birth when subscribing to the platform without giving a good reason for this. Nevertheless, more important is the secondary use of such information that is the issue of privacy concern for consumers. Ghosh (2016) and McFarland (2012) have argued that firms collect the personal information which they then use for secondary purposes without explicit permission from the consumers. Such secondary use include the sale of such information as addresses, names, email addresses, phone numbers, type of car owned, shopping habits, age, family situation, gender and Net ID among others.

Through data mining, marketer and web-based firms are able to gather and make inferences on the collected data. Such information is not only used for marketing purposes by the collecting site or marketers but can also be shared across departments and firms (Child & Petronia, 2009). Zephoria Digital Marketing (2017) found that SNS’s can either directly advertise prospects and consumers on behalf of companies using the personal information gathered or they can provide the information to marketing firms that use it for secondary reasons. Hann, Hui and Lee (2002) contend that privacy concerns with respect to marketing have been found to depend principally on target disclosures and perceived relevancy of use of the gathered information. Secondary use therefore also includes providing improper access to third parties.
McFarland (2012) contends that online marketers employ psychological models and sophisticated techniques of statistical analysis to predict consumers purchasing behavior and preferences and to determine the factors that have a strong influence on consumers choices and loyalty. Ghosh (2016) argues that the marketers combine the intelligence they obtain through data mining with detailed dossier on subgroups and specific individuals in an attempt to engage them and shape their purchasing behavior. These secondary activities and analyses that marketers perform on consumers personal information are in violation of consumer rights.

2.3.3 Big Data Surveillance

Ball (2016) explains that Big Data can be perceived as fundamentally incrementally new strategy which the boundaries or line of distinction between the divergent sources of data is are broken. Such data collected from diversely sourced information using sophisticated algorithms to shape and inform opinions of consumers, marketers and firms (European Data Protection Surveyor, 2015). Big Data relies on two things; one, the ability of sophisticated technological algorithms to augment data collection and storage; two, the ability of technology to analyze or examine, understand, interpret and explore the full advantage of the generated information.

The goal of creating Big Data for marketers is to aid the making of informed marketing decisions, decisions which bear close semblance to what targeted consumers would like to hear. Protection of consumers rights and privileges as relates to marketing online is therefore not a major consideration for firms and marketers when it comes to the generation of Big Data (Urban & Hauser, 2004). As such, Big Data allows the combination of information from various information sources including the social domains and this is in outright violation of consumer privacy. Ball (2016) explain that Big Data presents a shift from profiling or segmenting abstraction of consumer characteristics into segments or groups to the utilization of persistently adjusted quantitative models to forecast human behavior at the personal level.

The growth and spread of the web or the internet has left in its wake, a colossal amount of information being posted by and about consumers online on such platforms as blogs, forums and social media site as well as product reviews (Urban & Hauser, 2004). Netzer,
Feldman, Goldernberg and Fresko (2012) observe that Web 2.0 has the ability to gather places for internet users on websites, blogs, chart rooms and forums. These places and cites leave footprint in the form of huge amounts of data concerning consumers’ beliefs, thoughts, experiences as well as interactions. Urban and Hauser (2004) contends that as opposed to being mined by marketers, some of this information are considered consumer-generated meaning that customers and internet browsers sometimes leave information that marketers can interpret and use.

Netzer, et al., (2012) contend that cyberspaces including product review websites, chat rooms, blogs, social media and brand sites request and inspire consumers to post their reviews and views, which act as important sources of marketing information. As the level of information about customers have grown exponentially in these sites so has Big Data which continues to act as a significant source of consumer information for marketers (Netzer, et al. 2012). Feldman and Sanger (2006) contend that Big Data has allowed firms and marketers to syndicate or organize and meta-analyze consumers personal data through the wealth of information that consumers post online.

Furthermore, Netzer, et al. (2012) observes that through Big Data marketers are able to analyze an infinite information about customers preferences, purchase behaviors and individual's characteristics and to identify patterns or irregularities among customers. Netzer, et al. (2012), Feldman and Sanger (2006) observes that consumers unknowingly and voluntarily surrender information, some of which are personal information on websites, forums and blogs. Such information opens a window to the semantic and associative networks, depicted in description of and co-occurrences of brands in the reviews or comments.

However, it must be noted that the information process though Big Data is not entirely personal data. Other information that Big Data generates include; sales volume over time, profit and stock turnover as well as inventory among others (European Data Protection Surveyor, 2015). Despite this though, the value of Big Data for marketers and organizations lies in its ability to monitor human behavior and generate value informations for marketing purposes. In most instances, consumers themselves are unaware of the aggregation of their personal information by marketers and organizations alike (European Data Protection Surveyor, 2015; McFarland, 2012; Nagapavan, 2010).
2.4 Impact of Mobile Marketing on Consumer Privacy

2.4.1 Perceived Surveillance

Ball (2016) observes that as marketing is a data-sensitive undertaking, marketers have persistently endeavored to utilize data concerning customers, their behaviors and characteristics to allow them to enhance offering to customers and repeat purchase or customer loyalty (Pridmore & Zwick, 2011). Consequently, marketers have come up with various means of surveillance marketing including direct marketing accentuating persistent direct contact with the firms existing customers, database marketing and one-to-one marketing (Ball, 2016).

Malhotra, Kim and Agarwal (2004) suggest that the practice of data collection, whether legitimate or illegitimate, “is the starting point of various information privacy concerns (p.338).” Reflecting on the origin of privacy concerns, collection refers to individuals’ concerns about the amount of personal information demanded by others (Malhotra, et al. 2004). The act of data collection triggers the coordination of permeability rules which refer to the parameters for how much others should know about the private information within the co-owned privacy boundary (Child & Petronio, 2009).

Typically, when individuals are provided with a significant amount of control over information disclosure, they create boundary structures that reduce the amount of information collection by others or they establish boundaries with low permeability (Child & Petronio, 2009). However, the rapid advancement of mobile technologies has provided a more encompassing and powerful means of surveillance, which creates an open boundary structure with a high degree of information permeability. Increasingly, the aggressive data collection activities by mobile applications (apps) and operating systems induce the perception of intensive data logging, as well as the impression that vendors are constantly monitoring user behavior through smartphones.

Because smartphones contain various functions such as web browsers, emails, photo albums, games, calendars, and contact lists, apps can collect far more personally invasive data than was previously conceivable in conventional use of personal computers, e.g., identity, upcoming schedule, time spent on different apps, contact lists, real-time location, etc. Solove (2006) has defined surveillance as “the watching, listening to, or recording of
an individual’s activities (p.490).” In today’s mobile environment, vendors take advantage of the powerful surveillance technologies to track and profile mobile consumers. Mobile users may resist mobile apps for the fear that their activities may be watched, recorded, and transmitted to various entities.

According to Ball (2016) mobile marketers have also integrated surveillance marketing into customer-relationship management (CRM) and improved call centers through which customer information are gathered and exploited for marketing reasons. In CRM, there is a routine process of data mining and creation of consumer profiles to identify patterns in consumers' purchasing behavior and brand preferences. Netzer, et al. (2012) have noted what they call text mining by marketers. They equate text mining to knowledge discovery and explain that it is a process by which marketers and mobile phone service providers extract useful and non-trivial information from unstructured customer texts.

Feldman and Sanger (2006) argue that the ease of access of digitized data from various online and electronic sources including mobile phones has created an opportunity for marketers and businesses alike to explore opportunities presented by text mining. Netzer, et al. (2012) argue that the information provided by consumers voluntarily or unknowingly on through texts and phone calls to the service providers provide and insight into the customers' associative networks as conjured by their complaints and comments.

2.4.2 Perceived Intrusion

According to Child and Petronio (2009), “rules governing ownership are easily observed when they are violated,” and “when the individuals involved discover they must change or readjust their privacy rules to guard against unwelcome intrusions (p.2081).” In other words, data subjects’ perceptions of intrusion would be triggered when data recipients are able to make independent decisions about their personal information. The notion of intrusion has often been connected to the concept of personal space (Solove 2006).

If some consumers are not yet fully conscious of all the traces they leave on the on their texts and calls, most are discouraged about cookies and other techniques mobile service provider and marketers have developed and installed in their phones which recording their actions, phone conversation even the places they visit (Netzer, et al.2012) "Find my phone"
is just one of the many applications that exists which marketers not only use to surveil consumers but which actually violate their privacy.

In today’s mobile environment, due to the powerful technological surveillance means to track and profile a mobile user, the notion of personal space has expanded to incorporate realms of both physical and informational space. Solove (2006) defines intrusion as “invasive acts that disturb one’s tranquility or solitude” (p.491) and “involves the unwanted general incursion of another’s presence or activities” (p.555). It has been argued that intrusion interrupts the victim’s activities or routines, destroys his or her solitude, and often makes the victim feel uncomfortable (Solove 2006). Malware is an especially growing problem for smartphones (Dignan 2011). A plethora of data is accessible by malware developers, including browser history, usage patterns of apps, keyboard keystroke cache, phone numbers, contacts, current and past geographic location, etc.

As it is highly possible to have malware even from mobile app stores (Dignan 2011), users may resist mobile apps for the fear that the malicious apps may interrupt their activities through the unwanted presence. The major point that emerges is that intrusion can create discomfort and harm and therefore, the flow of personal information across boundaries requires users’ efforts to restore their comfort levels. Technology has permitted companies to explore immensely improved and exciting new applications such as data mining, data warehousing, target marketing, and self-service.

The mobile phone has heightened a diversity of consumer concerns about privacy (Dignan 2011; Child & Petronio, 2010). Particularly, consumer apprehension and trepidations include the explosion of databases among mobile service providers, the enormous volume of personal data that is being collected, and the possibility of privacy violations and loss of control in the process of collecting, accessing, and utilizing this information (European Data Protection Surveyor, 2015).

Faced with these concerns, consumers sometimes undertake actions such as supplying false or fictitious information to a web site, setting up their computers to reject cookies, or refusing to purchase from particular web sites (Dignan 2011; Child & Petronio, 2010). These potentially negative reactions that arise from threats to consumer privacy would eventually have a significant impact on a firm’s marketing performance (European Data Protection Surveyor, 2015; Dignan 2011; Child & Petronio, 2010).
2.4.3 Secondary Use of Information

In several instances, consumers may voluntarily issue their personal information to mobile service providers. Such information may issue when activating SIM, or subscribing to other services (Dignan 2011). More often than not, subscribers are unaware of the potential use of their personal information for purposes not originally intended (Culnan & Williams 2009). Moreover, the service providers do not prompt the consumers or their customers about their intention to use the services for purposes for which the information was not collected for. This is a violation of consumer privacy rights (European Data Protection Surveyor, 2015).

Just like in social media marketing and direct internet marketing, mobile marketing also raises concerns over secondary use of information. According to Smith, Milberg and Burke, (1996), secondary use of personal information refers to the situations where information is collected from individuals for one purpose but is used for another (for instance, profiling individuals and sending marketing messages), without authorization from the individuals (Dignan 2011; Child & Petronio, 2010).

The activity of secondary use of information by an organization, can “potentially threaten an individual’s ability to maintain a condition of limited access to his/her personal information, harm individuals, and subsequently threaten the organization’s legitimacy in its interactions with consumers, shareholders, and regulators (Culnan & Williams 2009). The practice of secondary use of personal information triggers the coordination of linkage rules which refer to “the establishment of mutually agreed-upon privacy rules used to choose others who may be privy to the collectively held information (Jin, 2012, p.70).”

In CPM, establishing a linkage means data access is granted to another entity to become a co-owner of private information. Users’ privacy concerns over secondary use of information would be triggered when a new linkage occurs without users’ (for example, data subjects) awareness or consent. The linkage coordination rules are often considered breached if the vendor reveals the gathered personal information to unauthorized entities, or if the vendor uses personal information for secondary purposes without consumers’ awareness and consent (Culnan & Williams 2009). According to Solove (2006, p.520), “the potential for secondary use generates fear and uncertainty over how one’s information will be used in the future, creating a sense of powerlessness and vulnerability.
2.5 Conceptual Framework

![Conceptual Framework Diagram]

**Independent Variables**
- Social media marketing
- Direct internet marketing
- Mobile marketing

**Intermediate Variables**
- Internet/mobile use
- Subscriptions to marketing news
- Perception of digital marketing
- Perception of online security

**Outcome/dependent variables**
- Collection of personal data
- Improper use of shared information
- Data mining
- Secondary use of personal data
- Intrusion of privacy
- Surveillance
- Sending SPAM & Cookies

Figure 2.2 Conceptual Framework

2.6 Chapter Summary

The chapter has reviewed the literature on the research problem. The chapter has focused on literature relating to three areas of interest. The reviewed literature is that relating to the effects of social media marketing on consumer privacy, impact of direct online marketing on consumer privacy and the impact of mobile marketing on consumer privacy. The review has revealed that there has been limited research on the issue and that studies that exist do not directly address the problem. However, an assessment of the literature has revealed that digital promotions do influence consumer privacy in different ways. This research attempts to bridge the literature gap by conducting a study on the subject matter. It seeks to provide information that will also help kindle scholarly interest on the subject. The next chapter, which is Chapter Three, provides the research methodology for the study.
CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

Chapter Three presents the research methodology for the study. The chapter details or describes the research design that the researcher utilized in the study, and also identifies, and describes the population of the study. The chapter further defines and explains the sampling design for the study and determine the sample size of the study. Chapter Three further explains the data collection instrument for the study, research procedure and the data analysis methods used.

3.2 Research Design

Blanche, Durrheim and Painter (2006) describe a research design as the all-encompassing strategy adopted or used by the researcher to integrate a spectrum of research attributes, which are both coherent and logical. By designing the research, the researcher guarantees or ascertains that the problem or issue the study sets out to investigate is addressed effectively and in a manner than generates reliable and valid results. Consequently, and as Bless, Higson-Smith and Kagee (2006) explain a research design can be perceived as the blueprint of the study highlighting the data collection method, the scrutiny and measurement of the data. Saunders and Thornhill (2012) proposes that by all means the research design, which a researcher settles on should be contingent upon or depend on the research problem that the researcher sets out to investigate. It follows then that the research problem defines the research design to be used to operationalize or investigate it. Without a relationship between the research problem under investigation and the research design chosen, the study would generate senseless results (Bless, Higson-Smith & Kagee, 2006).

This study deployed a descriptive research design. This design permits to identify and explicate the nature of relations between events, phenomenon and variables (Blanche, et al., 2006). Additionally, a descriptive design facilitates the determination of a "how" an event, phenomenon or variable affects other events and variables. According to several scholars including Babbie (2010) explains that the purpose of a descriptive design is to allow to researcher to describe what was observed. Consequently, a descriptive research
design was essential in this study as it provided the platform of how the researcher assessed how digital promotions has affected privacy rights of consumers.

3.3 Population and Sampling Design

3.3.1 Population

The larger pool of people, items, events or phenomena from which the researcher draws the individuals, elements, and cases for sampling is the population (Bartlett, et al., 2001; Blanche, et al., 2006 & Bless, et al., 2006). It is also upon the population that the research extrapolates the results of the research. Nevertheless, Bartlett, Kotrilk and Higgins (2001) instruct that such a population should be homogeneous, that is, it must exhibit and possess the information of interests to the researcher. The research is valid if the findings it generates close links to the opinions, features and characteristic of the population (Bartlett, et al., 2001).

This study focused on USIU students pursuing varying degrees who were using the internet and smartphone technologies at the time of the study. The population of USIU students as of May 2017 was 6,953. The target population for the study comprised of students across all academic levels of study pursuing degrees in Business Administration (BA) who are about 1,712. The choice for BA students was based on two reasons; one, as a single cluster, they make up 32.49% of the entire population of students hence they form a representative unit for the rest the students. Secondly, given their predisposition with issues in business they are more competent in answering questions regarding digital advertising. Table 3.1 shows a breakdown of BA students in terms of academic levels.

Table 3.1 Population Distribution

<table>
<thead>
<tr>
<th>Academic Levels</th>
<th>Number of Students</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Undergraduates</td>
<td>1,128</td>
<td>65.89%</td>
</tr>
<tr>
<td>2. Graduates</td>
<td>547</td>
<td>31.95%</td>
</tr>
<tr>
<td>3. Post-graduates</td>
<td>37</td>
<td>2.16%</td>
</tr>
<tr>
<td>Total</td>
<td>1,712</td>
<td>100%</td>
</tr>
</tbody>
</table>

3.3.2 Sampling Design

To obtain germane sample for consideration and inclusion in the research, a significant number of individuals are selected from the population. Saunders and Thornhill (2012) explain that it is normally from this population that a researcher collects and infers information. It follows therefore that the validity of the study results is contingent on the suitability of the sampling design (Blanche, et al., 2006). The sampling design comprises of the sampling frame, the sampling technique and the sample size.

3.3.2.1 Sampling Frame

A register or a list of individuals, cases and events from which the researcher obtains the sample is the sampling frame (Blanche, et al., 2006). Robson (2002) clarifies more that the sampling frame denotes to the source of the appropriate or correct population from which the survey sample is drawn.

The researcher obtained a list of students currently enrolled in USIU from the Registrar’s office located at the new student’s center building within the campus. The list provided the sampling frame for the study. The sample distribution was categorized as indicated in Table 3.2. The percentages representing the number of students are depicted to two decimal places for accuracy as the numbers are not absolute. The categorization was deemed vital as it allowed the researcher to collect information from students from all levels and years of study.

3.3.2.2 Sampling Technique

Robinson (2002) explains that the study objectives determine the methodology for deriving sample for inclusion in the study. Blanche, et al., (2006) adds further that the sampling process is not abstract but is guided by the scope and parameters of the study as well as the population and the objectives of the study. The current study used a stratified random sampling design. According to Babbie (2010) a stratified random sampling is a technique where units are randomly sampled from a population that has been divided into categories (strata). For this study, the stratification was done according to students' academic levels of study and included undergraduates, graduates and post-graduates at United States International University – Africa (USIU).
3.3.2.3 Sample Size

The sample size refers to the proportion of individuals that are chosen to participate in the study (Saunders & Thornhill, 2012). They comprise of the people that bear close characteristics with the population but which the researcher can access within the time and resource constraints. An appropriate sample size is obtained by applying a statistical formula recommended by Mugenda (2003):

The population of BA students was one thousand, seven hundred and twelve students. Mugenda (1999) propose that if the sample size of a population of less than 10,000 individuals can be given by the following formula:

i. Sample Size Calculation

Sample Size = \( \frac{\text{distribution of 50\%}}{\left(\frac{\text{margin of error\%}}{\text{Confidence Level Score}}\right)^2} \)

ii. Finite Population Correction

Correct Sample = \( \frac{\text{Sample size} \times \text{Population}}{\text{Sample Size} + \text{Population} - 1} \)

Where;
Margin of error = 0.05, Confidence level = 1.645 (measured at 90%)

Therefore:

Sample size = \( \frac{(0.5 \times (1 - 0.5))}{(0.05/1645)^2} \)

= 0.25/0.00092386...

= 270.6038

True sample

True Sample = 270.6038\*1712/ 270.6038 + 1712 – 1

= 463273.7056/1981.6038

= 233

The sample size for the study was thus 233 students.
Table 3.2: Sample Distribution

<table>
<thead>
<tr>
<th>Academic Levels</th>
<th>Number of Students</th>
<th>Sample Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Undergraduates</td>
<td>1,128 (65.89% of 1,712)</td>
<td>154</td>
</tr>
<tr>
<td>2. Graduates</td>
<td>547 (31.95% of 1,712)</td>
<td>74</td>
</tr>
<tr>
<td>3. Post-graduates</td>
<td>37 (2.16% of 1,712)</td>
<td>5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1,712</strong></td>
<td><strong>233</strong></td>
</tr>
</tbody>
</table>


3.4 Data Collection Methods

Blanche, *et al.*, (2006) and Bless, *et al.*, (2006) explain that data collection is the technique or strategy for obtaining or aggregating the information from the respondents. Data collection implies the method that the researcher uses whether it is the use of questionnaires, interview schedules, face-to-face interviews or telephone interviews or whether it is participation and observation (Thornhill & Saunders, 2000). This study collected categorical data concerning age, gender, academic level among others.

The researcher used structured questionnaires in which a combination of Likert scale questions was used to obtain data from the respondents. The questionnaire was categorized into four key parts. The first part of the questionnaire comprised of questions aimed at collected categorical data concerning respondents age, gender, academic level, internet and social media use. The second part of the questionnaire comprised on questions aimed at collecting categorical data regarding the effect of social media marketing on consumer privacy. The third part of the questionnaire comprised of the questions aimed at collecting information regarding the impact of direct internet marketing on consumer privacy while the fourth and last part of the questionnaire consisted of questions aimed at collecting categorical data on the impact of mobile marketing on consumer privacy. In total, the questionnaire comprised of 30 questions and each respondent took about 20 to 30 minutes to respond to all the questions in the item. The researcher asked short and precise to questions to prevent respondent fatigue and to ensure proper understanding.
3.5 Research Procedures

According to Bless, et al., (2006) research procedures are the processes and activities that the researcher undertakes when collecting data. The researcher performed the following set of the activities in the study. After developing the questionnaire, the researcher obtained a formal approval letter from USIU research office to present to USIU students amongst whom the study was conducted. After obtaining authorization for the study, the researcher first conducted a pilot study or a pre-test of the questionnaire and the feasibility of the study then adopted the questionnaire and the activities accordingly to ensure success of the data collection process.

The researcher corrected emerging concerns from the pilot study such as the typological errors and re-worded some questions to enhance respondent understanding. The researcher then proceeded to conduct the study and employed the use of research assistants to facilitate the process. During the data collection exercise, the research assistants presented the potential respondents the questionnaires to fill in their responses. The entire data collection process was done in a period not exceeding one week. A one-week duration for data collection was appropriate to ensure that the data collection was not rushed too much whilst also ensuring that the data collection does not drag on for an unnecessarily longer period.

The response rate of the study was 92.7% (having issued out 233 questionnaires to the respondents and receiving 216 fully and correctly filled-in questionnaires).

3.6 Data Analysis Methods

This study used the quantitative method of data analysis. To ensure easy analysis, the questionnaires were coded accordingly. The quantitative analysis comprised of both descriptive and inferential analyses. The data was presented using frequency tables, bar graphs and pie charts. Further associations between the variable was conducted by use of Statistical Package for Social Sciences (SPSS) program version 21, through which Cross-Tabulations, Correlations, regression and Analysis of Variance (ANOVA) was conducted among relevant variables to permit further interpretation of the data.

3.7 Chapter Summary

Chapter Three has outlined the methodology for the study. The chapter has identified and described the research design for the study as exploratory research design. It has noted that
this design facilitated the answering of the three research questions. The chapter has also defined the population for the study and identified the sampling design that was used in the study; the sampling design was stratified random sampling. The chapter has also identified the sample size and the data collection methods that were applied in the study.

The chapter has indicated that the study used structured questionnaires to collect relevant data from the research participants. The research procedure and the utilized method for data analysis has also been defined. The chapter has pointed out that a spectrum of descriptive and inferential statistics was used to present the research results and to interpret the data. This includes the use of pie charts, column and bar graphs, as well as Cross-Tabulations, Correlations, regression and Analysis of Variance (ANOVA). The next chapter, Chapter Four will present the results of the study.
CHAPTER FOUR

4.0 RESULTS AND FINDINGS

4.1 Introduction

This chapter provides the findings and results of the study. The chapter uses descriptive statistics (bar graphs, pie-charts and frequency tables) to present the study findings. The chapter also uses inferential statistics (cross-tabulations, correlation, analysis of variance and regression) for deeper understanding and interpretation of the findings as per the specific objectives of the study. The response rate of the study was 92.7% (having issued out 233 questionnaires to the respondents and receiving 216 fully and correctly filled-in questionnaires). The first part of the chapter presents the findings on the respondents’ biographical data.

4.2 Background Information

The first part of the instrument asked questions aimed at understanding the respondents background. This section of the chapter presents the study finds on respondents’ biographical data.

4.2.1 Grouping of Respondents by Gender

Figure 4.1 shows grouping of respondents by age. As shown 120 (56%) were male and 96 (44%) were female.

![Figure 4.1: Grouping of Respondents by Gender](image_url)
4.2.2 Grouping of Respondents by Level of Study

Table 4.1 is the grouping of respondents by level of study. One-hundred-and-forty-three of the respondents (66.20%) were “Undergraduate”, 70 (32.41%) were “Graduate/Masters” students, 3 (1.39%) respondents were “Post-Graduate” students.

<table>
<thead>
<tr>
<th>Grouping of respondents by level of study</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undergraduate</td>
<td>143</td>
<td>66.20%</td>
</tr>
<tr>
<td>Graduate/Masters</td>
<td>70</td>
<td>32.41%</td>
</tr>
<tr>
<td>Post-Graduate</td>
<td>3</td>
<td>1.39%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>216</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

4.2.3 Frequency of Internet Use

The respondents were asked to state how frequently they used the internet. As indicated in Figure 4.2, 2 (1%) said they did not use the internet at all, 5 (2%) used it “Less often” 41 (19%) used it “Often”, 26 (12%) used it “Quite often” and 142 (66%) used it “Very often”.

![Figure 4.2: Frequency of Internet Use](image)

4.2.4 Frequency of Social Media Use

The researcher asked the respondents to indicate how often they used social media. Five (2%) indicated they did not use social media at all, 12 (6%) used it “Less often”, 41 (19%) used it “Often”, 43 (20%) used it “Quite often” and 115 (53%) used it “Very often”. Table 4.2 shows the findings.
Table 4.2: Frequency of Social Media Use

<table>
<thead>
<tr>
<th>Frequency of use of Social Media</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>5</td>
<td>2%</td>
</tr>
<tr>
<td>Less often</td>
<td>12</td>
<td>6%</td>
</tr>
<tr>
<td>Often</td>
<td>41</td>
<td>19%</td>
</tr>
<tr>
<td>Quite often</td>
<td>43</td>
<td>20%</td>
</tr>
<tr>
<td>Very often</td>
<td>115</td>
<td>53%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.2.5 Grouping of Respondents by Age

Table 4.3 shows the categorization of respondents by age. Sixty-eight (31.5%) respondents were between 16 and 20 years old, 127 (58.8%) between 21 and 25 years, 18 (8.3%) between 26 and 30 years, and 3 (1.4%) were “Over 30” years old. The mean age for the respondents was 21.99 (about 22 years), the modal age was 21, the minimum and the maximum ages were 16 and 32 years, respectively.

Table 4.3: Grouping of Respondents by Age and Other Age-Related Facts

<table>
<thead>
<tr>
<th>Respondents’ Age</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 - 20</td>
<td>68</td>
<td>31.5%</td>
</tr>
<tr>
<td>21 - 25</td>
<td>127</td>
<td>58.8%</td>
</tr>
<tr>
<td>26 - 30</td>
<td>18</td>
<td>8.3%</td>
</tr>
<tr>
<td>Over 30</td>
<td>3</td>
<td>1.4%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean age</td>
<td>21.99</td>
</tr>
<tr>
<td>Modal age</td>
<td>21</td>
</tr>
<tr>
<td>Std. Deviation</td>
<td>2.581</td>
</tr>
<tr>
<td>Variance</td>
<td>6.660</td>
</tr>
<tr>
<td>Range</td>
<td>16</td>
</tr>
<tr>
<td>Minimum age</td>
<td>16</td>
</tr>
<tr>
<td>Maximum age</td>
<td>32</td>
</tr>
</tbody>
</table>

4.3 Effect of Social Media Marketing on Consumer Privacy

In the second section of the questionnaire, the respondents were asked to answer several questions pertaining to the effect of social media marketing on consumer privacy. This section of the chapter presents the findings.
4.3.1 Most Important Consumer Privacy Concerns when Using Social Media

The researcher asked the respondents to rank from the least important to the most important, consumer privacy that concerned them when using social media. “Permitting Third-Party access of shared information” was ranked as the most important privacy concern when using social media with a 96-percentage rating, this was followed by “secondary use of shared information” with 76-percentage rating and “interpreting personal data (data mining)” was ranked third with a mean percentage rating of 70%. “Collecting personal information” and “misuse of shared information” were given the least ranking with a 66-percentage rating each. Figure 4.3 shows the results that were obtained.

![Figure 4.3: Most Important Consumer Privacy Concerns when Using Social Media](image)

4.3.2 Information Shared on Social Media

Table 4.4 is indicative of the findings when respondents were asked what information they shared on social media. One respondent (0.5%) indicated that he/she shared only information about age, 7 (3%) shared only “gender” information, 25 (12%) shared only “name”, 23 (11%) shared only “contacts (Phone number/Email Address)” while 160 (74%) indicated that they shared all the above information (age, gender, name and contacts).
Table 4.4: Information Shared on Social Media

<table>
<thead>
<tr>
<th>Information Shared on Social Media</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only age information</td>
<td>1</td>
<td>0.5%</td>
</tr>
<tr>
<td>Only gender information</td>
<td>7</td>
<td>3.2%</td>
</tr>
<tr>
<td>Only Name</td>
<td>25</td>
<td>11.6%</td>
</tr>
<tr>
<td>Only Contacts (Phone number/Email Address)</td>
<td>23</td>
<td>10.6%</td>
</tr>
<tr>
<td>All the above</td>
<td>160</td>
<td>74.1%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.3.3 Use of Information Shared in Social Media for Marketing

The researcher asked the respondents if they agreed or disagreed that the information they shared on social media had been used for marketing purposes by marketers. Figure 4.4 is indicative of the results that were obtained, 44 (20%) respondents and 118 (55%) strongly agreed and agreed respectively, 25 (12%) disagreed, 3 (1%) strongly disagreed while 26 (12%) indicated that the information they shared on social media had “not at all” been used for marketing purposes.

Figure 4.4: Use of Information Shared in Social Media for Marketing

4.3.4 Most Important Personal Information Shared on Social Media

The researcher asked the respondents to rank from the least important to the most important, the most important personal information they had shared on social media. “Email address” was ranked as the most important personal information shared on social media with a 68-percentage rating, followed by “telephone number” with a 65-percentage rating whilst “gender” and “ethnicity/race/nationality” were given the least ranking with a 59 percentage and 40-percentage rating respectively. Figure 4.5 shows the results that were obtained.
4.3.5 Awareness of Use of Shared Information for Marketing

Table 4.5 shows the results of respondents’ awareness of use of shared personal information on social media for marketing. As indicated, 88 (41%) respondents were “not at all aware”, 42 (19%) were “slightly aware” and 45 (21%) were “somewhat aware”. Twenty-four respondents (11%) were “moderately aware” and 17 (8%) were “Extremely aware” that the personal information they shared on social media was being used by marketers or for marketing.

Table 4.5: Awareness of Use of Shared Information for Marketing

<table>
<thead>
<tr>
<th>Awareness of Use of Shared Information for Marketing</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all aware</td>
<td>88</td>
<td>41%</td>
</tr>
<tr>
<td>Slightly aware</td>
<td>42</td>
<td>19%</td>
</tr>
<tr>
<td>Somewhat aware</td>
<td>45</td>
<td>21%</td>
</tr>
<tr>
<td>Moderately aware</td>
<td>24</td>
<td>11%</td>
</tr>
<tr>
<td>Extremely aware</td>
<td>17</td>
<td>8%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.3.6 Perception about Intrusiveness of Social Media Adverts

The researchers asked the respondents their perception as to whether they found social media advertisements intrusive. As indicated in Figure 4.6, 8 (4%) respondents found the advertisements to be “not at all intrusive”, 34 (16%) found them “slightly intrusive”, 54 (25%) found them “intrusive”, 47 (22%) “moderately intrusive” and 73 (34%) found the advertisements “extremely intrusive”. 

Figure 4.5: Most Important Personal Information Shared on Social Media
4.3.7 Use of Shared Information for Target Marketing

The researcher asked the respondents to state whether it was true that marketers had used personal information shared on social media to target them with marketing information. As indicated in Table 4.6, 57 (26%) respondents were “neutral”, 13 (6%) thought it was “very untrue”, 24 (11%) “untrue” while 81 (38%) and 41 (19%) indicated that it was “true” and “very true” that marketers had used personal information shared on social media to target them with marketing information.

Table 4.6: Use of Shared Information for Target Marketing

<table>
<thead>
<tr>
<th>Marketers use information for marketing</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neutral</td>
<td>57</td>
<td>26%</td>
</tr>
<tr>
<td>Very untrue</td>
<td>13</td>
<td>6%</td>
</tr>
<tr>
<td>Untrue</td>
<td>24</td>
<td>11%</td>
</tr>
<tr>
<td>True</td>
<td>81</td>
<td>38%</td>
</tr>
<tr>
<td>Very true</td>
<td>41</td>
<td>19%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>216</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

4.3.8 Perception of Misuse of Shared Information on Social Media by Marketers

Figure 4.7 shows respondents’ perception on to whether information they shared on social media had been misused by marketers. As shown, 39 (18%) respondents thought that the shared personal information had “not at all” been misused by marketers, 12 (6%) “strongly” disagreed, 60 (28%) disagreed, 77 (36%) and 27 (13%) respondents, agreed and “strongly” agreed respectively that information they shared on social media had been misused by marketers.
4.3.9 Marketers' Use of Personal Information Shared on Social Media to Target Consumers

The researcher asked the respondents to show their level of agreement on whether marketers had used the personal information shared on social media to target them with marketing information. As indicated in Table 4.7, 15 (7%) respondents indicated “not at all”, 17 (8%) “strongly disagreed”, 26 (12%) disagreed, 117 (54%) agreed and 41 (19%) indicated that they “strongly agreed”.

Table 4.7: Marketers' Use of Personal Information Shared on Social Media

<table>
<thead>
<tr>
<th>Marketers use of information to target consumers</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>15</td>
<td>7%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>17</td>
<td>8%</td>
</tr>
<tr>
<td>Disagree</td>
<td>26</td>
<td>12%</td>
</tr>
<tr>
<td>Agree</td>
<td>117</td>
<td>54%</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>41</td>
<td>19%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.3.10 Concern over Customization of Shared Information to Target Social Media Users

Figure 4.8 shows study results when respondents were asked to indicate their level of concern with marketers’ customization of personal information shared on social media to target them with marketing information. Seventeen respondents (8%) indicated they were “not at all concerned”, 28 (13%) were “slightly concerned” and 47 (22%) were concerned. Forty-two respondents (19%) were “moderately concerned” and 82 (38%) were “extremely concerned”.

4.4 Impact of Direct Internet Marketing on Consumer Privacy

The researcher sought to establish the impact of direct internet marketing on consumer privacy. This section of the chapter presents the findings that were made in this regard.

4.4.1 Most Important Consumer Privacy Concerns for Internet Users

The researcher asked the respondents to rank from the least important to the most important, the consumer privacy issue that concerned them when using the internet. “Secondary use of shared data” was ranked as the most important privacy concern when using the internet with a 69-percentage rating, this was followed by “intrusive marketing emails” with 68-percentage rating and “browsing history” was ranked third with a mean percentage rating of 67%. “Improper email adverts” and “cookies” given the least ranking with a 66 and 60-percentage rating respectively. Figure 4.9 shows the results that were obtained.

Figure 4.9: Most Important Consumer Privacy Concerns for Internet Users
4.4.2 Sharing Personal Email for Receipt Marketing

Table 4.8 shows the respondents frequency of sharing personal email for receipt of marketing information. Seventy-six (35%) respondents indicated “not at all”, 6 (3%) disagreed to sharing personal email for such information, 103 (48%) agreed and 16 (7%) “strongly” agreed to having shared personal email for receipt of marketing information.

<table>
<thead>
<tr>
<th>Sharing of Personal Email for Receipt Marketing</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>76</td>
<td>35%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>6</td>
<td>3%</td>
</tr>
<tr>
<td>Disagree</td>
<td>15</td>
<td>7%</td>
</tr>
<tr>
<td>Agree</td>
<td>103</td>
<td>48%</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>16</td>
<td>7%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>215</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

4.4.3 Frequency of Receiving Marketing Information on Email

Figure 4.9 shows respondents’ frequency of receipt of marketing information on their personal emails. Fifteen (7%) respondents were “not sure” of how often they received marketing information on their personal emails, 38 (18%) “less often”, 69 (32%) frequently, 34 (16%) “quite frequently” and 60 (28%) respondents indicated that they received marketing information on their personal emails “very frequently”.

![Figure 4.10: Frequency of Receiving Marketing Information on Email](image-url)
4.4.4 Subscription to Newsletter for Marketing Information

Table 4.9 shows the results when respondents were asked whether they had subscribed to newsletters for marketing information. As shown, 73 (34%) respondents indicated they had “not at all” subscribed, 10 (5%) “strongly disagreed” and 22 (10%) disagreed that they had subscribed to newsletters for marketing information. Contrarily, 102 (47%) respondents and 9 (4%) respondents agreed and “strongly agreed” respectively that they had subscribed to newsletters for marketing information.

Table 4.9: Subscription to Newsletters for Marketing Information

<table>
<thead>
<tr>
<th>Subscription to newsletters for marketing information</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>73</td>
<td>34%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>10</td>
<td>5%</td>
</tr>
<tr>
<td>Disagree</td>
<td>22</td>
<td>10%</td>
</tr>
<tr>
<td>Agree</td>
<td>102</td>
<td>47%</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>9</td>
<td>4%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.4.5 Perception of Intrusiveness of Internet Marketing

The researcher asked the respondents to indicate whether they thought that internet marketing was intrusive. As shown in Figure 4.10, 12 (6%) respondents were “not sure”, 8 (4%) thought internet marketing was “not at all” intrusive, 79 (37%) thought it was intrusive “to some extent”, 70 (32%), that it was “sometimes” intrusive and 47 (22%) thought internet marketing was intrusive “most of the time”.

Figure 4.11: Perception of Intrusiveness of Internet Marketing
4.4.6 Frequency of Receipt of Marketing Information Based on Shared Personal Information

Table 4.10 shows the results when the researcher asked the respondents how often they received marketing information they deemed was based on the personal information they had shared on the internet. As shown 15 (7%) respondents indicated “not at all”, 69 (32%) “less often”, 56 (26%) “often”, 45 (21%) “quite often” and 31 (14%) indicated they often received marketing information they deemed was based on the personal information that they had shared on the internet “very often”.

Table 4.10: Frequency of Receipt of Marketing Information Based on Shared Personal Information

<table>
<thead>
<tr>
<th>Frequency of marketing information receipt</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>15</td>
<td>7%</td>
</tr>
<tr>
<td>Less often</td>
<td>69</td>
<td>32%</td>
</tr>
<tr>
<td>Often</td>
<td>56</td>
<td>26%</td>
</tr>
<tr>
<td>Quite often</td>
<td>45</td>
<td>21%</td>
</tr>
<tr>
<td>Very often</td>
<td>31</td>
<td>14%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.4.7 Online Marketers Access of Internet-Users' Browsing History from Search Engines

The researcher asked the respondents whether they agreed that online marketers had access to their browsing history from search engines they used. Twenty-three (11%) respondents indicated “not at all”, 16 (7%) “strongly” disagreed, 26 (12%) disagreed, 113 (52%) agreed and 38 (18%) “strongly agreed” that that online marketers had access to their browsing history from search engines they used. Figure 4.11 is indicative of these results.

Figure 4.12: Online Marketers Access of Internet-Users' Browsing History
4.4.8 Concern Sharing of Browsing History Information for Marketing

Table 4.11 shows respondents’ concern over the sharing of browsing history information by search engines for marketing. As shown, 15 (7%) respondents were “not at all concerned”, 31 (14%) were “slightly concerned”, 56 (26%) were “concerned”, 46 (21%) were “very concerned” and 68 (31%) were “extremely” concerned.

Table 4.11: Concern Sharing of Browsing History Information for Marketing

<table>
<thead>
<tr>
<th>Concern over the sharing of browsing history information for marketing</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all concerned</td>
<td>15</td>
<td>6.9%</td>
</tr>
<tr>
<td>Slightly concerned</td>
<td>31</td>
<td>14.4%</td>
</tr>
<tr>
<td>Concerned</td>
<td>56</td>
<td>25.9%</td>
</tr>
<tr>
<td>Very concerned</td>
<td>46</td>
<td>21.3%</td>
</tr>
<tr>
<td>Extremely concerned</td>
<td>68</td>
<td>31.5%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.4.9 Whether Browsers are Prompted for Permission before Cookies are Installed

Figure 4.11 shows the results when the respondents were asked whether they agreed that websites asked them for permission to install cookies in their computers when they browsed the internet. Fifty-nine (27%) respondents indicated “not at all”, 18 (8%) “strongly” disagreed, 41 (19%) disagreed, 73 (34%) agreed and 25 (12%) “strongly” agreed that websites asked them for permission to install cookies in their computers when they browsed the internet.

Figure 4.13: Whether Browsers Prompted for Permission before Cookies’ Installation
4.5 Impact of Mobile Marketing on Consumer Privacy

The researcher also sought to determine the impact of mobile marketing on consumer privacy. This section of the chapter presents the study findings with regard to the specific questions that were asked to help achieve this objective.

4.5.1 Most Important Privacy Concern Over Mobile Marketing

The researcher asked the respondents to rank from the least important to the most important, consumer privacy issue that concerned them about mobile marketing. “Surveillance by marketers” was ranked as the most important privacy concern about mobile marketing with a 73-percentage rating, this was followed by “inappropriate marketing news from mobile service providers” with a 66-percentage rating and “intrusive calls from mobile service providers” was ranked third with a mean percentage rating of 65%. “Intrusive texts messages from marketers” and “inappropriate calls from marketers” were given the least ranking with a 64 and 58-percentage rating respectively. Figure 4.12 shows the results that were obtained.

Figure 4.14: Most Important Privacy Concern Over Mobile Marketing

4.5.2 Extent of Customers Personal Information Sharing by Mobile Service Providers

Table 4.12 shows the result when the respondents were asked to indicate how they perceived the extent of personal information sharing by the mobile service providers. As shown, 53 (25%) respondents were “neutral”, 20 (9%) thought the service providers had
“not at all” shared their personal information, 91 (42%) thought the service providers had shared their personal information “to some extent”, 27 (13%) thought the providers had shared “to quite an extent” and 25 (12%) thought that the providers had shared their personal information to “extensively”.

Table 4.12: Extent of Customers Personal Information Sharing by Mobile Service Providers

<table>
<thead>
<tr>
<th>Concern of personal information sharing by the mobile service providers</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neutral</td>
<td>53</td>
<td>24.5%</td>
</tr>
<tr>
<td>Not at all</td>
<td>20</td>
<td>9.3%</td>
</tr>
<tr>
<td>To some extent</td>
<td>91</td>
<td>42.1%</td>
</tr>
<tr>
<td>To quite an extent</td>
<td>27</td>
<td>12.5%</td>
</tr>
<tr>
<td>Extensively</td>
<td>25</td>
<td>11.6%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.5.3 Appropriateness of Sharing Customers’ Personal Information by Service Providers

The researcher asked the respondents whether they thought the sharing of personal information by mobile service providers with marketers was appropriate. As shown in Figure 4.13, 18 (8%) indicated that they thought it was “not at all” appropriate, 82 (38%) “strongly” disagreed, 46 (21%) disagreed, 37 (17%) agreed and 33 (15%) “strongly” agreed that it was appropriate for the mobile service providers to share personal information with marketers.

Figure 4.15: Appropriateness of Sharing of Customers Personal Information
4.5.4 Perception of Violation of Personal Trust by Service Providers in Sharing Personal Info

Table 4.13 shows the respondents’ perception as to whether the sharing of personal information by mobile service providers with marketers was a violation of personal trust. Twenty-two (10%) respondents thought it was “not at all” a violation of personal trust, 18 (8%) and 26 (12%) “strongly” disagreed and disagreed respectively that it was a violation of personal trust. Contrarily, 83 (38%) respondents and 67 (31%) agreed and “strongly” agreed respectively, that it was a violation of personal trust for mobile service providers to share customers’ personal information marketers.

Table 4.13: Perception of Violation of Personal Trust by Service Providers

<table>
<thead>
<tr>
<th>Violation of personal trust by mobile service providers in sharing information</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>22</td>
<td>10.2%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>18</td>
<td>8.3%</td>
</tr>
<tr>
<td>Disagree</td>
<td>26</td>
<td>12.1%</td>
</tr>
<tr>
<td>Agree</td>
<td>83</td>
<td>38.4%</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>67</td>
<td>31%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.5.6 Perception of Intrusiveness Marketing Information from Mobile Service Providers

The researcher asked the respondents whether marketing information they received on their phones from mobile service providers were intrusive. Figure 4.14 shows the results. Twenty-five (12%) respondents found the marketing information not to be intrusive at all, 50 (23%) respondents thought they were “slightly intrusive”, 69 (32%) “intrusive”, 29 (13%) “very intrusive” and 43 (20%) found the marketing information they received on their phones from mobile service providers to be “extremely intrusive”.

![Figure 4.16: Perception of Intrusiveness Marketing Information from Mobile Service Providers](image)
4.5.7 Appropriateness of Advertisements from Marketers' Received on Phones

Table 4.15 shows the respondents’ perception of the appropriateness of the advertisements they received on their phones from marketers. Forty-nine (23%) respondents found them not to be appropriate at all, 34 (16%) and 39 (18%) “strongly” disagreed and disagreed respectively that they were appropriate. Seventy-eight (36%) respondents and 16 (7%) agreed and “strongly” agreed respectively that the advertisements were appropriate.

Table 4.14: Appropriateness of Advertisements from Marketers' Received on Phones

<table>
<thead>
<tr>
<th>Appropriateness of the advertisements received on phones from marketers</th>
<th>Frequency (n)</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>49</td>
<td>23%</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>34</td>
<td>16%</td>
</tr>
<tr>
<td>Disagree</td>
<td>39</td>
<td>18%</td>
</tr>
<tr>
<td>Agree</td>
<td>78</td>
<td>36%</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>16</td>
<td>7%</td>
</tr>
<tr>
<td>Total</td>
<td>216</td>
<td>100%</td>
</tr>
</tbody>
</table>

4.6 Cross-Tabulations of Selected Variables

The research conducted a cross-tabulation analyses between different variables of the study to determine whether there were somehow related. This part of the chapter provides the results that were obtained.

4.6.1 Information Shared and Awareness of Use of Information Marketing Cross Tabulation

A cross-tabulation analysis was conducted to examine the relationship between the kind of information respondents shared on social media and their awareness that such information could be used for marketing purposes as shown in Table 4.16, 66 of the 160 respondents who shared all the personal information (age, gender, name and contacts) were “not at all” aware that such information could be used for marketing to them, as compared to just 15 (out of 160) who were “extremely aware”. Interesting none of the respondents who were “extremely aware” that personal information they shared could be used for marketing to them shared information regarding their age, gender of name. Moreover, only 2 respondents out of the 23 who shared contacts were in extremely aware that personal information they shared could be used for marketing to them. More results of the cross-tabulation analysis are shown in the table.
Table 4.15: Cross-tabulation of Information Shared and Awareness of Marketing Use

<table>
<thead>
<tr>
<th>Information Shared on Social Media</th>
<th>Awareness of Use of Shared Information for Marketing</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not at all aware</td>
<td>Slightly aware</td>
</tr>
<tr>
<td>Age</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Gender</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>Contacts (Phone/#/Email Address)</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>All the above</td>
<td>66</td>
<td>31</td>
</tr>
<tr>
<td>Total</td>
<td>88</td>
<td>42</td>
</tr>
</tbody>
</table>

4.6.2 Sharing of Personal Information and Frequency of Receiving Marketing Adverts on Email Cross-Tabulation

A cross-tabulation analysis was conducted to examine the relationship between personal respondent’s perception of personal information sharing by the internet service providers and frequency of email marketing information. As shown, 9 out of 16 who “strongly” agreed that service providers shared their personal information reported receiving marketing information “very” frequently. More results are as indicated in Table 4.17.

Table 4.16: Cross-tabulation of Sharing of Personal Information and Frequency of Marketing Emails

<table>
<thead>
<tr>
<th>Service providers sharing of personal information</th>
<th>Frequency of Receiving Marketing Info on Email</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not sure</td>
<td>Less frequently</td>
</tr>
<tr>
<td>Not at all</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Disagree</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>Agree</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>14</td>
<td>38</td>
</tr>
</tbody>
</table>
4.6.3 Mobile Service Providers Sharing of Personal Information and Perception of Violation of Personal Trust Cross-tabulation

A cross-tabulation analysis was conducted to examine the relationship between mobile service providers sharing of personal information and perception of violation of personal trust. As shown in Table 4.18, 39 respondents out of 91 who thought that the mobile service providers shared personal information “to some extent”, said that their personal trust had been violated. Similarly, 12 out of 25 respondents who thought that the mobile service provider shared the personal information “extensively”, also “Strongly” agreed that the mobile service providers had violated their personal trust.

Table 4.17: Cross-tabulation of Mobile Service Providers Sharing and Violation of Personal Trust

<table>
<thead>
<tr>
<th>Mobile service providers sharing of personal information</th>
<th>Perception of Violation of Personal Trust</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not at all</td>
<td>Strongly disagree</td>
</tr>
<tr>
<td>Neutral</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>Not at all</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>To some extent</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>to quite an extent</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Extensively</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>22</td>
<td>18</td>
</tr>
</tbody>
</table>

4.6.4 Mobile Service Providers Sharing of Personal Information and Intrusiveness of Marketing Information Cross-Tabulation

A cross-tabulation analysis was conducted to examine the relationship between mobile service providers sharing of personal information and respondent’s perception of intrusiveness of marketing information. 13 out of 25 respondents who thought the mobile service providers “extensively shared personal information, found the marketing information they received to be “extremely intrusive”. And, 35 respondents out of 91 who thought the mobile service providers shared personal information “to some extent”, found the marketing information they received to be “somewhat intrusive”. More results of the cross-tabulation analysis are as indicated in Table 4.19.
Table 4.18: Cross-tabulation of Mobile Service Providers Sharing and Intrusiveness of Marketing

<table>
<thead>
<tr>
<th>Mobile service providers sharing of personal information</th>
<th>Perception of Intrusiveness Marketing Information from Mobile Service Providers</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neutral</td>
<td>Not at all intrusiv e</td>
<td>Slightly intrusiv e</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>15</td>
</tr>
<tr>
<td>Not at all</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>To some extent</td>
<td>8</td>
<td>23</td>
</tr>
<tr>
<td>to quite an extent</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Extensively</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>25</td>
<td>50</td>
</tr>
</tbody>
</table>

4.7 Correlation Analysis among Selected Variables

The researcher conducted a Pearson correlation analysis between the dependent and the independent variables to determine the nature relationship between them. This part shows the results of the correlation analysis.

4.7.1 Correlation of Social Media Marketing and Consumer Privacy

A Pearson correlation analysis was conducted between social media marketing (independent variable) and consumer privacy (the dependent variable). As shown in Table 4.20, the Pearson correlation coefficient of $r = .172$, $<.05$ was obtained. This positive value indicated that consumer privacy was positive linked to social media marketing. However, the correlation value was small indicating a weak relationship between the two variables.

Table 4.19: Correlation of Consumer Privacy and Social Media Marketing

<table>
<thead>
<tr>
<th>Consumer Privacy</th>
<th>Pearson Correlation</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig. (2-tailed)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>216</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social Media Marketing</th>
<th>Pearson Correlation</th>
<th>.172*</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig. (2-tailed)</td>
<td></td>
<td>.012</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>216</td>
<td>216</td>
<td></td>
</tr>
</tbody>
</table>

* Correlation is significant at the 0.05 level (2-tailed).
4.7.2 Correlation of Consumer Privacy and Direct Internet Marketing

A Pearson correlation analysis was conducted between direct internet marketing (independent variable) and consumer privacy (the dependent variable). As shown in Table 4.21, the Pearson correlation coefficient of \( r = .163, <.05 \) was obtained. This positive value indicated that consumer privacy was positive linked to direct internet marketing. Similarly, the correlation value was indicative of a weak relationship between the variables.

Table 4.20: Correlation of Consumer Privacy and Direct Internet Marketing

<table>
<thead>
<tr>
<th>Consumer Privacy</th>
<th>Pearson Correlation</th>
<th>Sig. (2-tailed)</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>216</td>
</tr>
<tr>
<td>Direct Internet</td>
<td>Pearson Correlation</td>
<td>.163*</td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td>Sig. (2-tailed)</td>
<td>.016</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.016</td>
<td>216</td>
</tr>
</tbody>
</table>

* Correlation is significant at the 0.05 level (2-tailed).

4.7.2 Correlation of Consumer Privacy and Mobile (Phone) Marketing

A Pearson correlation analysis was conducted between Mobile Marketing (independent variable) and consumer privacy (the dependent variable). As shown in Table 4.22, the Pearson correlation coefficient of \( r = .206, <.05 \) was obtained. This positive value suggested that consumer privacy was positive associated to mobile marketing. Similarly, as was the case with social media marketing and direct internet marketing, the correlation value was indicative of a weak relationship between the variables.

Table 4.21: Correlation of Consumer Privacy and Mobile (Phone) Marketing

<table>
<thead>
<tr>
<th>Consumer Privacy</th>
<th>Pearson Correlation</th>
<th>Sig. (2-tailed)</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>216</td>
</tr>
<tr>
<td></td>
<td>Pearson Correlation</td>
<td>.206**</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>.002</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.002</td>
<td>216</td>
</tr>
</tbody>
</table>

** Correlation is significant at the 0.01 level (2-tailed).
4.8 Regression Analysis

4.8.1 Regression Model Summary for Consumer Privacy

A regression test was conducted to evaluate the significance of digital promotion (independent variable) on consumer privacy. This part of the chapter provided the results that were derived from the regression analysis between consumer privacy (dependent variable) and social media marketing, direct internet marketing and mobile marketing (independent variables). The total variability of the models indicated by R Square .050 suggested that 5% of the variance (or change) in the model could be explained by social media marketing, direct internet marketing and mobile marketing as is shown in Table 4.23.

Table 4.22: Model Summary for Consumer Privacy

<table>
<thead>
<tr>
<th>Model</th>
<th>R</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.223$^a$</td>
<td>.050</td>
<td>.036</td>
<td>1.474</td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), social media marketing, direct internet marketing and mobile marketing

4.8.2 ANOVA Analysis for Consumer Privacy

Table 4.24 indicates that consumer privacy (the dependent variable) is statistically significant as $F (3, 212) =.013, p <.05$. This means that the model has an explanatory value or power, that is, the three independent variables (social media marketing, direct internet marketing and mobile marketing) help predict the consumer privacy (dependent variable). To explain further, formidable evidence exist that the model is useful as .013 is less than .05. The ANOVA results are shown in Table 4.24.

Table 4.23: ANOVA Analysis for Consumer Privacy

<table>
<thead>
<tr>
<th>ANOVA$^a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

a. Dependent Variable: Consumer Privacy

b. Predictors: (Constant), social media marketing, direct internet marketing and mobile marketing
4.8.3 Regression Coefficient Analysis for Consumer Privacy

The researcher conducted a multiple regression analysis to assess further, the nature of the association between the independent variables and the dependent variable. Shown in Table 4.25 are the results that were obtained.

**Table 4.24: Regression Coefficient Analysis for Consumer Privacy**

<table>
<thead>
<tr>
<th>Model</th>
<th>Unstandardized Coefficients</th>
<th>Standardized Coefficients</th>
<th>t</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
<td>Std. Error</td>
<td>Beta</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2.428</td>
<td>.441</td>
<td>5.508</td>
<td>.000</td>
</tr>
<tr>
<td>(Constant)</td>
<td>.132</td>
<td>.086</td>
<td>.103</td>
<td>1.526</td>
</tr>
<tr>
<td>Social Media Marketing</td>
<td>.209</td>
<td>.082</td>
<td>.175</td>
<td>2.557</td>
</tr>
<tr>
<td>Direct Internet Marketing</td>
<td>-.142</td>
<td>.080</td>
<td>-.120</td>
<td>-1.765</td>
</tr>
</tbody>
</table>

a. Dependent Variable: Consumer Privacy Concerns/Misuse of Shared Information

The three equations for the model are;

i. Consumer Privacy = C + XSocial Media Marketing
   Hence;
   
   \[ \text{Consumer Privacy} = 2.428 + .132 \text{Social Media Marketing} \]

ii. Consumer Privacy = a + YDirect Internet Marketing
   Hence;
   
   \[ \text{Consumer Privacy} = 2.428 + .209 \text{Direct Internet Marketing} \]

iii. Consumer Privacy = a + ZMobile Marketing
   Hence;
   
   \[ \text{Consumer Privacy} = 2.428 - .142 \text{Mobile Marketing} \]

The general equation for predicting the impact digital promotion consumer privacy are;
Consumer Privacy = C + XSocial Media Marketing + YDirect Internet Marketing
+ ZMobile Marketing

Hence;

*Consumer Privacy* = 2.428 + .132*Social Media Marketing* + .209*Direct Internet Marketing* - .142*Mobile Marketing*

The three equations and general equation for consumer privacy developed, it can be seen the coefficients for social media marketing, direct internet marketing and mobile marketing are, .132, .209 and -.142 respectively. These suggest for every additional social media marketing, an average increase of .132 can be expected in consumer privacy at a constant of 2.428. It further reveals that for every additional direct internet marketing, an average increase of .209 can be expected in consumer privacy at the same constant and also that for every additional mobile marketing, an average decrease of -.142 can be expected in consumer privacy at a constant of 2.428.

**4.9 Chapter Summary**

Chapter Four has presented the study findings using a variety of descriptive statistics including bar graphs, pie-charts and frequency tables. The chapter has presented the findings regarding every question that the respondents were asked in the data collection instrument. The chapter has also used inferential statistics of which cross-tabulations, correlation, analysis or variance (ANOVA) and regression were applied. The next chapter, Chapter Five, provides the summary of the key findings, the discussions of the major findings, the conclusion of the study and the research recommendations.
CHAPTER FIVE

5.0 DISCUSSION, CONCLUSION AND RECOMMENDATION

5.1 Introduction

Chapter Five provides the summary of the study and the major findings of the study. The Chapter also details and discusses the major findings of the study in line with the three research objectives of the study. The chapter then provides the conclusion and the recommendations. Recommendations are provided both for improvement and for future research.

5.2 Summary

The general objective of the study was to determine how digital promotions infringe on consumer privacy. The study was guided by the following three specific research objectives; to determine ways in which social media marketing has affected consumer privacy, to evaluate the impact of direct internet marketing on consumer privacy and to determine the impact of mobile marketing on consumer privacy.

The research methodology, which was adopted was as follows. The study deployed a descriptive research design to explore or find out ‘how’ digital marketing has affected consumer privacy. The target population for the study comprised of United States International University – Africa (USIU-A) students of which 233 were sampled for the study. The study used stratified random sampling technique to ensure that students at every level of study were given an equal chance of participation in the study. A structured questionnaire was used to collect the relevant information from the students. This study used the quantitative method of data analysis, as such both descriptive and inferential statistics where be used. Microsoft Excel and Statistical Package for Social Sciences (SPSS) program version 21 were used to analyze and present the collected data.

The study made the following findings. The study determined that 97% of the respondents used the internet often and that 92% used social media often. It also determined that all the respondents owned a smart phone. The study established that “permitting Third-Party access of shared information” and “secondary use of shared information” were the most
important privacy concern issues for respondent and that “collection of personal information” and “misuse of shared information” were the least important concerns of the respondents. The study found that most respondents shared all personal information including, gender, age, name and contacts (phone number and email address). A majority of the respondents agreed that the information they shared on social media had been used for marketing purposes by marketers.

It found that email address and telephone number were the most important personal information shared on social media and that least important personal information shared was gender and “ethnicity/race/nationality”. The study established that the majority of the respondents were not aware that the personal information they shared on social media was being used by marketers for marketing. It also found that the majority of the respondents found social media advertisements intrusive. A majority of the respondents thought that marketers had used the personal information they shared to target them with marketing information and that the majority thought that marketers had misused shared information.

The study found that “secondary use of shared data” and “intrusive marketing emails” were the most important privacy concern for the respondents when using the internet and that “improper emails” and “cookies” were the least important. It found that about the same number of respondents had frequently received marketing information as those that had not and that the majority of the respondents frequently received marketing information through email. The study found that about the same number of respondents had subscribed to newsletters for receipt of marketing information as those that had not. It found that a significant number of respondents found internet marketing intrusive sometimes and that the majority of the respondents often received marketing information based on personal information they previously shared online. The study further established that the majority of the respondents believed that marketers had access to their browsing history from search engines they used and that a significant number was concerned about the sharing of such data.

The study also found that “surveillance by marketers” and “inappropriate marketing news from mobile service providers” were the most important privacy concerns with regard to mobile marketing and that “Intrusive texts messages from marketers” and “inappropriate calls from marketers” were of the least importance to respondents. It also found that a greater number of respondents believed that mobile service providers had shared their
personal information that the majority deemed this inappropriate. The study found that the majority of the respondents considered the sharing of personal information by mobile service providers as a violation of personal trust. It found that the majority found the marketing information they received on their phones from mobile service providers was intrusive.

The study found that the digital promotion and consumer privacy were positively associated. It found a positive Pearson correlation coefficient between social media marketing and consumer privacy and so was that between direct internet marketing (independent variable) and consumer privacy as well as that conducted between mobile marketing consumer privacy. It found that total variability of the models indicated by R Square .050 suggesting that 5% of the variance (or change) in the model could be explained by social media marketing, direct internet marketing and mobile marketing. It further established that consumer privacy was statistically significant, $F (3, 212) = .013, p < .05$ meaning that the model has an explanatory value or power, that is, the three independent variables help predict the consumer privacy (dependent variable). It established that the general equation for the consumer privacy was:

$$y = 2.428 + .132 \text{Social Media Marketing} + .209 \text{Direct Internet Marketing} -.142 \text{Mobile Marketing}$$

5.3 Discussions

5.3.1 Effect of Social Media Marketing on Consumer Privacy

Social media has a multiplicity of effects on the consumer privacy of its users especially with respect to how such information is used for marketing purposes. This include the collection of personal information without informing the users of the intended use of such information, misuse of the shared information, interpretation of collected information, secondary use of shared information as well as allowing third-party access of the shared information (Zephoria Digital Marketing, 2017; Campaign, 2016; McForland, 2012).

The study established that “permitting Third-Party access of shared information” and “secondary use of shared information” were the most important privacy concern issues for respondent with percentage ratings of 96% and 76% respectively, and that “collection of personal information” and “misuse of shared information” were the least important concerns of the respondents with percentage ratings of 70% and 66% respectively. “E-mail
address” and “Telephone number”, which were ranked as the most important personal information shared on social media with a 68 and 65-percentage ratings, are also the most likely to be used by marketers to convey unwarranted marketing information to the consumers.

However, despite ranking as among the least of the concerns for consumers, “misuse of shared information” with a mean rating of 70% is still indicative of respondents’ apprehension about sharing information on social media. In fact, this finding confirms a previous finding by Changi (2007) which determined that up to 45% of those surveyed indicated that they worried about how companies used such information.

The study also found that the majority of the respondents (75%) agreed that the information they shared on social media had been used for marketing purposes by marketers. It confirms the observation made by Gerlach, et al., (2015) when they noted that the information that users of SNS provide is often misused by the providers and marketers. This finding goes further to suggest why people are concerned about secondary use of shared information. Campaign (2016) found that 20% of marketers collect information about consumers’ location. This study found that most respondents shared all personal information including gender, age, name and contacts (phone number and email address).

However, to make the issue of privacy a really worrisome one is the degree to which the respondents of the current study are unaware of the uses of their information -60% are unaware of the uses of such information for marketing as compared to just 8% who are extremely aware. This finding corroborates a previous finding by Chartered Institute of Marketing (CIM) (cited in Campaign, 2016) which after conducting a study involving some 25,000 consumers and marketing gurus, found that 9 in 10 consumers had zero idea of how social media sites use their information.

Spinelli (2010) contends that Facebook and MySpace often divulge or disclose personal profiles, videos, pictures and the ability to send messages to family, acquaintances, family and co-workers. According to Gan and Jenkins (2015), they observed that the users of Twitter and Facebook are often unaware or the perils connected with signing up to social media platforms, uploading a picture on Facebook, updating status, enabling the geo-location for tagging amongst other activities. Nagapavan (2010) found that social media sites that collect personal information on that scale often without the knowledge of the
subscribers are in contravention of consumer rights. It is therefore understandable the study finding that a significant number of the respondents (49%) are concerned that information they share on social media is misused.

5.3.2 Impact of Direct Internet Marketing on Consumer Privacy

The study found that “secondary use of shared data” and “intrusive marketing emails” were the most important privacy concern for the respondents when using the internet with a mean percentage rating of 69% and 68% respectively and that “improper emails” and “cookies” were accorded the least ranking with a 66 and 60-percentage rating respectively. This is further confirmed with 69% of the respondents indicating that they found marketing information on email intrusive. Furthermore, the majority of the respondents 76% received marketing information sent by marketers indicating that marketers are increasingly using unauthorized information to send the emails. This is also indicative of the fact that the websites and marketers are obtaining such personal information without first acquiring the explicit permission of the internet users who visit such websites.

This finding corroborates a previous finding by the eMarketer (2009) which established that in the United States of America (US), about 61% of all medium and large corporations in the US engage in email marketing regularly. This is despite the fact that consumers who receive such emails have not previously subscribed to newsletters. According to Grondcolas, et al., (2007) marketers have acquired consumers email addresses and communicated to them without consumers’ consent. This is in contravention of permission marketing. As the study has established, there seems to be collection of personal information online, often without consumers’ consent. This has enabled marketers to acquire consumers’ emails without their consent as observes Grondcolas, et al., (2007).

In fact, the study found that that a significant number of respondents found internet marketing intrusive sometimes and that the majority of the respondents often received marketing information based on personal information they previously shared online. This is perhaps due to the fact that some corporations have specialized on data mining whereby their build information regarding customers based on what they browse online and construct patterns on customers preferences based on the information they share online and the websites they visit. Betancourt (2010) contends that firms are mining social web to create dossiers on consumers. It is indeed, therefore not surprising that "interpreting
personal data” (data mining” was ranked third with a mean percentage rating of 70%. Implying that consumers consider is a serious violation of their privacy online.

Grondcolas, et al., (2007) notes that some websites and social media sites require internet browsers to provide a variety of personal information including email address, name, age, gender, geographical location and contact information when browsing through or subscribing to these platforms without providing a good reason for the request. Such information is normally sold to the highest bidder or used internally for market segmentation in the firms’ marketing strategy. This information further allows the marketers to guess customer preferences and target them with marketing information that they perceive that specific customers would be most delighted to receive. The study further established that the majority of the respondents believed that marketers had access to their browsing history from the search engines they used and that a significant number was concerned about the sharing of such data.

Other studies have made interesting findings regarding internet marketing. In most instances, such digital promotions and advertisements disregard consumers’ privacy issues and laws, and increasingly, personal privacy is becoming an issue of great concern for most consumers (Al-Shakhouri & Mahmood, 2009). Papacharissi and Fernback (2005) observe that 27% of internet users in the US are concerned about online privacy violations and 54% find the tracking of personal information online a harmful practice and that 86% prefer an “opt-in” policy, which require websites to ask for permission before collecting and potentially using personal data.

5.3.3 Impact of Mobile Marketing on Consumer Privacy

Malhotra, et al. (2004) suggest that the practice of data collection, whether legitimate or illegitimate, “is the starting point of various information privacy concerns (p.338).” However, despite the growing concern among consumers with the issue of firm collection and sharing of personal data, the onset of mobile telephony has complicated the issue for consumers. The rapid advancement of mobile technologies has provided a more encompassing and powerful means of surveillance, which creates an open boundary structure with a high degree of information permeability. In today’s mobile environment, vendors take advantage of the powerful surveillance technologies to track and profile mobile consumers (Child & Petronio, 2010).
The study found that “surveillance by marketers” was ranked as the most important privacy concern about mobile marketing with a 73-percentage rating, this was followed by “inappropriate marketing news from mobile service providers” with 66-percentage rating. The problem with such surveillance and one which is highly problematic is that such surveillance is not only unwarranted but also permit the mobile service providers to track their customers daily routines including the places they frequency and the kind of information they browse for in their smart phones. Child and Petronio (2009) has argued that mobile telephone providers currently have the ability to monitor what kind of information their subscribers browse for online, but also their preferences in terms of the clothes they wear and even the kinds of food they prefer through various sophisticated software that are available in the smart phones which customers unknowingly install.

It has been argued that intrusion interrupts the victim’s activities or routines, destroys his or her solitude, and often makes the victim feel uncomfortable (Solove, 2006). Yet mobile phone service providers are proving to be master intruders of personal privacy in terms of the marketing messages they themselves send to their subscribers informing them of new services and products. Such messages and calls that the service providers make to customers have the potential of and often do interrupt subscribers daily routine including private and important customers' calls, mobile conferences among other activities that customers may be in the process of doing when such intrusion happen.

Malware is an especially growing problem for smartphones (Dignan, 2011). Users may resist mobile applications(apps) for fear that the malicious apps may interrupt their activities through their unwanted presence. The major point that emerges is that intrusion can create discomfort and harm and therefore, the flow of personal information across boundaries requires users’ efforts to restore their comfort levels. Some of the malware are actually created by marketers with the goals of corrupting the operating systems of the smartphones and acquiring access to personal information that they may finds useful in their marketing communication and market segmentation.

The study found that 76% of the respondents were of the opinion that the kind of information that marketers send to them on their phones were inappropriate. At the same time, 69% of the respondents considers the collection and sharing of personal information by mobile phone service providers a violation of trust. This suggests that a large proportion
of consumers consider mobile marketing a gross violation of consumer privacy especially when their explicit permission is not sought first.

The activity of secondary use of information by an organization, can “potentially threaten an individual’s ability to maintain a condition of limited access to his/her personal information, harm individuals, and subsequently threaten the organization’s legitimacy in its interactions with consumers, shareholders, and regulators (Culnan & Williams 2009). The practice of secondary use of personal information triggers the coordination of linkage rules which refer to “the establishment of mutually agreed-upon privacy rules used to choose others who may be privy to the collectively held information” (Jin, 2012, p.70).

5.4 Conclusion

5.4.1 Effect of Social Media Marketing on Consumer Privacy

Social networking sites including Foursquare, Facebook, LinkedIn, Google + and Instagram do collect personal information with or without subscribers’ awareness. This is serious violation of consumer privacy privileges. The exponential use of social media makes it a platform through which the providers and other people or organizations can obtain a lot of personal information. However, most of the users of these sites are unaware that their personal data is being collected and are often unaware of the perils connected with signing up to social media platforms, uploading a picture on Facebook, updating status, enabling the geo-location for tagging amongst other activities. The personal data collected by social media sites includes names, telephone numbers, national identity card numbers, social, insurance and credit security numbers, employee numbers, personal or family medical information and personal or family financial information, making it a treasure trove for marketers. This research has established that marketers acquire and misuse personal information from and in social media sites and use the information for objectives not initially intended.

5.4.2 Impact of Direct Internet Marketing on Consumer Privacy

Direct internet marketing is equally guilty of violating consumer privacy rights. One such issue is with regard to direct email marketing. Marketers have acquired consumers’ email addresses and communicated to them without their consent something which contravenes the idea of permission marketing, where marketing communication is based on consumers’ issuance of permission or consent to receive marketing information. The fact that several
web-based firms including social media have the tendency to share personal information with marketers for a profit or to use the information themselves; the issue of improper marketing emails is a major concern for consumer. Companies and e-marketers are acquiring personal information and using them without obtaining consent of the consumers. Through data mining, marketer and web-based firms are able to gather and make inferences on the collected data. Such information is not only used for marketing purposes by the collecting site or marketers but can also be shared across departments and firms or the collecting firms can as well generate patterns in personal data shared and sell them to marketers who do direct internet marketing.

5.4.3 Impact of Mobile Marketing on Consumer Privacy

The speedy growth of mobile technologies has provided a more encompassing and powerful means of surveillance, which creates an open boundary structure with a high degree of information permeability. Increasingly, the aggressive data collection activities by mobile apps and operating systems induce the perception of intensive data logging, as well as the impression that vendors are constantly monitoring user behavior through smartphones, which has various functions such as web browsers, emails, photo albums, games, calendars, and contact lists, apps can collect far more personally invasive data than was previously conceivable in conventional use of personal computers.

As such, just like in social media marketing and direct internet marketing, mobile marketing also raises concerns over secondary use of information. Some of the main issues of concern with regard to mobile marketing are; permission for the collection of personal information, secondary use of personal information (such profiling individuals and sending marketing messages), surveillance and the interpretation of collected information without authorization from the individuals. Hence, mobile marketing raising another instance of grave concern with the whole idea of digital marketing.

5.5 Recommendations

The study makes the following recommendations for improvement for further research at the backdrop of the study findings and the information obtained from the review of existing literature.
5.5.1 Recommendations for Improvement

5.5.1.1 Effect of Social Media Marketing on Consumer Privacy

The government of Kenya should strengthen existing laws on consumer protection and engage the Senate to formulate regulations that address privacy concerns facing the Kenyan community in the age of digitization and digital marketing. The government of Kenya, through the Ministry of Information, Communication and Technology should emphasize respect of consumer privacy as a requisite for social media service providers’ access to Kenyan markets. The consumer protection authority or/and the government through the Ministry of Information, Communication and Technology should sensitize consumers on how social media providers and marketers abuse their privacy privileges as consumers and where they should seek redress in cases where such privileges have been violated. Consumers should take caution and exercise restraint in relation to the kind of personal information they share on social media.

5.5.1.2 Impact of Direct Internet Marketing on Consumer Privacy

The government of Kenya should enact policies to properly regulate the use of internet in Kenya. Through the Ministry of Information, Communication and Technology the government should work to ensure that the potential harm of the internet to the Kenyan population is minimized as much as possible. The government through the relevant agencies should explore ways of ensuring that marketers are taken to account for their violation of consumer privacy rights and in so doing should engage the Senate to ensure that stringent laws are enacted to protect the vulnerable consumers or internet users as much as possible. The government and the consumer protection authority in Kenya should define proper and effective policies and strategies respectively to enhance consumer protection when they use the internet. The government through the Ministry of Information, Communication and Technology should flag websites, search engines and social media platforms which they deem are in constant violation of consumer privacy rights.

5.5.1.3 Impact of Mobile Marketing on Consumer Privacy

The parliament should define new laws that address the issue of consumer privacy in mobile marketing. The parliament should ensure that such laws should identify compensatory or restorative modalities for mobile service providers who violate consumer
privacy or permit third-party access of shared information. Furthermore, the government should levy taxes on mobile advertisements and marketing information sent to phones in the same way posters and billboards are taxed. The government should enact laws demanding that mobile service providers declare their intended purpose of use for the personal information they collect from subscribers.

5.5.2 Recommendations for Further Research

Researchers should conduct further studies to facilitate the understanding of consumer privacy. Future research should concentrate on assessing ways in which digital marketing infringes consumer privacy privileges especially among different age groups, regions and on different digital platforms. Researchers and academicians should conduct more research to help the understanding of why even those who are aware of how marketers can access and use personal information are still willing to issue out such sensitive information. Researchers should also conduct studies to determine whether secondary access to personal information shared with mobile service providers, on social media and websites are surrendered willingly and the gains these entities make by allowing third party access to the shared personal information. Researchers should also study ways in which consumer privacy impact on digital promotions.
REFERENCES


Internet. [Online], available at: http://www.heinz.cmu.edu/~acquisti/shb/Petronio.pdf. [28/02/17]


Nagapavan, C. (2010). Marketing Using the Social Media and Privacy Issues. [E-mail], available at: cnp@cuj@gmail.com, or cnp@cuj.ac.in. [Accessed: 02/03/17]


APPENDIX 1: LETTER OF INTRODUCTION

Odupoy, Sophie
+254 – 721 630 380
2017.

Dear

Professor Wambalaba
Head of Research USIU

RE: LETTER OF INTRODUCTION

I am graduate student currently pursuing a Master of Science in Business Administration at USIU- A. I am required, as part of the degree program, to do a conduct a research project, accordingly, am in the process of doing a study.

My research topic is, “IMPACT OF DIGITAL PROMOTIONS ON CONSUMER PRIVACY: A CASE STUDY OF EXPERIENCE OF UNITED STATES INTERNATIONAL UNIVERSITY STUDENTS”. As the topic suggest, I plant to conduct my study in USIU. This letter is therefore to request to be granted permission to conduct the study within the institution.

I affirm to adhere strictly, to the rules governing research as and to follow all relevant ethical standards when conducting the study. The responses will be treated as with utmost confidentiality and the respondents will be granted anonymity. Your permission is highly appreciated

Yours Sincerely,

Sophie Odupoy
APPENDIX 2: QUESTIONNAIRE

IMPACT OF DIGITAL PROMOTIONS ON CONSUMER PRIVACY: A CASE STUDY OF UNITED STATES INTERNATIONAL UNIVERSITY – AFRICA (USIU – A)

Date: __________________

The purpose of the study is to determine the impact of digital promotions on consumer privacy.

Kindly read each query cautiously and respond to it to the best of your ability, where necessary mark [✓] the boxes provided. There are no accurate or inaccurate responses; your answers are crucial to the study. All replies to this survey are completely confidential. All identifying information if any will be removed during the data entry and analysis; however, you are advised to respond anonymously.

Thank you for your participation in this study.

PART 1: BIOGRAPHICAL INFORMATION

1. Please indicate your age.

________________________

2. Kindly indicate your Gender.

[ ] Male
[ ] Female

3. Please indicate your academic level of study

[ ] Undergraduate
[ ] Graduate/Masters
[ ] Post-graduate
[ ] PhD

4. How often do you use the internet?

[ ] Not at all
[ ] Less often
[ ] Often
[ ] Quite often
[ ] Very often

5. How often do you use Social Media? (i.e. Foursquare, Facebook, LinkedIn, Google + and Instagram)

[ ] Not at all
[ ] Less often
[ ] Often
[ ] Quite often
[ ] Very often
PART II: EFFECT OF SOCIAL MEDIA MARKETING ON CONSUMER PRIVACY

6. In the table below are some of the consumer privacy concerns when using social media. Please rank in order of importance, which one concerns you the most.

<table>
<thead>
<tr>
<th>Consumer Privacy Concerns</th>
<th>Least Important</th>
<th>Most Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Collecting personal information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Misuse of share information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Interpreting personal information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Secondary use of shared personal information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Allowing third-party access to shared information</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. Which of the following information have you had to share on social media sites?
   - [ ] Age
   - [ ] Name
   - [ ] Contacts (phone number/email address)
   - [ ] All the above

8. Do you believe that marketers or social media sites have used the information you provided to market to you their products and services or those of other firms?
   - [ ] Not at all
   - [ ] Slightly disagree
   - [ ] Disagree
   - [ ] Agree
   - [ ] Strongly disagree
   - [ ] Strongly agree

9. In the table below are some of the personal information that you provide when using social media. Please rank in order of importance, which one you believe marketers have used to market to you.

<table>
<thead>
<tr>
<th>Personal Information</th>
<th>Least Important</th>
<th>Most Important</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1. Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Race/Ethnicity/Nationality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Email address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Telephone number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10. Were you aware or were you informed that the information you provided on social media could be used for marketing purposes?
    - [ ] Not at all aware
    - [ ] Slightly aware
    - [ ] Somewhat aware
    - [ ] Moderately aware
    - [ ] Extremely aware
11. How intrusive do you find advertisements on social media?
   [ ] Not at all intrusive  [ ] Slightly intrusive
   [ ] Intrusive  [ ] Moderately intrusive
   [ ] Extremely intrusive

12. Consider the kind of marketing messages that you receive on social media sites. Would you say it is true that marketers have used your personal data to market to you?
   [ ] Neutral  [ ] Very untrue
   [ ] Untrue  [ ] True
   [ ] Very true

13. Would you agree that marketers have misused your personal data available on social media?
   [ ] Not at all  [ ] Strongly disagree
   [ ] Disagree  [ ] Agree
   [ ] Strongly agree

14. Would you say that marketers have purposely used the data that you provided on social media sites to target you with particular advertisements?
   [ ] Not at all  [ ] Strongly disagree
   [ ] Disagree  [ ] Agree
   [ ] Strongly agree

15. How concerned are you about the use of your personal data (that is available on social media) by social media networks and marketers to customize advertisements and promotions to you?
   [ ] Not at all concerned  [ ] Slightly concerned
   [ ] Concerned  [ ] Moderately concerned
   [ ] Extremely concerned

PART III: IMPACT OF DIRECT INTERNET MARKETING ON CONSUMER PRIVACY

16. In the table below are some of the consumer privacy concerns when using the internet (not including social media). Please rank in order of importance, which one concerns you the most.

<table>
<thead>
<tr>
<th>Consumer Privacy Concerns</th>
<th>Least Important</th>
<th>Most Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Intrusive marketing emails</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Improper email advertisements/promotions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Secondary use of provided data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Browsing history</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Cookies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

17. Have you ever given your personal email and permission to a website to send you marketing information in the past?
18. How frequently have you received marketing promotions/advertisements on your email?
[ ] Not at all  [ ] Strongly disagree
[ ] Disagree  [ ] Agree
[ ] Strongly agree

19. Have you subscribed to any newsletter that would provide marketers with your personal email and other personal details?
[ ] Not at all  [ ] Strongly disagree
[ ] Disagree  [ ] Agree
[ ] Strongly agree

20. Do you find marketing information that you receive on email or when you browse the internet intrusive?
[ ] Not at all  [ ] Not at all
[ ] to some extent  [ ] Sometimes
[ ] Most of the time

21. How often do you find that marketers or websites are providing you advertisements that are based on information that you may have provided to another marketing or social media site?
[ ] Not at all  [ ] Less often
[ ] often  [ ] Quite often
[ ] Very often

22. Do you believe that internet-based marketers have access to your browsing history when you use the search engines?
[ ] Not at all  [ ] Strongly disagree
[ ] Disagree  [ ] Agree
[ ] Strongly agree

23. How much does it concern you that marketers, website and search engines are sharing information for marketing purposes?
[ ] Not at all concerned  [ ] Slightly concerned
[ ] Concerned  [ ] Moderately concerned
[ ] Extremely concerned

24. Do marketing Information prompt you for permission to install cookies in your computer or mobile device?
[ ] Not sure  [ ] Strongly disagree
[ ] Disagree  [ ] Agree
[ ] Strongly agree

PART IV: IMPACT OF MOBILE MARKETING ON CONSUMER PRIVACY

25. In the table below are some of the consumer privacy concerns over mobile marketing. Please rank in order of importance, which one concerns you the most.
### Consumer Privacy Concerns

<table>
<thead>
<tr>
<th>Consumer Privacy Concerns</th>
<th>Least Important</th>
<th>Most Important</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1. Intrusive texts from marketers</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>2. Inappropriate calls from marketers</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>3. Surveillance by marketers and service providers</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>4. Intrusive calls from service providers</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>5. Improper marketing communication from service providers</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

26. To what extent would you say that mobile service providers have shared your personal information with marketers?

- [ ] Neutral
- [ ] Not at all
- [ ] to some extent
- [ ] to quite an extent
- [ ] extensively

27. Would you consider the sharing of your personal information by the service providers with other marketers and organizations as proper if you were not consulted?

- [ ] Not sure
- [ ] Strongly disagree
- [ ] Disagree
- [ ] Agree
- [ ] Strongly agree

28. Can you say that by sharing your personal information with marketers or other firms your mobile service provider has violated your trust?

- [ ] Not sure
- [ ] Strongly disagree
- [ ] Disagree
- [ ] Agree
- [ ] Strongly agree

29. Would you consider marketing information that you receive from service providers as intrusive?

- [ ] Not at all intrusive
- [ ] Slightly intrusive
- [ ] Somewhat intrusive
- [ ] Moderately intrusive
- [ ] Extremely intrusive

30. Would you say that the marketing communication that you receive from other organizations or marketers is appropriate?

- [ ] Not sure
- [ ] Strongly disagree
- [ ] Disagree
- [ ] Agree
- [ ] Strongly agree

---

Thank you for Your Participation in the Study