A LOCATION-BASED PRIVACY PRESERVING MODEL FOR M-LEARNING ADOPTION TO ENHANCE DISTANCE EDUCATION IN KENYA

PETER BWANCHETE OBIRIA

MASTER OF SCIENCE

(Computer Systems)

JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY

2017

A Location-Based Privacy Preserving Model for M-Learning Adoption to Enhance Distance Education in Kenya

Peter Bwanchete Obiria

A Thesis Submitted in Partial Fulfillment for the degree of

Master of Science in

Computer Systems in the Jomo Kenyatta University of

Agriculture and Technology

2017

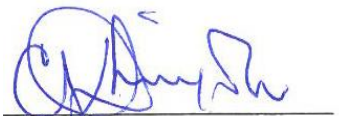
DECLARATION

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

Signature: _____ Date: _____

Peter Bwanchete Obiria

This thesis has been submitted for examination with our approval as the university supervisors.

Signature:  Date: 20.3.2017

Dr. Cheruiyot W.K

JKUAT, Kenya

Signature: _____ Date: _____

Dr. Michael Kimwele

JKUAT, Kenya

DEDICATION

I dedicate this work to my family members for their loving kindness, encouragement and prayers. God bless you.

ACKNOWLEDGEMENT

I acknowledge the Supremacy of Almighty God for bringing me this far. Many thanks to my able supervisors: Dr. Cheruiyot and Dr. Kimwele; for their constant guidance. I also appreciate my family members for their sincere love and moral support. Finally, I am grateful to all who assisted me in one way or the other in the entire period.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

LIST OF ACRONYMS

DRM	-	Digital Rights Management
GPS	-	Global Positioning System
GSMA	-	Groupe Speciale Mobile Association
ICT	-	Information Communication Technology
IDT	-	Innovation Diffusion Theory
IETF	-	Internet Engineering Task Force
LBS	-	Location Based Service
P3P	-	Platform for Privacy Preferences
PDRM	-	Personal Digital Rights Management
PLS	-	Partial Least Squares
TAM	-	Technology Acceptance Model
TPB	-	Theory of Planned Behavior
TRA	-	Theory of Reason Action
UNESCO	-	United Nations Educational, Scientific and Cultural Organization
UTAUT	-	Unified Theory of Acceptance and Use of Technology
W3C	-	World Wide Web Consortium

WLAN	-	Wireless Local Area Network
ZKP	-	Zero-knowledge proofs
SPSS	-	Statistical Package for Social Sciences
URL	-	Universal Resource Locator
PIR	-	Private Information Retrieval
IMEI	-	International Mobile Equipment Identity
PINs	-	Personal Identification Numbers

ABSTRACT

Developments in mobile learning have seen the adoption of high power, location-aware mobile gadgets in distance education. Location-based privacy in mobile learning is essential to retain users' trust, key to influencing usage intention. While extant studies have proposed models for mobile technologies adoption into learning, few have integrated location privacy aspects and their influence on m-learning implementation. Hence, there was need to develop a location-based privacy-preserving model to evaluate learners' behavioral intention to use location-aware mobile systems for distance education.

The research employed descriptive design and with a questionnaire, data was collected by sending a URL link to 336 University students registered for Distance Learning, and replies were obtained from 323 learners, representing 96.13% respondents. Using SPSS version 20 and WarpPLS 5.0, data was statistically analyzed and results discussed accordingly to answer the research's research questions.

A new model based on extant theoretical models was presented, tested and found to fit well based on the recommended quality indices. The research shall provide University management with informed approach to consider privacy-preserving aspects in m-learning implementation. It will also provide enlightened guidance to mobile learning application developers on the need to cater for learners' location-based privacy.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Research

The upsurge of mobile devices and their capabilities thereof in the past few years has made mobile learning (m-learning) to establish itself as a learning more accessible, personalized and flexible for students (Wagner, 2008). Whether formal or informal, m-learning, has significantly evolved over the years from the laptop era to the current generation of ultramodern smart phones that are location-aware (Hwang *et al.,* 2008). It is also claimed that m-learning is not just an extension of e-learning, but a totally different learning concept. According to Kambourakis (2013), the differences between the e- and m- in regards to learning are so prominent that it compels following an entirely different path towards information presentation, instructional design, and graphic and user experience design.

Therefore, with the advent of smart phones equipped with mobile sensing technology into education realm, large scale collection of personal specific data is now possible. Typical sensor information include GPS, Location, WLAN, cell tower ID, browsing history, microphone and so on. It is now easy to infer a user's home address, office location, when and means of movement among others from this personal data collected. Through statistical modelling over the sensor data time-series, it is possible to infer behavior patterns of the user such as their outdoor Buthpitiya *et al*., (2011) and indoor Zhu and Zhang (2011) mobility patterns. Consequently, such personal data if not

protected has severe privacy effects, including a hindrance to seamless adoption of mobile learning technologies. Therefore, preserving location privacy of learners while sensitive data is stored or processed in m-learning systems is a non-trivial concern.

Consequently, a secure location-based privacy mechanism is essential to retain users' trust, key to influencing usage intention of any new technology. This is because any risk on privacy can have drastic effects on users' perceptions of a system's reliability and trustworthiness (Adams & Blandford, 2003). Mobile technologies provide several possibilities for constantly monitoring learners in space, which at times can be regarded as trampling on user's privacy sphere; hence, creating a tradeoff between preserving user's privacy and providing essential assistance to learners (Kambourakis, 2013). For example, the monitoring of learners content of communication, geographic location, and/or browsing behavior may be easily assumed to lead to user profiling in mid or long term.

Accordingly, a privacy-preserving mechanism is needed to enable users be identifiable only if necessary. As a result, it is important to identify key underlying factors that can cause privacy concerns in online mobile learning and limitations of the current privacy protection methods. In the context of m-learning, the provision of privacy-preserving mechanisms is crucial to safeguard private sensitive data (Kambourakis, 2013). Moreover, a presentation done by Kukulska-Hulme (2013) in a United Nations Educational, Scientific and Cultural Organization (UNESCO) mobile

learning symposium, revealed several challenges facing m-learning implementation, among them being data security, privacy and trust.

Kenya like other countries in the world is grappling with upsurge in her university distance learning enrollment; fueled by increased need for education and social-economic factors. However, due to dynamic technological change, the modes of delivery introduced by these institutions have constantly evolved from the crude correspondence, to e-learning and now m-learning. Universities have developed a great interest on how to engage mobile technologies in making learning of students more interactive and supported anywhere, anytime and on the go. Ambitious projects are ongoing with some institutions already rolling out distance learning using portable mobile equipment. One such institution is Kenyatta University which transformed its school of distance learning to Digital School of Virtual and Open Learning to incorporate m-learning aspects. It offers free tablets fully loaded with registered units to its new students during enrollment.

However, detailed literature analysis by Ariffin (2011), Jacob and Issac (2007), Litchfield *et al.,* (2007), Rajasingham (2011), and Rapetti *et al*., (2011), made a number of assertions on areas in urgent need of investigations:

i. **There is need for secure platform for M-learning implementation across higher learning institutions: -** This allegation is supported by Graf (2002) who claims that ICT usage in online learning can cause many security risks, such as loss of confidentiality and availability, the exposure of critical data, and vandalism

of public information services. In addition, studies done in Malaysian schools found that personal space invasion (that is personal privacy in this context), that result to cyber bullying was one of the challenges to effective mobile learning implementation. Conversely, with many clients and services existing in pervasive environment, location-aware entities are able to collect personal data raising concerns of such information, private and confidential to users being disclosed when clients are looking for services and when service providers are providing the services. It was therefore found that security is one of the criteria students use to determine usage intention of mobile applications and devices.

ii. **There is an urgent need for security knowledge and awareness of learning and teaching strategies to efficiently use mobile technologies in learning: -** According to Chen and He (2013), security issues are attached to users' poor awareness of security measures, improper behaviors, and lack of education. For instance Weippl and Ebner (2008), argue that many institutions' main online learning providers have installed firewalls and anti-virus software to protect their learning resources. Furthermore, they continue to enhance the content and technology in their online learning systems to secure online learning (Alwi & Fan, 2010; Srivastava & Sinha, 2013). But in recent years, even though users' security knowledge and skills have grown, security issues such as information manipulation by outsiders and insiders and loss of confidentiality still happen from time to time (Dietinger, 2003).

iii. **There is a high demand to investigate security threats, countermeasures and solutions for implementing mobile learning in a secure platform for reliability and sustainability:-** Extant studies have identified security and privacy issues, especially for the m-learning ecosystem as worth looking into. To effectively fulfill security and privacy requirements in this dynamic computing environment, choices regarding security must take into account the user's different contextual attributes which may vary frequently and rapidly (Kambourakis, 2013).

iv. **Investigations are needed to develop security strategies for effective m-learning implementation: -** Secure and trusted m-learning system implementation is a major concern in applications and systems where information sharing is needed as such systems should prevent data loss or corruption and that security is lacking on all major platforms (Mahalingam, 2012). Their assertions are backed by the upsurge in number of applications infected with malware that rose from 80 to 400 between January and June 2011, as reported by ("Lookout Mobile Security", 2011). On the same note, mobile threat has been found to be one of the top five threats grown substantially in the year 2011 as reported in ("SOPHOS Security Threat Report", 2012). In the report, more than 50 third-party applications on Google's Android Marketplace were infected with Trojan that was designed to gain administrative privileges over personal phone without user's permission.

1.2 Problem Statement

Developments in mobile learning have seen the adoption of high-power, location-aware mobile gadgets into distance education which offer additional freedom through service mobility. However, mobile devices have the ability to leak their user's location data consequently tracking their movement in space besides allowing ruthless businesses to overwhelm the devices with spam related to that individual's location leading to overload of m-learning systems already known to contain low processing power (Duckham & Kulik, 2006). In addition, the data collected can lead to stalking and intrusive inferences that result in the abuse of user profiling which is generally unacceptable. Lack of security and privacy awareness on unauthorized user's location data collected by location-aware mobile devices hamper sustainable adoption of m-learning systems.

1.3 Justification

Security and privacy aspects in m-learning are quite different from those tackled in e-learning context which is a result of users being worried about the use of sensitive personal data collected without their implicit consent. Mobile devices have the ability to expose its user's location and consequently tracking their movement in space. Vulnerability issues in mobile technologies are becoming common due to lots of ad-hoc mobile networks, high penetration of mobile devices and lack of user security and privacy awareness.

Findings of this research benefit distance learners by providing rich content on the need to protect their location information and proposing a viable solution. Institutions of higher learning implementing mobile learning also benefit through the research's deep insight on location-based factors that hamper seamless adoption of m-leaning. Finally, the research provides informed guidance to mobile learning application developers on the need to ensure that learners' privacy aspects are well catered for.

1.4 General Objective

To develop a location-based privacy-preserving model for m-learning adoption to enhance distance education in Kenya

1.5 Specific Objectives

i. To determine how secure location-based privacy relate to intention to use m-learning systems;

ii. To evaluate extant m-learning models in preserving learners' location-based privacy;

iii. To develop a location privacy-preserving model for evaluating learners' behavioral intention to use location-aware m-learning systems to enhance distance education in Kenya;

iv. To evaluate the effects of the identified constructs on the intention to use m-learning systems for distance education in Kenya.

1.6 Research Questions

In order to fulfill the above objectives, the research sought answers to the following questions:

i. How does location-based privacy relate to intention to use m-learning systems?

ii. How do extant m-learning models address learners' location-based privacy?

iii. How can a location privacy-preserving model be developed to evaluate learners' behavioral intention to use location-aware m-learning systems to enhance distance education in Kenya?

iv. What are the effects of identified constructs on the intention to use m-learning systems for distance education in Kenya?

1.7 Scope

This research dwelt on location-based privacy of m-learning systems that when implemented enhance open and distance learning. Respondents to the research were students of selected universities enrolled for open and distance learning using mobile systems.

1.8 Limitations

The research faced the limitations in terms of scope and area of coverage. A sample size of 336 of respondents was obtained using Yamane (1967:886) formula from a population of 2100 enrolled in distance learning from selected institutions, which resulted to scope limitations and generalizability.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

This chapter presents a literature research and theoretical basis for the thesis culminating into a research model, gaps in research and the contributions of the research into the body of knowledge. It starts with concepts clarification, then impact of location privacy on m-learning usage intention, the research's contributions and extant research gaps.

2.2. Concept Clarification

This section presents a detailed description of important concepts related to the theme of research. These include: distance education, m-learning, security, and privacy.

2.2.1. Distance Education

Distance education is the delivery of courseware from afar. It is a general term covering the broad range of teaching and learning events in which the student is separated (at a distance) from the instructor, or other fellow learners (Williams, 2009). Additionally, it can be termed as the acquisition of knowledge and skills through mediated information and instruction, encompassing all technologies and other forms of learning at a distance (Hoyle, 2014). Distance learning has seen tremendous evolution through introduction of a host of technologies that included radio programming, local television and eventually telephone and video-based courses as delivery media. In addition, videoconferencing, FAX, and satellite, were utilized shortly after their invention as learning object delivery media (Bartley & Golek, 2004). This mode of learning passed features to M-Learning,

which augments the delivery methodology with mobile course access. In addition, M-Learning demonstrates another important characteristic of Distance Learning; it takes advantage of new methods for learning distribution.

Based on the above stated definitions the following concept description for distance education can be formulated for this research: Distance education is the teaching and learning process over distance whereby a variety of situation-specific media, correspondence techniques, programs, support and management structures are utilized to establish and improve communication and feedback between skilled experts from institutions and students over a wide geographical area irrespective of time, space and location.

2.2.2. Mobile Learning

Mobile learning (m-learning) is the capacity to obtain educational resources, research materials and information at any time and place, through mobile communication devices (GSMA, 2010, p. 6). This gives students limitless opportunities to learning and may at times substitute formal learning activities. M-learning is thought to be more ubiquitous as it enables teaching and learning to take place at any geographical location and at any time. According to Traxler (2009), m-learning means mobile e-learning aimed to be a continuation of conventional e-learning to solve its perceived inadequacies and limitations.

All students cannot afford personal computers and Internet connectivity, making e-learning not accessible to every student. M-learning therefore is an extension of e-

learning affording more students the opportunity to connect to resources and Internet. Accessibility to resources and material needed for distance education promotes and boosts interactivity since more students can afford mobile phones. Improved communication technologies enable students to have access to further education irrespective time and place.

In terms of distance education, movable communication devices are utilized for purposes of removing limitations to interactivity on teaching and learning with regard to location (Cavus & Ibrahim, 2009). Students are flexible in distance learning when the opportunity exists to access teaching and learning at any time and from anywhere offering students more autonomy and choices in distance education (Rekkedal, 2005). Locations where students are situated are diverse and the teaching and learning process has to be adjusted to accommodate all role players in distance education. An important objective of m-learning is to add flexibility in dealing with distance education programmes (Lim, 2011). Flexibility in learning enables role players to learn at anytime and anywhere, making learning movable and adaptable to students' unique circumstances.

2.2.3. Security

In online learning realm, security is the protection from malicious or accidental misuse of resources (Adams & Blandford, 2003). Other studies indicate that security has three basic components: confidentiality (privacy), integrity, and availability (Serb et al, 2013; Weippl & Ebner,2008; Adams & Blandford, 2003). This research will dwell on

confidentiality/privacy which is the protection of sensitive information from unauthorized access and the absence of unauthorized disclosure of information (Weippl & Ebner, 2008; Serb et al, 2013).

According to Graf (2002), ICT usage in online learning can cause many security risks, such as loss of confidentiality and availability, the exposure of critical data, and vandalism of public information services. A study by Chen and He (2013) asserts that security issues are attributed to users' poor awareness of security measures, improper behaviors, and lack of education. For instance Weippl and Ebner (2008), argue that many institutions' main online learning providers have installed firewalls and anti-virus software to protect their learning resources. Furthermore, they continue to enhance the content and technology in their online learning systems to secure online learning (Alwi & Fan, 2010; Srivastava & Sinha, 2013). But in recent years, even though users' security knowledge and skills have grown, security issues such as information manipulation by outsiders and insiders and loss of confidentiality still happen from time to time (Dietinger, 2003).

2.2.4. Privacy

The term "privacy" covers a number of facets, and has seen varying definitions proposed. The first distinction is the one that is often made between bodily privacy (concerned with protection from physically invasive procedures, such as genetic testing), communication privacy (concerned with security of communications, like mail and email), territorial privacy (concerned with intrusions into physical space, like homes and

workplaces), and information privacy (concerned with the collection and handling of personal data) (Pfitzmann & Ohntopp, 2001).

In regards to "information privacy," Alan Westin, a privacy pioneer, developed one of the most influential and commonly quoted definitions: "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*" (Westin, 1967). According to Zafar *et al.,* (2014), privacy is the condition culminating through authorizing and authenticating users, to ensure data integrity and protecting the personal information against unattended access. These authors, on the context of m-learning further clarify that while security is a methodology of ensuring integrity of data and protecting policies of the institution; privacy, is maintaining of an environment where the student can control how his private information is stored and shared. In contrast, Nissenbaum (2010) treats privacy as an internalized norm embedded in the daily life of people engaged in social pursuits. While, MacCarthy (2014) argues that privacy is a right to an appropriate flow of information, where appropriate is defined by the context in which the information is generated, disclosed and used. The author adds that privacy rules are context-based informational norms that govern the transmission of information to protect the integrity of the context.

Mobile technologies provide several possibilities for constantly monitoring learners in regards to protecting user privacy. However, this may sometimes be regarded as trampling on user's privacy sphere. While, collecting and evaluating personal data

such as user's preferences and goals be essential to provide assistance for learners, achieve assessment, or ease collaboration between users; it may become a tradeoff between preserving user's privacy, monitoring and controlling learner's behavior (Kambourakis, 2013). For example, the monitoring of learners content of communication, geographic location, and/or browsing behavior may be easily assumed to lead to profiling the user in the mid or long term. So, a privacy-preserving mechanism is needed to enable users to be identifiable only when necessary or if they wish.

Location privacy is a special type of information privacy which concerns the right of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others (Duckham & Kulik, 2006). Control of location information is a key concern in location-based privacy; making it fundamental to this research due to recent developments in mobile learning that has seen the adoption of high power, location-aware mobile gadgets like smart phones and iPad in distance education.

2.3. Accelerators of mobile learning insecurity

Data security is a fundamental concern when mobile learning is considered. It is a common believe that mobile devices are not a secure means of transferring and storing confidential information and data (Shohola & Joy, 2016). A number of threats to m-learning security exist. First is mobile malware which is any type of malicious software that is specifically targeted toward smartphones, tablets and other mobile devices. The

large and constantly growing smartphone user base has made mobile malware an enticing hobby to hackers. Hackers compromise mobile devices by inserting malware into mobile apps, often free apps that users then download and install. Once an app with malware has been installed, hackers can steal private information from the device, install other apps or open "backdoors" on the device, allowing them to take remote control of the device at a later time (Ivec, 2015). The authors argue that, the average smartphone user downloads over 100 applications. Out of 4 million Android applications that were analyzed by the Webroot Threat Research Team, 42% of those applications were malicious, unwanted or suspicious, 14% were untrustworthy, 6% showed moderate risk and only 38% were benevolent.

Also, Mobile Security Report (2016) indicates that: 1).10.8% of all apps discloses sensitive data over the network; 2). 24.7 % of mobile applications have at least one high risk security flaw (issues that expose data that a malicious individual use to gather private, sensitive information and/or monitor a user's activity); and 3). 50.0% of popular apps send data to an ad network including but not limited to phone numbers, IMEI number (a unique identifier assigned to cellular devices), call logs, location coordinates, and more.

Wi-Fi hijacking or snooping is another way enabling hackers to intercept communications between smartphones and unsecured Wi-Fi hotspots, just as they can with desktop or laptop computers. This means that a hacker easily gain access to usernames, passwords and even credit card or classified institution information. Hackers

can exploit vulnerabilities when Bluetooth connectivity is turned on. For example, “bluebugging” allows a hacker to gain access to another user’s device through Bluetooth and control some of its functions, including making phone calls or sending text messages to premium numbers or eavesdropping on calls made by the user (Shonola & Joy, 2016).

Lastly, security deals with sensors that are installed on mobile devices (Ivec, 2015). Ideally, most mobile devices come with location tracking, Bluetooth, RFID and cameras built-in. These standard sensors are a new area for attack. Fourth is the threat due to constant mobile connectivity. Mobile devices have constant access to the Internet and other devices, which makes things easier for cyber criminals.

2.4. Mobile devices and m-learning location-based privacy

With increasing use of mobile devices and applications for storing or accessing personal and sensitive information, many users are not aware of the growing privacy threats in using these devices and many users are also not aware that some mobile apps are not so secure (Shonola & Joy, 2016). As more people use smartphones and tablets for their educational activities, the more attractive these devices and their applications become targets to attackers with malicious intents. More worrying is that a popular platform like Android provides a comfortable environment to exploit and propagate security attacks (Russello *et al.* 2011). Conversely, to mitigate the attacks, Android developers are integrating privacy mechanisms and features that allow protection of users from malicious apps.

However, lack of awareness on mobile devices and m-learning location-based privacy is concerning as many learners considers privacy as unimportant until an issue arises (Shonola & Joy, 2014). For instance, despite the fact that PINs and passwords are the most widely used methods of authentication on mobile devices, a number of studies indicate that many mobile users are either unaware of, or do not bother to use these security features (Kurkovsky & Syta, 2010). Even when they use them, it is particularly worrying that many users reuse the same username and password for different applications. Hence, a compromise of a user's credentials for one app, easily lead to the compromise of another.

2.5. Location-based Privacy and M-Learning usage Intention

This section presents a case to justify that location-based privacy is worth protecting through a description of various identifiable goals for an ideal location privacy-preserving m-learning system. It also includes the challenges germane to location privacy and detailed description of probable effects of vulnerable m-learning location environment.

2.5.1. Learner's Location-based Privacy Goals

One of the areas of concern in location privacy preservation is user's identity. According to Duckham and Kulik (2006), hiding user's identity while keeping the position of the anonymous mobile object visible to clients is one of the possible goals to ensure privacy. The identity of a user can be her name, a unique identifier, or any set of properties uniquely identifying the user. If a user publishes position information without personal

information, an attacker can still try to derive the user's identity by analyzing the position information and additional context data such as the visited objects. In general, quasi-identifiers can be used to identify the user as shown in (Bettini *et al.*, 2005).

Another protection goal is to provide position information of a user only with a given precision to clients. For instance, a user might want to provide precise position information to his friends, while coarse positions with city-level granularity are provided to location-based news feed service. Generally, this goal is what is known as position obfuscation or cloaking discussed in (section 2.5.4). It is also worth considering that a user position usually carries more information than only geometric information like longitude and latitude values (Wernke *et al.*, 2008).

Usually, the semantic of a location defines the criticality of position information. For example, a user might be okay to share an exact position as long as he/she does not enter certain semantic locations such as a hospital, since this be used to derive further private information like the health status of the user. Therefore, a specific goal of protecting spatial information is the protection of semantic location information. In general, this is achieved by ensuring that a position is associated with several alternative locations of different semantics. For instance, a semantic position might be protected if the user is within a hospital or within one or more locations that are no hospitals (Damiani *et al.*, 2009).

Preserving temporal information is one other expectation that learners would want protected. Temporal information defines the point in time or time period when the

spatial information of the user is valid (Wernke *et al.,* 2008). In some scenarios, spatial information is only considered critical if it is associated with temporal information. For instance, a user might be willing to share with others where he is traveling, whereas, he does not want to reveal that he is speeding. This means that real-time updates cannot be used in this case without raising privacy concerns, whereas temporally delayed updates could be used to reach the protection goal. In such scenarios, it must be considered that even if temporal information is not explicitly stated e.g., as a timestamp of the position update, it can be implicitly derived. For instance, this is possible by knowing the time when the information was received by the LBS and by knowing the location update algorithm that produced the update. In general, the user might want to control the temporal resolution of his position or complete movement trace.

2.5.2. Challenges Germane to Unsecured Location Privacy

According to Duckham and Kulik (2006), key risks related to failure to protect location privacy within a location-aware computing environment include:

i. **Location-Based Spam:** Location can be used by unscrupulous businesses to bombard an individual with unsolicited marketing for products or services related to that individual's location. Location-based "spam" would lead to overload of an m-learning device which is already known to contain low processing power, eventually resulting to denial of service.

ii. **Personal Wellbeing and Safety:** Location is indivisibly linked to personal safety. Unrestricted access to information about an individual's location can

potentially lead to harmful encounters, for example stalking or physical attacks. Personal safety and wellbeing affect adoption in that, the moment learners would realize that their whereabouts can be easily tracked and the data obtained used to cause physical injury, and then many people will be unwilling to adopt m-learning system.

iii. **Intrusive Inferences:** Location constrains access to spatiotemporal resources, like meetings, medical facilities, homes, or even crime scenes. Location can therefore be used to infer other personal information about an individual, such as individual's political views, state of health, or personal preferences. Many people would want their information kept private and on occasions when their location data can be accessed and even more information deduced, it becomes a fundamental concern that hampers seamless adoption of m-learning in education.

2.5.3. Effects of Unsecured Location Privacy on M-Learning Adoption

A number of negative effects arise due to failure to protect location privacy within a location-aware computing environment. A porous location can be used by ruthless businesses to overwhelm an individual with unsolicited marketing for products or services related to that individual's location. These lead to overload of an m-learning device; which is already known to contain low processing power, eventually resulting to denial of service. Uncontrolled access to information about an individual's location, potentially lead to harmful encounters, like stalking or physical attacks. These affect adoption in that, the moment learners realize that their whereabouts can easily be tracked and data obtained used to cause physical injury, then few people will be willing to adopt

m-learning. Finally, open location access can lead to intrusive inferences. Since location constrain access to spatiotemporal resources, like meetings, medical facilities, homes, or even crime scenes. It can therefore be used to infer other personal information about an individual; it becomes a fundamental concern that hampers seamless adoption of m-learning in education.

2.6. Location Privacy Enhancing Technologies

In this section, the research identifies a number of approaches that can be harnessed to assure users and stakeholders that m-learning can be indeed secure and worth adopting. A critical analysis is done based on the prior described learners' goals in section 2.2.1. There are a number of works representing the state of the art techniques to protect location privacy (Chow & Mokbel, 2011; Krumm, 2009; Wang & Liu, 2009). Therefore, the goal of this section is to provide an overview of the fundamental principles of these approaches.

2.6.1. Anonymity

Anonymity involves the separation of information about an individual, such as location, from that individual's actual identity. Pseudonymity is a special type of anonymity where an individual is anonymous, but retains a persistent identity (a pseudonym) (Pfitzmann & K¨ ohntopp., 2001.). For instance, (Espinoza, *et al*., 2001) describe a location-aware system for allowing users to leave and read digital notes at specific locations ("geonotes"). One of the ways users can protect their privacy is to associate an alias (pseudonym) with a note in place of their real name (Duckham & Kulik, 2006).

Gruteser and Grunwald (2003), presents a spatial approach to providing anonymity in location-aware computing environments. The authors used a quad tree-based data structure to examine the effects of adapting the spatial precision of information about an individual's location according to the number of other individuals within the same quadrant, termed "spatial cloaking." Individuals are defined as k-anonymous if their location information is sufficiently imprecise in order to make them homogenous from at least k−1 other individuals. Additionally, the authors explore the orthogonal process of reducing the frequency of temporal information, termed "temporal cloaking."

According to (Duckham & Kulik, 2006), a number of disadvantages to using anonymity-based approaches exist. First, the approaches often rely on the use of a trusted anonymity "broker," which retains information about the true identity of a mobile individual, but does not reveal that identity to third party service providers. Second, anonymity often presents a barrier to authentication and personalization, which are required for a range of applications (Hong & Landay. , 2004). Pseudonymity does allow some personalization and is therefore sometimes preferred to general anonymity in order to combat this problem. Nevertheless, zero-knowledge interactive proof systems are a promising new research direction that may help overcome these limitations.

The idea of a zero-knowledge proof is to prove the knowledge of a certain fact without actually revealing this fact (Duckham & Kulik, 2006). Zero-knowledge proofs (ZKPs) involve **a prover**, who attempts to prove a fact, and **a verifier**, who certifies the prover's proof. The verifier may determine the correctness of the proof, but does not learn how to

prove the fact or anything about the fact itself. In a ZKP, a prover may provide the correct response to a challenge purely by chance. To combat this possibility, there are usually several rounds of challenges and responses in a ZKP. As the number of rounds increases, the probability that the prover will give the correct answer in every round decreases. Typical ZKPs will verify a proof with a probability of $1-1/2^n$, where n is proportional to the number of rounds used (Duckham & Kulik, 2006).

Anonymity-based system for location privacy is faced by a number of problems, key to that being the ability to infer a person's identity from his or her location. According to Duri *et al* (2002), anonymity strategies are vulnerable to data mining. Moreover, a study by (Beresford and Stajano (2003) to investigate ways of subverting anonymity-based privacy protection show how simple heuristics can be used to de-anonymize pseudonyms, providing users with much lower levels of location privacy than expected. Therefore, anonymity does not mitigate privacy concerns, perceived privacy risks and has reduced trust levels; so alone anonymity does provide total location privacy protection.

2.6.2. Position Dummies

The goal of position dummies is to secure a user's actual position by sending multiple false positions ("dummies") to the LBS together with the true position (Kido *et al*., 2005). An essential advantage of this approach is that the user herself can generate dummies without any need for other TTP components. However, it is challenging to create dummies which cannot be distinguished from the true user position, in particular,

if an adversary has additional context information such as a map and can track the user for longer times.

A proposal by Shankar *et al.*, (2009), presented an advanced method to generate dummies is presented in the SybilQuery approach. The approach assumes that the user has a database of historic traffic which allows him to create additional dummy positions that cannot be distinguished from the real user position.

2.6.3. Cryptography-Based Approaches

These approaches use encryption to protect user positions. According to Mascetti et al. (2010)'s proposal, their approach was able to notify users when friends are within their proximity without revealing the current user position to the LBS. Consequently, the authors assume that each user shares a secret with each of his buddies and use symmetric encryption techniques. Ghinita et al. (2008), proposed approaches that make use of the private information retrieval (PIR) technique to provide location privacy. By using PIR, LBS can answer queries without learning or revealing any information of the query. The used PIR technique relies on the quadratic residuosity assumption, which states that it is computationally hard to find the quadratic residues in modulo arithmetic of a large composite number for the product of two large primes (Ghinita et al, 2008).

The basic idea of this approach is to divide position information into shares, which are then distributed among a set of (non-trusted) LBSs. In order to recover positions, the client needs the shares from multiple servers. The advantage of this approach is that compromised LBS cannot reveal any position information since it does not have all the

necessary shares. However, in this approach LBSs cannot perform any computations on the shares, for instance, performing range queries. Generally, cryptographic approaches raise the question of whether location-based queries such as nearest-neighbor-queries or range-queries can be done efficiently over the encrypted data.

2.6.4. Obfuscation

This is the process of degrading the quality of information about a person's location, with the aim of protecting that person's location privacy. The term "ob-fuscation" is introduced in (Duckham & Kulik, 2005), but a number of closely related concepts have been proposed in previous work. The "need-to-know principle" aims to ensure that individuals release only enough information that a service provider needs to know to provide the required service (Hutter et al, 2004). The idea of a need-to-know principle is closely related both to obfuscation and the fundamental fair information practice principle of consent and use limitation

Worboys and Duckham (2004) emphasizes on the distinct mechanisms available in literature for degrading the quality of location information: inaccuracy, imprecision, and vagueness. Inaccuracy concerns a lack of correlation between information and reality; imprecision concerns a lack of specificity in information; vagueness concerns the existence of boundary cases in information. The authors assert that any combination of the three mechanisms maybe used as the basis for an obfuscation system. An inaccurate description of an agent's location means that the agent's actual location differs from the conveyed location. An imprecise description of location might be a region including the

actual location. A vague description would involve linguistic terms, for example that the agent is “far” from a certain location. According to Duckham and Kulik (2005; Gruteser and Grunwald (2003), most recent research seem to use imprecision to degrade the quality of location information.

Obfuscation has several fundamental advantages that complement the other privacy protection strategies. Obfuscation and anonymity are similar, in that both strategies attempt to hide data in order to protect privacy. The crucial difference between obfuscation and anonymity is that while anonymity aims to hide a person’s identity, obfuscation is an explicitly spatial approach to location privacy that aims to allow a person’s identity to be revealed. Potentially, this combats one of the key limitations of anonymity approaches: the need to authenticate users. At the same time, degrading the quality of location information makes inferring identity from location more difficult. Obfuscation is flexible enough to be tailored to specific user requirements and contexts, unlike regulatory strategies; does not require high levels of complex infrastructure and is less vulnerable to accidental disclosure of personal information, unlike privacy policies; and is lightweight enough to be used without the need for trusted privacy brokers, unlike many anonymity approaches.

Even though current research indicates existence of many situations where there are possibilities of getting high quality location-based services based on low quality positional information (Duckham & Kulik, 2005); obfuscation aims at achieving a balance between the level of privacy of personal information and the quality of service

of a location-based service. Consequently, in situations where the user requires a higher quality of service than can be achieved at a user's minimum acceptable level of privacy, then other privacy protection strategies must be relied upon instead. In addition, obfuscation assumes that the individual is able to choose what information about his or her location to reveal to a service provider.

2.7. Empirical Review

According to Kambourakis (2013), issues of security and privacy in m-learning realm are expected to be quite different from those confronted in legacy e-learning systems. These authors argue that the involved parties may be worried about the use of sensitive personal data collected indirectly such as mobile phone number, IP address, location data, International Mobile Equipment Identity (IMEI), unique phone ID, and so forth. Similar concerns, but for security, apply to usual learning activities like those of e-examination which may be totally uncontrollable under the m-learning setting.

Responding to the aforementioned needs, several studies have identified security and privacy issues, especially for the m-learning ecosystem as worth looking into. As a result, Kambourakis (2013) asserts that, to effectively fulfill security and privacy requirements in this dynamic computing environment, choices regarding security must take into account the user's different contextual attributes which may vary frequently and rapidly. For instance, in terms of access control this means not only regulating users' permissions on-the-fly, but also the policies based on contextual data.

Implementing a secure and trusted m-learning system is a major issue in applications and systems where information sharing is needed (Mahalingam, 2012). Their claims that, such systems should prevent data loss or corruption and that security is lacking on all major platforms, are backed by the upsurge in number of applications infected with malware that raised from 80 to 400 between January to June 2011, as reported by ("Lookout Mobile Security" , 2011). On the same note, mobile threat has been found to be one of the top five threats grown substantially in the year 2011 as reported in ("SOPHOS Security Threat Report", 2012). In the report, more than 50 third-party applications on Google's Android Marketplace were infected with Trojan that was designed to gain administrative privileges over personal phone without user's permission.

Despite increased number of research proposing models for adoption of mobile technologies into learning, for instance the work by Liu (2010), few of these studies lack conclusive integration of privacy aspects and how it can influence m-learning adoption in institutions of higher learning. Until now, most m-learning advances have focused on course development, deployment and delivery, paying little attention to security and privacy. For instance, Martin *et al*., (2011) investigated the state-of-the-art in models and middleware that facilitates mobile and ubiquitous learning (u-learning) development, and established that further development is needed in the privacy and security field to build systems that guarantee user's rights. In several cases, security and privacy concerns have been downplayed, considered and conceptualized in a similar way as in the context of e-learning. It is with these

revelations that this research endeavored to propose a location-based privacy-preserving model as described in subsection 2.10.

2.8. Theoretical Background

Previous studies have proposed multiple models in bid to explain the adoption and usage of technology by individuals or organizations. Venkatesh *et al*. (2003) proposed the Unified Theory of Acceptance and Use of Technology (UTAUT) by integrating elements across eight major user acceptance models. The theories include: technology acceptance model (TAM), innovation diffusion theory (IDT), the motivational model, the theory of reasoned action (TRA), the theory of planned behavior (TPB), a model combining the TAM and TPB, the model of PC utilization and social cognitive theory. According to UTAUT, four key constructs determine technology usage intention and behavior: performance expectancy, effort expectancy, social influence and facilitating conditions.

Additionally, individual level factors (e.g., gender, age, experience and voluntariness of use) are suggested to moderate the impact of the key constructs on usage intention and behavior. The model accounted for 70% of the variance in usage intention, significantly greater than any of the extant user acceptance models when tested on the same data (Venkatesh *et al*., 2003).

According to UTAUT, facilitating conditions influence the usage of technology; and privacy concerns being a specific part of facilitating conditions, reflect a user's subjective views of service providers' information practices to prevent misuse of

personal information. Prior research on privacy has focused on what motivates or hinders personal information disclosure. Among the studies, the construct of privacy concerns is one that features most in information systems research.

The rational choice theory by Westin (1967), which advocate that human action is "rational" in character and those individuals will gauge the likely costs and benefits of any action and choose the course that maximizes overall rewards; is one of the hypotheses which may help predict individuals' tendencies to disclose personal information. Applying the rational choice perspective to the LBS context, we may interpret the information disclosure in LBS as a non-monetary exchange where consumers disclose their location information in return for value such as locatability and personalization provided by LBS providers. On the same note, this research attempts to develop and test a research model with contrary actors capturing a set of elements in which users make a delicate balance between privacy concerns, perceived risks , trust and privacy awareness that influence behavioral intentions to adopt m-learning system already embedded with LBS.

Consistently, this research follows the direction of technology adoption literature as described in Liao *et a.l*, (2011) and Zhou (2012) by specifying a model that directly captures several constructs of these authors. We bring onboard the construct of privacy awareness and investigate its impact on intention to use and its correlation with privacy concerns.

2.9. A Review of Extant Theoretical Models

2.9.1. The Learning Environment, Learning Processes and Learning Outcomes (LEPO) Framework (Phillips *et al.*, 2010)

In this case the authors conceptualize learning as having three components which are: Learning Environment (which facilitates learning), Learning Processes - the activities which are part of learning and Learning Outcomes -the knowledge, behaviors, skills or understanding which can be demonstrated. Two general actors interact with these three components, the student and the teacher.

This model is derived from, and encompasses, various models of learning as well as research about the characteristics of students and teachers. The LEPO framework, while inclusive of all aspects of learning, is largely pedagogically neutral, because it does not specify how students and teachers interact with learning environments, processes and outcomes. At the same time, it is a very broad framework, seeking to include other models and frameworks as subsets of the LEPO 'whole'. Additionally, in the context of privacy preservation, it is also found to lay deficient and cannot be relied upon to preserve learners' location privacy.

2.9.2. Examining the Impact of Privacy, Trust and Risk Perceptions beyond Monetary Transactions: An Integrated Model (Liao *et al.*, 2011)

This research was designed to build an integrated model from existing theories to examine the effect of privacy, trust, risk and related factors on two activities: online transactions and online privileged information searching. The differences in the

requirements for privacy and the accuracy of the provided personal information between the two activities were both found to have an effect on the privacy control opportunities that a consumer can exercise. The research majored on offering empirical evidence of privileged information searching, its antecedents and its relationship with online transactions. Whereas this research has borrowed a considerable number of constructs from this model, it does not offer a direct solution to location privacy, a gap we would want to fill.

2.9.3. A framework for Sustainable Mobile Learning in Schools (Ng & Nicholas, 2013)

This framework was created to explain the findings and actions of a three-year project investigating M-learning in a secondary school in Australia. It is based on a person-centered model involving leadership and management, teachers, students, technicians and community. The aim of the framework was to explore the varied influences on the sustainability of M-learning programme in schools using PDAs.

The model identified and majored on five components for sustainability of ICT in education which includes: economic sustainability, social sustainability, political sustainability, technological sustainability, and pedagogical sustainability. Therefore this model is seen to run deficient of both security and privacy factors that influence the intention to use m-learning systems.

2.9.4. Toward A Sustainable Deployment of M-learning: A conceptual Model in Higher Education (Abu-Al-Aish *et al.*, 2013)

The authors in this research aimed to develop and evaluate a sustainable M-learning deployment model for higher education with pre- and post-deployment stages. They identified critical success factors essential for successful deployment of m-learning systems. The identified factors for pre-deployment stage included: Cross Management Initiative, Awareness and Motivation, On-going technical support, Usability, and On-going M-learning Innovation. They identified the following factors for post-deployment: Quality of Service, continuous usability testing, Trust and Confidence, Availability and suitability of learning materials, collaborative learning, and achievement evaluation. The model was based on analysis of existing literature and results obtained from two of their previous studies (Abu-Al-Aish *et al*., 2011; Abu-Al-Aish *et al.* 2012), to determine the student readiness for mobile learning. This model just like the others described herein above does not present anything to do with location privacy of users of mobile equipment.

2.10. Location-Based Privacy Model proposition

The research focused on works by Liao *et al.,* (2011) and Zhou (2012) that proposed Perceived Risk, Privacy Concerns and Trust as factors influencing behavioral intention. This research added the concept of Privacy Awareness and endeavored to establish its impact on usage intention as well as its correlation with the aforementioned variables.

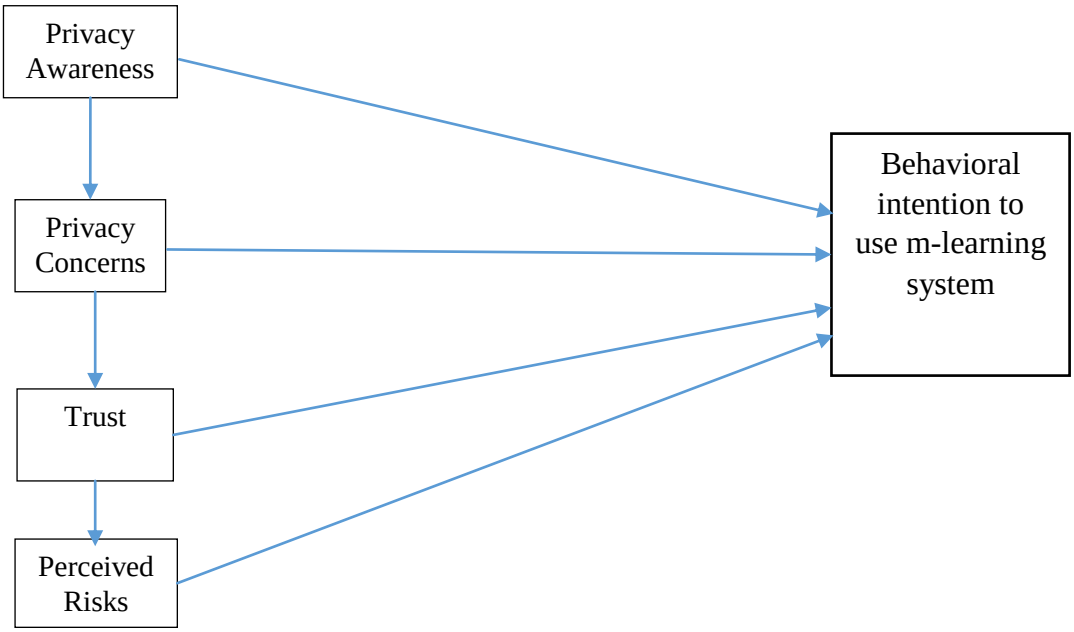


Figure2. 0 The Conceptual Model

2.10.1. Behavioral Usage Intention

This was the main variable of the research. Several studies have already asserted that behavioral intention is the fundamental determinant of actual behavior. Consequently, a number of literature reviews have listed numerous variables that act as factors influencing behavioral intention as shown in the listing by (Faruq & Hartini , 2013).

2.10.2. Privacy Awareness

Privacy awareness comes from the concept of social awareness, a passive involvement and raised interest in social issues like naming the problem, speaking out, consciousness raising and researching (Greene & Kamimura, 2003). On the same note, privacy awareness can be defined as the individuals' knowledge on the privacy risks, privacy concerns, privacy policies associated with the Internet, and the legal implications of privacy invasions and identity theft (Liao *et al.*, 2011).

Awareness of the effects of new technologies on individual rights to privacy have long been discussed in literature (Mason, 1986; Straub *et al.*, 1990). It is though unclear whether Individuals' perceptions and societal responses are highly attuned to the new and evolving dimension that location privacy presents and how difficult it were to affect those perceptions. The study by Dinev and Hu (2007) found that technology awareness led to positive user behavioral intention to use protective technologies against information security threats. Therefore, we believe that, in the same vein, privacy awareness might be associated with learner's behavioral intention.

Moreover, new studies indicate that user electronic privacy awareness is growing (GovTech, 2009). Also, many users of LBS are quite aware that there are privacy risks. However, most users do not understand how location data can potentially be used against them. For example, when an app requests access to the user's current location, will the app also identify them personally and tie that information to their location data? If so, the risks may be exponentially compounded. In this case, the user is not simply an anonymous person with a known location. Rather, it is Peter A. Doe, phone number 123-4567, email peter@doe.com, located at position x. However, the multiplied risk of this information may be lost on many users. Hence, a need to establish means to hide some if not all of these vital user's personal information identifiers.

Studies on factors influencing e-government adoption among Lebanese postgraduate students has found that awareness significantly influence behavioral intention (Charbaji & Mikdashi, 2003). A similar study by Rahman *et al*. (2012) confirmed these findings.

Other studies, on the relationship between independent variable and dependent variable as also found that awareness perfectly affects relationships between variables (Omar *et al.*, 2011).

2.10.3. Privacy Concerns

Privacy concerns indicate user concern on personal information disclosure (Li, 2011). This has since been conceptualized and operationalized by several studies in more detail: the Concern for Information Privacy (CFIP) instrument was developed by Smith *et al.(*2011), identified four dimensions of information privacy concerns: 1) collection reflected the concern that extensive amounts of personally identifiable data are being collected and stored in databases; 2) unauthorized secondary use reflected the concern that information is collected from individuals for one purpose but is used for another secondary purposes without consent; 3) errors reflected the concern that protections against deliberate and accidental errors in personal data are inadequate; and 4) improper access reflected the concern that data about individuals are readily available to people not properly authorized to view or work with data.

Current studies indicate that privacy concern has significant effects on user adoption of instant messaging (Lowry *et al.,* 2011), web-based healthcare services (Bansal *et al.,* 2010), electronic health records, software firewalls Kumar *et al.,* (2008) and ubiquitous commerce. Additionally, numerous extant studies have treated the construct of privacy concerns as a precursor to various behavior-related variables. Assertions by Dinev & Hart (2006), confirms that privacy concerns are generally considered as a cost of

adopting new technology. Consequently, there are high chances that similar effects can apply in the adoption of location-based systems for m-learning. Negative impact of privacy concerns on behavioral intention has been empirically supported in the e-commerce context (Chellappa & Sin, 2005; Malhotra *et al*., 2004). Similarly, the research expects a negative relationship between privacy concerns and behavioral intention in the context of LBS for m-learning.

In the context of e-commerce, Pan and Zinkhan (2006) argued that consumers are concerned about their privacy risks along with the collection or secondary use of personal information that they have not given consent to. Accordingly, rendering personal information to online organizations requires individuals to surrender a certain level of trust. Okazaki *et al,* (2009), found that privacy concerns were a significant predictor of trust and perceived risk in mobile advertising.

2.10.4. Trust

Trust has appeared in several prior research studies. It has been defined as the willingness of a party to be vulnerable to the actions of another party (Chow & Angie, 2006). It is the hope that an exchange partner will not engage in opportunistic behavior (Kim & Ahn, 2006). Finally, Pavlou *et al.*, (2007) asserts that trust is the willingness to depend and often includes three beliefs: ability, integrity and benevolence (Kim et al., 2008). Ability means that service providers have the knowledge and skills to fulfill their tasks whereas, integrity denotes that service providers keep their promise and do not deceive users. While benevolence signifies that service providers care about users'

interests and not just their own benefits. Trust may directly facilitate usage intention as it ensures that users develop positive outcomes in future. In addition, trust may mitigate perceived risk. When users develop trust in service providers, they believe that service providers have ability and integrity to protect their personal information from risks. Extensive research has shown the effect of trust on behavioral intention and perceived risk (Beldad *et al.*, 2010; Luo *et al.*, 2010).

2.10.5. Perceived Risks

Perceived risk theory has been widely applied to commerce-related IT innovations in recent years, in which consumers' behavior of IT adoption is viewed as an instance of risk-taking (Liu et al, 2012). For example, (Lee, 2009) employs five sub-dimensions of perceived risk in studying Internet banking adoption, including performance, social, time, financial and security risk. However, little prior work has explored how perceived risk of location privacy predicts the intension to use and the adoption thereof of m-learning systems. According to Gupta *et al.* (2010), and Glover and Benbasat (2011), comparing positive effect of trust on usage intention, perceived risk may negatively affect usage intention. This is for the sole reason that when users anticipate negative outcomes in future, they might become reluctant to adopt and use m-learning systems that are already location-aware.

2.11. Contribution of this Research

This research was designed to build a model germane to location-based privacy derived from existing theories to examine the effects of antecedent variables on the intention to

use m-learning systems. The model's verification with or without moderating variables lend the research both a theoretical and practical contributions. This becomes the first research to critically analyze location-based privacy constructs that includes privacy awareness, privacy concerns, trust and perceived risk and their ability to or otherwise influence usage intention.

2.12. Gaps in Existing Literature

Even though, several studies have proposed models for adoption of mobile learning technologies; few have integrated location-based privacy aspects and their influence on m-learning usage intention into distance learning. Therefore, location privacy is worth considering as such concerns hamper seamless penetration of mobile technologies into higher education. A considerable gap exists on the effort to determine the effects of location privacy awareness on usage intention as well as its correlation with privacy concerns. It is therefore the endeavor of this research to establish a location-based privacy-preserving model that can be used to evaluate user location privacy aspects in m-learning domain.

2.13. Summary

This chapter presented in-depth descriptions of key concepts, thorough research of existing models and a careful identification of important privacy enhancing technologies. It also proposed a location-based privacy model for m-learning adoption based on empirical evidence identified from extant studies.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

The previous chapter reviewed the literature on privacy of distance education offered through mobile equipment culminating into a proposition of gaps in existing studies. This chapter covers the research design and methodology adopted in this research.

3.2 Research Design

According to Mugenda and Mugenda (2008), research design is the overall plan of conducting the research in order to answer the research questions and achieve the objectives of the research. The research adopted quantitative design approach. This method was chosen because of its particular value to establish topic-related occurrences, trends, comparisons and statistical relationships (Thietart, 2007). The viewpoints of the respondents were significant in relation to the purpose of the research. Fraenkel and Wallen (2009), state that, the survey as a method of inquiry was of particular worth for scientific investigation to gather specific information on a certain topic. In addition, it presents valuable numerical or quantitative explanations of trends, approaches, and/or perceptions of a study by investigating a sample of the population (Creswell, 2009). Surveys in research were used to gather specific information at certain points in time amongst certain group within a population to assess the nature and/or manifest existing situations or conditions (Cohen *et al.*,2008).

3.3 Target Population

The target population for this research comprised of students enrolled for open and distance learning at Kenyatta University's Digital School of Virtual and Open Learning. More specifically, the research focused on the students on their second semester as this level consisted of learners with considerable experience in the mode of study.

3.4 Sampling Technique

The research used Simple Random Sampling technique for its ideal applicability when the population members are similar on important variables and also its ability to ensure high degree of representativeness (Hawaii, 2015). The research used the Yamane (1967) formula to formulate the appropriate sample size. This formula is 95% reliable with less than 5% deviation factor.

Figure 3.0 Formula for Calculating Sample Size

$$n = N / [1+Ne^2]$$

Where,

e=Deviation of sampling

n=Sample Size

N=Size of Population

Therefore, taking a population size of 2100 as the number of students enrolled for online distance learning using mobile gadgets in this university at the time of research, the sample size was obtained as follows:

e=0.05

N=2100

n= 2100/ [1+2100*0.05^2]

=336

The resultant sample size of 336 was fully representative of the total population (Yamane, 1967; Hawaii, 2015)

3.5 The Instruments

This research employed a structured questionnaire to collect data. Walliman (2011), asserts that asking questions is one of the basic research techniques for collecting both quantitative and qualitative structured information from people. Questionnaires are usually designed for specific research and to collect numerous kinds of data, like people's opinions or patterns of attitude. The questionnaire is a flexible tool, both financially and time efficient, and enables getting large number of participants without having to talk to everyone.

3.6 Data Collection

Considering the sampling technique described above (section 3.3), 336 structured questionnaires were administered to both undergraduate and postgraduate students using an email link. The questionnaire developed based on previous similar studies consisted of two parts. The first part was to collect respondents' demographic data, and the second part dealt with their perceptions about awareness of privacy matters, location

privacy concerns, trust, and risk perceptions. These research constructs were measured using previously validated instruments. Excluding demographic questions, all items were based on a 5-point Likert scale (1 for strongly agree and 5 for strongly disagree).

3.7 Pilot Testing

Pilot testing was carried out in another population with similar characteristics where 20 students were used. Pretesting of the instrument enabled the research to access the clarity of the instrument and its ease of use. According to Mugenda and Mugenda (2003), pre testing allows errors to be discovered as well as acting as a tool for forming a research team before the start of actual data collection.

They further argue that effective revision is the result of determining participants interest, discovering if the questions have meaning to the participant, checking for participant modification of questions intent, examining question continuity and flow, experimenting with question sequencing patterns, and fixing the length and the timing of the instrument.

3.7.1 Validity Test

Validity is a measure of how well a test measures what it is supposed to measure (Kombo & Tromp, 2006). According to Best and Khan (2009), a test is said to be valid to the degree that it measures what it claims to measure. The validity of the research instrument was established through consultation with the research supervisors.

3.7.2 Reliability Test

Kombo and Tromp (2006) define reliability as the measure of how consistent the results from a test are. Mugenda and Mugenda (2003) define it as a measure of degree to which research instruments give consistent results after repeated trials. Reliability measures the stability of research instruments across two or more attempts.

In this research, Cronbach Coefficient Alpha was used to test the reliability of the questionnaire. Cronbach Alpha is the measure of squared correlation between observed scores and true scores. This attribute of the instrument is referred to as stability where the results are similar.

3.8 Measurement Model

This research adopted the PLS measurement model that is usually assessed according to three tests: reliability, convergent validity, and discriminant validity (Hair *et al*., 2013). Reliability was evaluated via factor loading, Cronbach's α, and composite reliability (CR) (Hair *et al.*, 2013). Factor loadings of all constructs were tested to establish if they are above the threshold of 0.7, to indicate sufficient item reliability (Fornell & Larcker, 1981). Also the measure of Cronbach's α and CR were assessed to affirm that they were higher than the recommended 0.7 thresholds for sufficient reliability. For convergent validity, Fornell and Larcker (1981) suggested that the value of average variance extracted (AVE) of at least 0.5 reveals sufficient convergent validity. As per this criterion, the constructs used in this research were measured to determine whether they demonstrate sufficient convergent validity. Furthermore, the inter-construct correlations matrix was done to determine whether the square root of AVE

for each construct be larger than the correlation of the specific construct with any other constructs in the model, to indicate adequate discriminant validity (Fornell & Larcker, 1981). Positive test results be indicating model validity.

3.9 Data Analysis

3.9.1 Qualitative Data

To answer this research's first question, data was analyzed by identifying themes and patterns available from the respondents, which were then further organized into coherent categories. The patterns and connections within and between categories were then identified. Interpretation of the data was finally done to attach meaning and significance to the analysis.

3.9.2 Quantitative Data

The data analysis involved editing, classification and cross tabulation of the collected data. Further analysis using descriptive and inferential analysis procedures, with the aid of Statistical Package for Social Sciences (SPSS v20) software and WarpPLS5.0 as analytical tools was used. Inferential analysis was also achieved using Pearson Correlation Coefficient. The research also used pseudo F-test (f^2 effect size), which allows a scholar to evaluate the independent variable's incremental explanation of a dependent variable and the hardly used by extant studies Stone's (1974) and Geisser's (1974) cross-validated redundancy measure Q^2, which allows for assessment of the model's predictive relevance (Ringle *et al.*,2012).

3.10 Summary

This chapter presented the research design and methodology adopted for the research. A justification of sample size used is also given and a description of the measurement model. The next chapter covers the actual analysis of the data findings.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

4.1 Introduction

This research aimed at developing and validating location-based privacy-preserving model based on the perception of learners usage of location aware mobile learning systems for distance education. An online survey based on Google Docs was developed comprising of two main sections. The first section captured the personal information and demographics of the respondents while the second section was used to obtain respondents' perceptions on location-based privacy for m-learning. Research items in the second section were further grouped into two thematic groups to aid in meeting the research's objectives. The first group comprised of research items numbered 1 to 6 that resulted to qualitative data, while the second group had the items numbered 7 to 21 that resulted to quantitative data; later used to develop and validate the model. The Likert scale of (1=Strongly Agree, 2=Agree, 3=neither Agree nor Disagree, 4= Disagree, 5=Strongly Disagree) was used.

4.2 Data Collection and Sample Characteristics

The URL link was sent by e-mail to 336 University students registered for Distance Learning, and replies were obtained from 323 learners, representing 96.13% respondents of which 277 were valid. The demographic characteristics of the sample are shown in Table 4.0

Table 4.0 Demographic Distribution

		Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Centre	Nairobi	17	6.1	6.1	6.1
	Nakuru	95	34.3	34.3	40.4
	Kisumu	24	8.7	8.7	49.1
	Mombasa	3	1.1	1.1	50.2
	Kericho	2	.7	.7	50.9
	Kakamega	9	3.2	3.2	54.2
	Garissa	74	26.7	26.7	80.9
	Embu	53	19.1	19.1	100.0
Course	Diploma in I.T	52	18.8	18.8	18.8
	Diploma Project Management	56	20.2	20.2	39.0
	Diploma in Disaster Management	30	10.8	10.8	49.8
	BCOM	74	26.7	26.7	76.5
	BSC. I.T	21	7.6	7.6	84.1
	MSc. Records Management & Archiving	40	14.4	14.4	98.6
	Bachelor of Science	4	1.4	1.4	100.0
Level of Study	Diploma	102	36.8	36.8	36.8
	Undergraduate	135	48.7	48.7	85.6
	Postgraduate	40	14.4	14.4	100.0
Year of Study	Year 1	138	49.8	53.9	53.9
	Year 2	114	41.2	44.5	98.4
	Year 3	25	9.0	1.6	100.0
Age Group	18-24 years	35	12.6	12.6	12.6
	25-30 years	16	5.8	5.8	18.4
	31-35 years	24	8.7	8.7	27.1
	36-40 years	86	31.0	31.0	58.1
	41-45 years	1	.4	.4	58.5
	46-50 years	115	41.5	41.5	100.0
Gender	Male	161	58.1	58.1	58.1
	Female	116	41.9	41.9	100.0

The respondents in this research were found to be evenly distributed from various regions across the country, where the institution had centers implementing distance learning. It was though notable that, there were higher respondents from Nakuru, Garissa, and Embu with a frequency of 95, 74 and 53 respectively. Centers in Kericho and Mombasa recoded minimal number of respondents of 2 and 3 respectively as shown on Table 4.0. The research also found that higher number of respondents were those doing a bachelor of commerce (BCOM) course, followed by Diploma Project Management, then Diploma in I.T by a frequency of 74,56 and 52 respectively.

On the level of study, higher numbers were from the undergraduate respondents followed by diploma and then by postgraduate with a frequency of 135,102 and 40 respectively. On the year of study, the first years recorded higher numbers (138), followed by the second years (114) and lastly the third years (25). On the age group category, 46-50 years had higher numbers (115), while 41-45 years recorded minimal (1). Finally, the male gender recorded higher numbers followed by female with 161 and 116 respectively.

4.3 Data Analysis and Findings

To analyze questionnaire data, the research used statistical Package for Social Scientists (SPSS) version 20. Excerpts from SPSS are presented in tabular format and thereafter discussed for clarity. Keen interest was put on how the respondents answered key questionnaire items influencing the overall theme of the research. In this subsection the survey items were contextualized to suite the m-learning research theme of location

privacy whose definition was posed as a special type of information privacy which concerns the right of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others. The preceding tables help analyze the findings, item by item.

Table 4. 1 How important is location privacy to you?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very important	90	32.5	32.5	32.5
	Important	118	42.6	42.6	75.1
	Not Important	69	24.9	24.9	100.0
	Total	277	100.0	100.0	

On one hand, many respondents viewed that location privacy was important to them. This is seen with higher cumulative percentage of 75.1 as shown on Table 4.1. On the other hand, higher number of respondents recorded that their location privacy had been breached at some point in time as shown with a frequency of 151 of those that said YES in Table 4.2.

Table 4. 2 Has your location privacy been breached before?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	151	54.2	54.2	54.2
	NO	44	16.1	16.1	70.3
	NOT SURE	82	29.7	29.7	100.0
	Total	277	100.0	100.0	

Higher numbers of respondents claimed that "*Theft of mobile device with sensitive data and Data Interception*", were the main issues of concern on the privacy aspects they had while using mobile devises for learning. This is evident by the record 119 of respondent frequency in Table 4.3.

Table 4. 3 What are the privacy aspects you may have when using mobile devices for learning?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	"Theft of mobile device with sensitive data, Data Interception"	119	43.0	43.0	43.0
	"Theft of mobile device with sensitive data, Unauthorized access to mobile device, Denial of Service"	7	2.5	2.5	45.5
	"Theft of mobile device with sensitive data, Unauthorized access to mobile device"	30	10.8	10.8	56.3
	"Theft of mobile device with sensitive data, Virus / Malware attack, Data Interception, Denial of Service"	40	14.4	14.4	70.8
	"Theft of mobile device with sensitive data, Virus / Malware attack, Data Interception, Unauthorized access to mobile device, Denial of Service"	4	1.4	1.4	72.2
	"Theft of mobile device with sensitive data, Virus / Malware attack, Data Interception"	63	22.7	22.7	94.9
	"Virus / Malware attack, Unauthorized access to mobile device"	14	5.1	5.1	100.0
	Total	277	100.0	100.0	

Table 4. 4 What do you think are the damaging effect(s) of mobile learning location privacy threats to the learners?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	"Loss of confidential information, Denial of Service, Loss of control (e.g.over online assessment), Loss of content quality"	40	14.4	14.4	14.4
	"Loss of confidential information, Denial of Service, Loss of study hours (e.g. due to downtime)"	14	5.1	5.1	19.5
	"Loss of confidential information, Loss of content quality"	30	10.8	10.8	30.3
	"Loss of confidential information, Loss of control (e.g.over online assessment), Psychological damage"	7	2.5	2.5	32.9
	"Loss of confidential information, Loss of control (e.g.over online assessment)"	45	16.2	16.2	49.1
	"Loss of control (e.g.over online assessment), Loss of content quality, Loss of study hours (e.g. due to downtime)"	74	26.7	26.7	75.8
	"Personal Safety due to Intrusive inferences, Denial of Service, Loss of control (e.g.over online assessment), Psychological damage"	6	2.2	2.2	78.0
	"Personal Safety due to Intrusive inferences, Loss of confidential information, Denial of Service, Loss of content quality"	21	7.6	7.6	85.6

On one hand "*Loss of control like in online assessment, Loss of content quality, Loss of study hours (e.g. due to downtime)",* featured as the main threat to learners on location mobile learning by recording a higher frequency of 74 as shown in Table 4.4. On the other hand *"Loss of goodwill / integrity, Loss of person's hours",* was found to be having more damaging privacy effects on Higher Education Institutions implementing mobile learning going by the higher respondents of 81 in Table 4.5.

Table 4. 5 What do you think are the damaging effect(s) of mobile learning privacy threats to the Higher Education Institution?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	"Loss of confidential information, Loss of goodwill / integrity, Loss of person's hours"	46	16.6	16.6	16.6
	"Loss of confidential information, Loss of goodwill / integrity, Loss of reliability, Loss of person's hours"	4	1.4	1.4	18.1
	"Loss of confidential information, Loss of goodwill / integrity, Loss of reliability"	21	7.6	7.6	25.6
	"Loss of confidential information, Loss of reliability, Loss of person's hours"	36	13.0	13.0	38.6
	"Loss of confidential information, Loss of reliability"	44	15.9	15.9	54.5
	"Loss of goodwill / integrity, Loss of person's hours"	81	29.2	29.2	83.8
	Loss of reliability	45	16.2	16.2	100.0
	Total	277	100.0	100.0	

The research found that among the methods used to assess mobile learning privacy threats, "*Report by users of unusual behavior of device and Frequency of Denial of Service*", were the most frequently used as recorded by a higher frequency of 111 in Table 4.6.

Table 4. 6 How do you think the mobile learning privacy threats or issues are assessed?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	"Frequency of Denial of Service, Log file analysis"	40	14.4	14.4	14.4
	"Report by users of unusual behavior of device, Frequency of Denial of Service"	111	40.1	40.1	54.5
	"Report by users of unusual behavior of device, System monitoring/Alert, Frequency of Denial of Service, Log file analysis"	4	1.4	1.4	56.0
	"Report by users of unusual behavior of device, System monitoring/Alert, Log file analysis"	27	9.7	9.7	65.7
	"Report by users of unusual behavior of device, System monitoring/Alert"	14	5.1	5.1	70.8
	"System monitoring/Alert, Frequency of Denial of Service, Log file analysis"	36	13.0	13.0	83.8
	Report by users of unusual behavior of device	45	16.2	16.2	100.0
	Total	277	100.0	100.0	

Respondents viewed it unnecessary for m-learning systems to disclose how their data are collected, processed, and used indicated by a higher frequency of 113 in Table 4.7. Additionally, many respondents appeared undecided on whether online privacy should have a clear and visible disclosure as shown by a higher frequency of 98 in Table 4.8

Table 4. 7 M-learning systems seeking information should disclose how data are collected, processed, and used.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	96	34.7	34.7	34.7
	Agree	66	23.8	23.8	58.5
	neither Agree nor Disagree	2	.7	.7	59.2
	Disagree	113	40.8	40.8	100.0
	Total	277	100.0	100.0	

Table 4. 8 Good learners' online privacy should have a clear and visible disclosure.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	66	23.8	23.8	23.8
	Agree	64	23.1	23.1	46.9
	neither Agree nor Disagree	98	35.4	35.4	82.3
	Disagree	49	17.7	17.7	100.0
	Total	277	100.0	100.0	

The research established that majority of respondents affirmed that it was important that they know how their personal information will be used. This is shown by cumulative percentage of 51.6 in Table 4.9. Likewise on Table 4.10, many respondents (cumulative percentage 97.8) expressed fear that the information collected by location aware m-learning systems be misused.

Table 4. 9 It is very important that I am aware of how my personal information will be used.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	98	35.4	35.4	35.4
	Agree	45	16.2	16.2	51.6
	neither Agree nor Disagree	104	37.5	37.5	89.1
	Disagree	30	10.8	10.8	100.0
	Total	277	100.0	100.0	

Table 4. 10 I am concerned that information collected by location- aware m-learning systems could be misused.

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly Agree	47	17.0	17.0	17.0
Agree	224	80.9	80.9	97.8
neither Agree nor Disagree	5	1.8	1.8	99.6
Disagree	1	.4	.4	100.0
Total	277	100.0	100.0	

The research also found that many respondents (cumulative percentage 98.4) feared the possibility of other people accessing their personal information from location-aware m-learning systems as shown on Table 4.11. On the same note, many respondents expressed anxiety that their personal information in m-learning systems could be used in a way that they do not foresee as shown by cumulative percentage of 69.7 in Table 4.12.

Table 4. 11 I am concerned that others can find my private information from location- aware m-learning systems

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	57	20.6	22.3	22.3
	Agree	195	70.4	76.2	98.4
	Disagree	4	1.4	1.6	100.0
	Total	256	92.4	100.0	
Missing	0	21	7.6		
Total		277	100.0		

Table 4. 12 I am concerned of my personal information in the m-learning systems as it could be used in a way that I do not foresee.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	68	24.5	28.2	28.2
	Agree	100	36.1	41.5	69.7
	neither Agree nor Disagree	69	24.9	28.6	98.3
	Disagree	4	1.4	1.7	100.0
	Strongly	36	13.0		
Total		277	100.0		

The research findings indicated that many respondents were optimistic that m-learning service providers keep learners' interests in mind as seen by cumulative percentage of 71.8 in Table 4.13. Similarly, higher number of respondents express higher disposition to trust in that m-learning service providers keep their promise on protecting their privacy as shown by cumulative percentage of 53.8 in Table 4.14. Consistently, accumulative percentage of 69.6 in Table 4.15, indicate a higher respondent number of those that supported the survey item that m-learning service provider is dependable in preserving learner's location privacy.

Table 4. 13 M-learning service provider keeps learners' interests in mind (i.e would not intentionally endanger learner's privacy)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	47	17.0	17.0	17.0
	Agree	152	54.9	54.9	71.8
	neither Agree nor Disagree	4	1.4	1.4	73.3
	Disagree	74	26.7	26.7	100.0
	Total	277	100.0	100.0	

Table 4. 14 M-learning service provider keeps its promise on protecting learners' privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	40	14.4	14.4	14.4
	Agree	109	39.4	39.4	53.8
	neither Agree nor Disagree	18	6.5	6.5	60.3
	Disagree	74	26.7	26.7	87.0
	Strongly Disagree	36	13.0	13.0	100.0
Total		277	100.0	100.0	

Table 4. 15 M-learning service provider is trustworthy in preserving learner's location privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	46	16.6	18.0	18.0
	Agree	132	47.7	51.6	69.5
	neither Agree nor Disagree	4	1.4	1.6	71.1
	Disagree	74	26.7	28.9	100.0
	Total	256	92.4	100.0	
Missing	0	21	7.6		
Total		277	100.0		

Higher respondents expressed reservations on the unforeseen outcomes due to providing m-learning service providers with personal information with cumulative percentage of 68.2 in Table 4.16.

Table 4. 16 Providing m-learning service provider with my personal information would involve many unexpected outcomes.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	93	33.6	33.6	33.6
	Agree	96	34.7	34.7	68.2
	neither Agree nor Disagree	14	5.1	5.1	73.3
	Disagree	74	26.7	26.7	100.0
	Total	277	100.0	100.0	

The research got an interesting finding after many respondents disagreed with the survey item as presented by a frequency of 110 in Table 4.17. Conversely, there was higher respondent's cumulative percentage of 55.2 agreeing to the survey item. In addition, many respondents saw high potential for loss in disclosing their personal information to m-learning service provider as shown by cumulative percentage of 52.0 in Table 4.18.

Table 4. 17 It would be risky to disclose my personal information to m-learning service provider

RISK2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	107	38.6	38.6	38.6
	Agree	46	16.6	16.6	55.2
	neither Agree nor Disagree	14	5.1	5.1	60.3
	Disagree	110	39.7	39.7	100.0
	Total	277	100.0	100.0	

Table 4. 18There would be high potential for loss in disclosing my personal information to m-learning service provider

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	93	33.6	33.6	33.6
	Agree	51	18.4	18.4	52.0
	neither Agree nor Disagree	74	26.7	26.7	78.7
	Disagree	59	21.3	21.3	100.0
	Total	277	100.0	100.0	

A considerably higher number of respondents strongly supported the survey item as presented in Table 4.19 with a higher frequency of 135. While a frequency of 53 agreed, 80 undecided, 8 disagreed and 1 strongly disagreed. Likewise, many respondents supported the survey item as shown in Table 4.20 with cumulative percentage of 98.2.

Table 4. 19 Given the chance, I intend to use location aware mobile equipment for learning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	135	48.7	48.7	48.7
	Agree	53	19.1	19.1	67.8
	neither Agree nor Disagree	80	28.9	28.9	96.7
	Disagree	8	2.9	2.9	99.6
	Strongly Disagree	1	.4	.4	100.0
Total		277	100.0	100.0	

Table 4. 20 I expect my use of location aware mobile gadget for learning to continue in the future.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	103	37.2	37.3	37.3
	Agree	168	60.6	60.9	98.2
	neither Agree nor Disagree	5	1.8	1.8	100.0
	Total	276	99.6	100.0	
Missing	0	1	.4		
Total		277	100.0		

The research also found that higher responds supported the survey item on the intention to use location aware mobile equipment for learning as shown by cumulative percentage of 71.8. Similarly, many respondents supported the survey item that protecting learners' location privacy will improve the sustainability of M-learning as shown by cumulative percentage of 95.2 in Table 4.22

Table 4. 21 I have intention to use location aware mobile equipment for learning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	98	35.4	35.4	35.4
	Agree	101	36.5	36.5	71.8
	neither Agree nor Disagree	78	28.2	28.2	100.0
	Total	277	100.0	100.0	

Table 4. 22 Protecting learners' location privacy will improve the sustainability of M-learning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	62	22.5	22.5	22.5
	Agree	191	71.9	71.9	95.2
	neither Agree nor Disagree	16	4.6	4.6	100.0
	Total	277	100.0	100.0	

Finally, the last survey item got high respondents support in that evaluating the effect of m-learning systems in meeting needs of learners' location privacy promotes sustainability as shown by cumulative percentage of 85.2 in Table 4.23.

Table 4. 23 To evaluate the impact of m-learning systems in meeting needs of learners' location privacy will promote sustainability.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	91	32.9	32.9	32.9
	Agree	145	52.3	52.3	85.2
	neither Agree nor Disagree	41	14.8	14.8	100.0
	Total	277	100.0	100.0	

4.4 Summary

In this chapter, a detailed data analysis was done revealing higher respondents from remote regions of the country, far from the main campus that is located in near the capital, Nairobi. Conversely, other centers like Mombasa recoded minimal number of respondents. Higher numbers were from the undergraduate followed by diploma and then postgraduate. The research found that data Interception was the main issue of concern for learners using mobile devises for learning, while Loss of goodwill / integrity was the main concern for Institutions of Higher Education implementing mobile learning. However, respondents disagreed with the survey item that stated m-learning systems to disclose how data are collected, processed, and used; adding that it was not important that learners know how their personal information will be used. The findings also indicated that many respondents feared the possibility of others accessing their personal information. Conversely, respondents were optimistic that m-learning service providers keep their interests in mind, while many others saw high potential for loss in disclosing their personal information to m-learning service provider.

Finally, many respondents were skeptical in disclosing their personal information to m-learning service provider due to high potential for loss. Respondents expressed high intention to use location aware mobile equipment for learning, agreeing that evaluating and protecting learners' location privacy advances sustainability. Therefore, there was need to develop a location-based privacy preserving model for m-leaning adoption to evaluate learners' behavioral intention to use location-aware systems.

CHAPTER FIVE

A LOCATION-BASED PRIVACY PRESERVING MODEL FOR M-LEARNING ADOPTION

5.1 Introduction

In section 2.9, the research described a number of extant theoretical models germane to location-based privacy, showing their pros and cons that informed the development of a new location-based privacy model as described in section 2.10. In this chapter, a location-based privacy-preserving model is presented to improve trust, mitigate both privacy concerns and perceived privacy risks; more importantly identify the effects of privacy awareness on learners' behavioral intention to use location-aware m-learning systems.

5.2 Statistical Model Analysis

Partial Least Squares (PLS) approach was adopted for statistical analysis in this research. PLS is a component-based approach for testing structural equation models. This approach has numerous advantages over its main alternative, Covariance-Based Structured Equation Modelling (CBSEM) as listed by (Urbach & Ahlemann, 2010) . The CBSEM on one hand is applicable for theory testing and is parameter-oriented hence, optimal for parameter accuracy. PLS on the hand is prediction-oriented, optimal for prediction accuracy; thus a more appropriate technique for theory development studies (Urbach & Ahlemann, 2010).

WarpPLS5.0 was used to test the measurement model and the structural model (Ringle *et al.* 2005). This software provides a powerful PLS-based SEM, easy to use with a step-by-step user interface guide among several other features. The software was selected due to its ability to handle complex reflective and formative models, giving the user the option to choose between them.

After a thorough research based on the research's objectives, a reflective model was adopted for this research. This is because the evaluation of formative measurement models give rise to concerns such as redundancy analysis and that PLS-SEM studies are usually build on satisfactory evaluations that ensure reliability and validity of the reflective measurement model construct (Ringle *et al.*, 2012).

5.3 Measurement Model

The measurement model fit was assessed by a confirmatory factor analysis (CFA). Ten common model-fit measures were used to estimate the model's overall goodness of fit as shown on Table 5.1. Prior to testing the psychometric validity of the measurement model, Harman's one-factor test was performed to assess the level of common method bias of all measurement items of every construct; following Podsakoff *et al.* (2003). The partial least squares (PLS) method of structural equation modelling (WarpPLS 5.0) was used for its ability to handle complex predictive models. Indicators that were found to load poorly were removed. The reliability of individual items, internal consistency between items and the model's convergent and discriminant validity was scrutinized to ensure appropriate measurement model.

5.4 Structural Model

In the structural model, also called inner model, the latent variables (LVs) are related with each other according to substantive theory. This research included this section to fill a gap left by many extant studies on prediction and model estimations that only use the coefficient of determination (R^2 values) to characterize the ability of the model to explain and predict the endogenous latent variables. According to (Ringle et al.,2012), few studies use pseudo F-test (f^2 effect size), which allows a scholar to evaluate the independent variable's incremental explanation of a dependent variable. These are calculated as the absolute values of the individual contributions of the corresponding predictor latent variables to the R-square coefficients of the criterion latent variable in each latent variable block. With these effect sizes users can ascertain whether the effects indicated by path coefficients are small, medium, or large. The recommended values are 0.02, 0.15, and 0.35; respectively (Cohen, 1988). Values below 0.02 suggest effects that are too weak to be considered relevant from a practical point of view, even when the corresponding P values are statistically significant; a situation that may occur with large sample sizes (Kock, 2015).

In addition, (Ringle et al.,2012) asserts that none of the studies in their findings use Stone's (1974) and Geisser's (1974) cross-validated redundancy measure Q^2, which allows for assessing the model predictive relevance (Wold 1982). In addition, changes in Q^2 allow assessing the relative impact of the structural model for predicting the observed measures of an endogenous latent variable by the q^2 effect size (Chin 1998b). According to Kock (2015), acceptable predictive validity in connection with an endogenous latent

variable is suggested by a Q-squared coefficient greater than zero. In accordance to Ringle *et al.,* (2012) who urges researchers to use statistical criteria such as f^2, Q^2, and q^2, the research incorporated these measures to make a stronger case for model predictive capabilities.

While assessing the pseudo F-test (f^2 effect size), warpPLS5.0 was run to provide an option of viewing both direct and indirect effects along with various paths making up the structural model. This research found that, the result supports a direct effect amongst all variables as shown emboldens in Table 5.1. The indirect effect was also significant to some variables.

Table 5.1: Effect sizes for total effects and Q-Squared

	AWARENESS	**CONCERNS**	**TRUST**	**RISK**	**INT_USE**
WARENESS					
CONCERNS	**0.256**				
TRUST	0.025	**0.011**			
RISK	0.003	0.006	**0.028**		
INT_USE	**0.114**	**0.029**	**0.175**	**0.033**	
Q-SQUARED		(0.259)	(0.022)	(0.028)	(0.399)

To assess the prediction quality, q^2, warpPLS5.0 was used and the result indicated a substantial prediction ability of this proposed model as shown the Table 5.1 (values are in brackets).

5.5 Model Fit Validation from Results

After the analysis process, the result of the model was as shown in Figure 5.1, clearly showing the path coefficients, necessary to determine model fit. In addition, the outcome was analyzed in tabular format to ease interpretation as shown in the preceding tables.

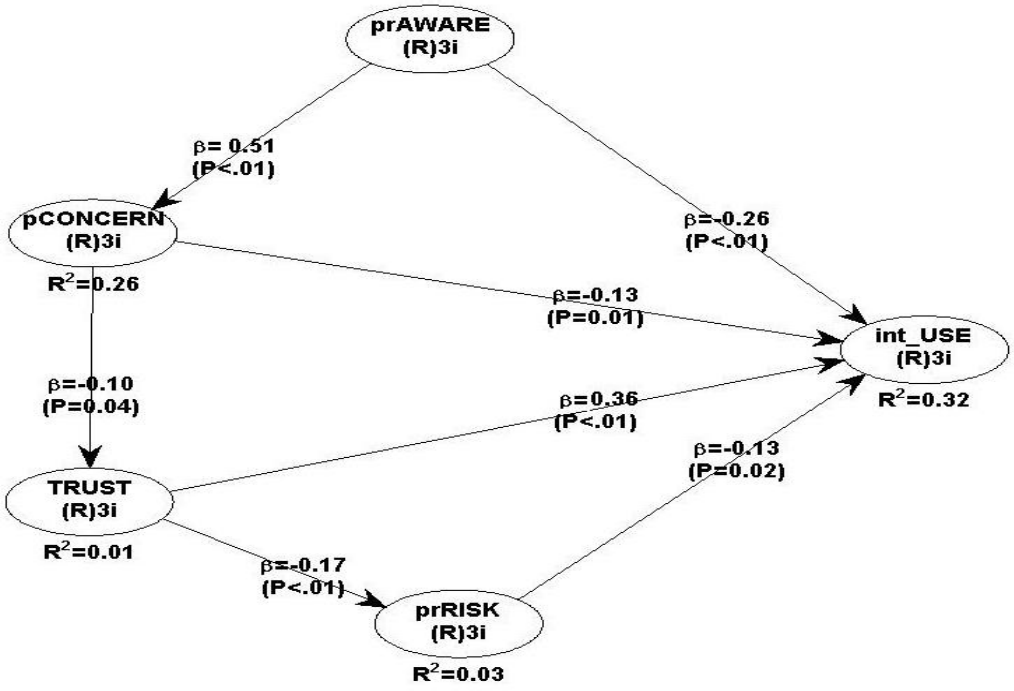


Figure 5.1: Results of PLS analysis

5.5.1 Model fit Quality Indices

To assess the model fit with the obtained data, it is recommended that the p-values for both the average path coefficient (APC) and the average r-squared (ARS) be both lower than .05 (Ned Kock 2009). In addition, the average variance inflation factor (AVIF) should be lower than 5. The table 5.2 show the results obtained.

Table 5.2: Model fit quality indices

	Values obtained	*Acceptable Values*
Average path coefficient (APC)	0.236	P<0.001
Average R-squared (ARS)	0.154	P<0.002
Average adjusted R-squared (AARS)	0.149	P<0.003
Average block VIF (AVIF)	1.460	<= 5
Average full collinearity VIF (AFVIF)	1.603	<= 5
Tenenhaus GoF (GoF)	0.283	small >= 0.1 medium >= 0.25 large >= 0.36
Sympson's paradox ratio (SPR)	0.857	>= 0.7
R-squared contribution ratio (RSCR)	0.944	>= 0.9
Statistical suppression ratio (SSR)	1.000	>= 0.7
Nonlinear bivariate causality direction ratio (NLBCDR)	0.714	>= 0.7

Table 5.2 above, provides the model fit indices with p values of the estimated model. It was found that, all the three major fit criteria, that is: the APC, ARS and AVIF were perfectly met and therefore, the model exhibited acceptable predictive and explanatory quality.

5.5.2 Discriminant Validity

It was also worth measuring the model's discriminant validity. This entailed computing the constructs' mean, standard deviation, composite reliability, average variance extracted (AVE), and square root of the AVE; and their correlations. According to Kock (2015), a measurement instrument and related dataset are considered to have acceptable discriminant validity if the square-roots of the AVEs for each latent variable are higher

than any of the correlations between that latent variable and other latent variables. To test the discriminant validity, the square root of AVE and factor correlation coefficients were compared. As listed in Table 5.3, for each variable, the square root of AVE was significantly larger than its correlation coefficients with other variables, suggesting good discriminant validity.

Table 5.3 Correlations among latent variables with sq. rts. of AVEs in Diagonal

N0.	constructs	N0. of Items	Mean	SD	Composite Reliability (CR)	AVE	Correlations				
							1	2	3	4	5
1	Privacy Awareness	3	2.03	0.82	0.804	0.588	**0.767**				
2	Privacy Concerns	3	1.73	0.79	0.734	0.417	-0.467	**0.646**			
3	Trust	3	1.75	0.86	0.719	0.461	0.484	-0.005	**0.679**		
4	Perceived Risk	3	1.77	0.83	0.753	0.504	0.359	-0.324	-0.11	**0.71**	
5	Intention to Use	3	1.64	0.72	0.828	0.635	-0.483	0.187	-0.28	-0.25	**0.797**

5.5.3 Reliability

As described in the research's methodology (section 3.7), the model's reliability was also worth considering. Table 5.3 was used to achieve this. The composite reliability (CR) measures were all greater than 0.71, above the recommended value of 0.7 for construct reliability (Bagozzi & Yi, 1988).

5.5.4 Convergent Validity

A satisfactory level of convergent validity was maintained since the AVE values of most of the constructs were above the suggested threshold value of 0.50 in Table 5.3.

Table 5.4 Indicator Loadings

Indicator	Privacy Awareness	Privacy Concerns	Trust	Perceived Risk	Intention to Use
AWARE1	**0.73**	-0.009	0.132	0.623	0.102
AWARE2	**0.776**	0.081	0.172	-0.17	-0.076
AWARE3	**0.864**	-0.092	-0.354	-0.448	-0.014
CONC1	-0.34	**0.986**	0.183	0.204	0
CONC2	0.074	**0.959**	-0.276	0.138	0.11
CONC3	0.49	**0.451**	0.268	-0.704	-0.247
TRUST1	0.136	-0.12	**0.897**	0.113	0.202
TRUST2	0.879	-0.1	**0.594**	0.116	-0.193
TRUST3	-0.563	0.162	**0.816**	-0.164	-0.094
RISK1	0.188	0.214	0.076	**0.877**	0.203
RISK2	0.064	-0.204	0.032	**0.807**	-0.397
RISK3	-0.2	0.002	-0.086	**0.947**	0.172
USE3	0.077	-0.018	-0.135	0.087	**0.885**
USE4	0.333	0.126	0.145	-0.46	**0.857**
USE5	-0.192	-0.023	0.095	0.06	**0.844**

Another aspect used to determine model fit is item loadings. The items area expected to load highly on related constructs than in any other. In general, higher factor loading is considered better, and usually loadings below 0.30 are not interpreted. As general rule of thumb, loadings above 0.71 are excellent, 0.63 very good, 0.55 good, 0.45 fair, and 0.32 poor

(Tabachnick & Fidell, 2007). In this research, the indicators loaded highly where they are supposed to load as shown in Table 5.4 (loadings shown in bold).

5.6 Discussion

This research was designed to develop a secure location-based privacy-preserving model from existing theories for m-learning adoption; to enhance distance education by evaluating learners' behavioral intention to use location-aware m-learning systems. Through literature review, the research identified perceived risk, trust, privacy concerns and privacy awareness as factors that influence learner's behavioral intention. Extant research has shown how privacy concerns, trust and perceived risk significantly influence online transactions (Liao et al, 2011). However, research regarding location privacy awareness and its combined effects with the fore-mentioned factors on behavioral intention was lacking; adding much complexity to the understanding of the perception-versus-behavior relationship for this online learning activity. This research offered some empirical evidence of location privacy awareness, privacy concerns, trust and perceived risk and their relationships with behavioral intention to use m-learning systems. The following graphs helps in discussing the results, case by case.

i. Relationship between Privacy awareness and privacy concerns

Privacy awareness is seen to positively relate to privacy concerns, a finding consistent with Dinev and Hart (2006). This implies that individuals who are aware of the possibility of their information being available by other parties and used without their explicit consent tend to exhibit more online privacy concerns as shown in figure 5.2.

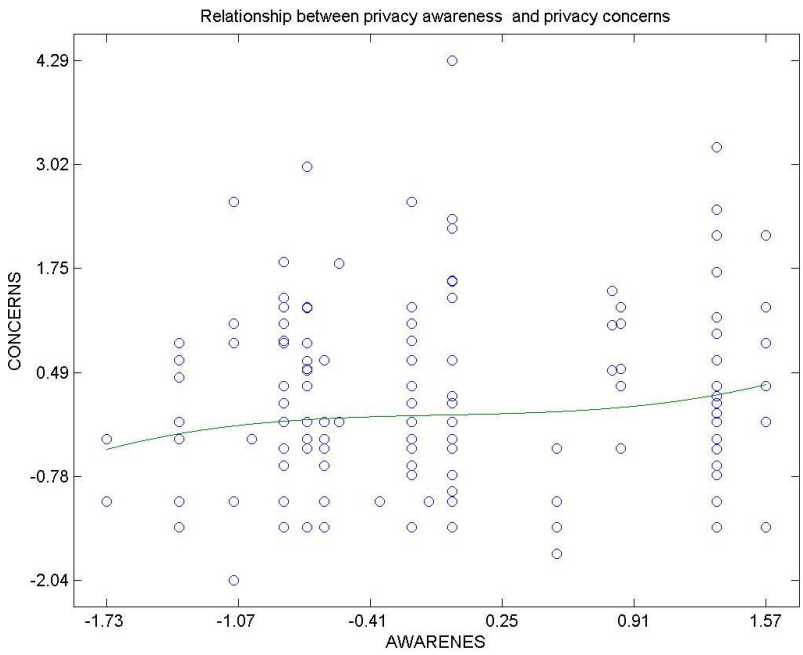


Figure 5.2: Relationship between Privacy awareness and privacy concerns

ii. Relationship between Privacy awareness and Intention to Use

The research discovered that new studies indicated growing user online privacy awareness, according to (GovTech, 2009). Also, it was found that many users of LBS are quite aware that there are privacy risks, of which majority do not understand how unprotected location data can potentially be used against them. In line to this, this research investigated learners' behavioral usage intention, should they know the effects of their unsecured location information. It was found that privacy awareness negatively relates to intention to use as shown in Figure 5.3.

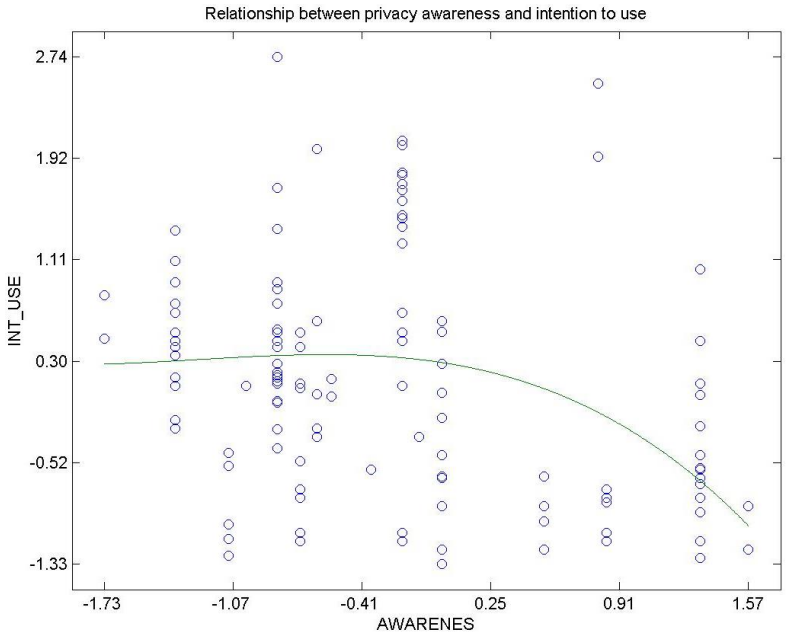


Figure 5.3: Relationship between Privacy awareness and Intention to Use

iii. Relationship between privacy concerns and Trust

Privacy concern reflects user concern on personal information disclosure willingly or personal information discovery unaware through location aware mobile systems. The results are consistent with extant findings by (Junglas & Watson, 2008; Bansal et al., 2010). If service providers cannot ensure that users' personal information is properly collected and used, users may lower their trust in service providers and increase their perceived risk. Users become worried about negative outcomes associated with information disclosure, such as information abuse (Zhou , 2012). Consistently, this research found that privacy concerns had significant effects on trust as shown in Figure 5.4. Thus service providers need to implement effective measures to reduce users' privacy concern perhaps through posting privacy policies to inform users about their

privacy practice on information collection, storage and usage. They can also present privacy seals issued by the authoritative third-party organizations to signal trustworthiness. In addition, they can apply advanced encryption technologies such as secure socket layer to ensure personal information storage security. With these measures, users' privacy concern may be mitigated and their trust be established.

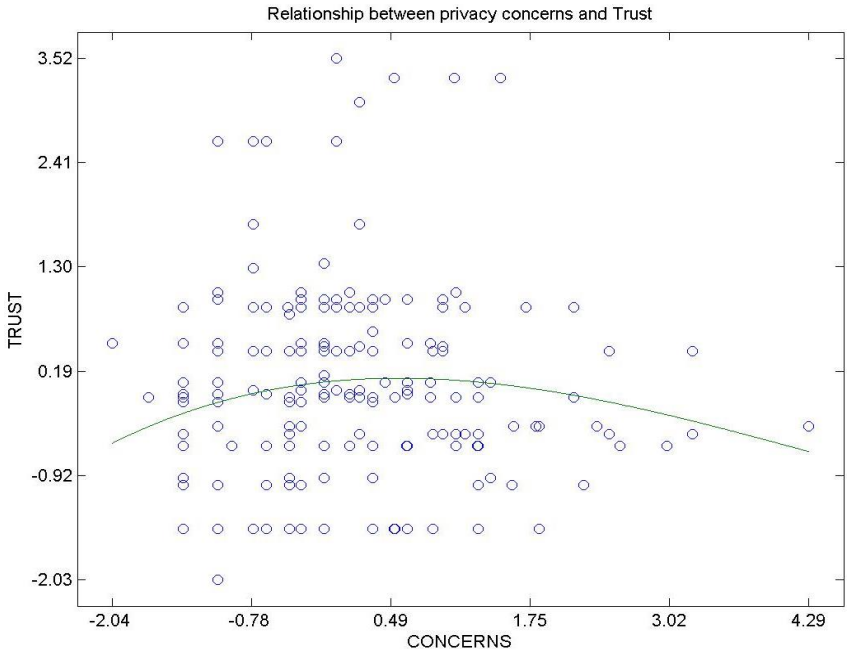


Figure 5.4: Relationship between privacy concerns and Trust

iv. Relationship between Trust and Perceived Risk

On the same vein, Trust was found to affect perceived risk, and both factors affect usage intention as shown in Figure 5.5. Trust provides a guarantee that users acquire positive outcomes in future (Gefen et al. 2003). Consistent with extant studies, trust is seen to lower perceived risk.

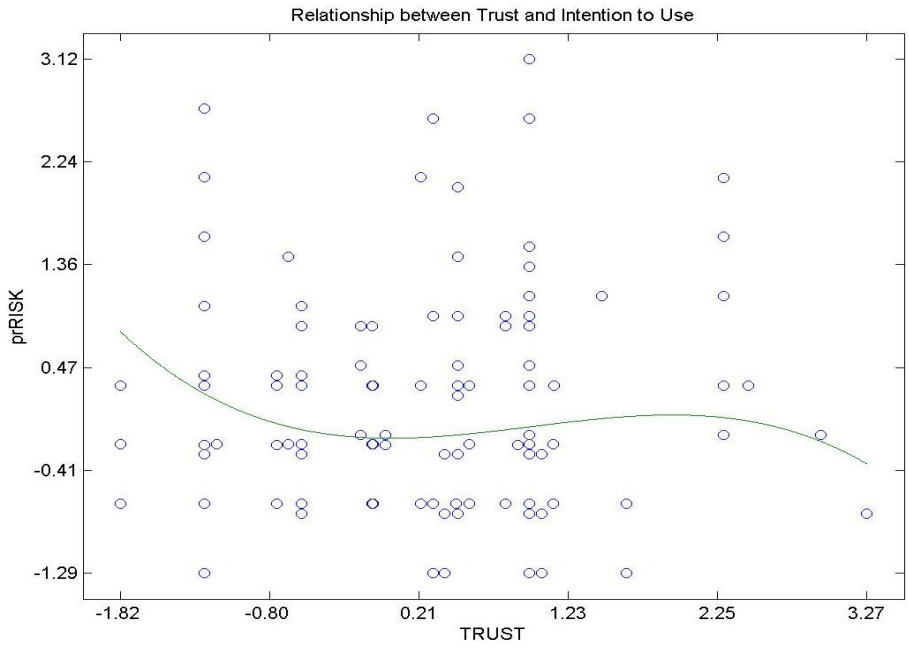


Figure 5.5: Relationship between Trust and Perceived Risk

v. Relationship between Trust and Intention to Use

Findings from this research also exhibited a significant effect of trust on intention to use as shown on Figure 5.5. This can be explained from the fact that, when users trust a system, their willingness to use or continue using it improves accordingly.

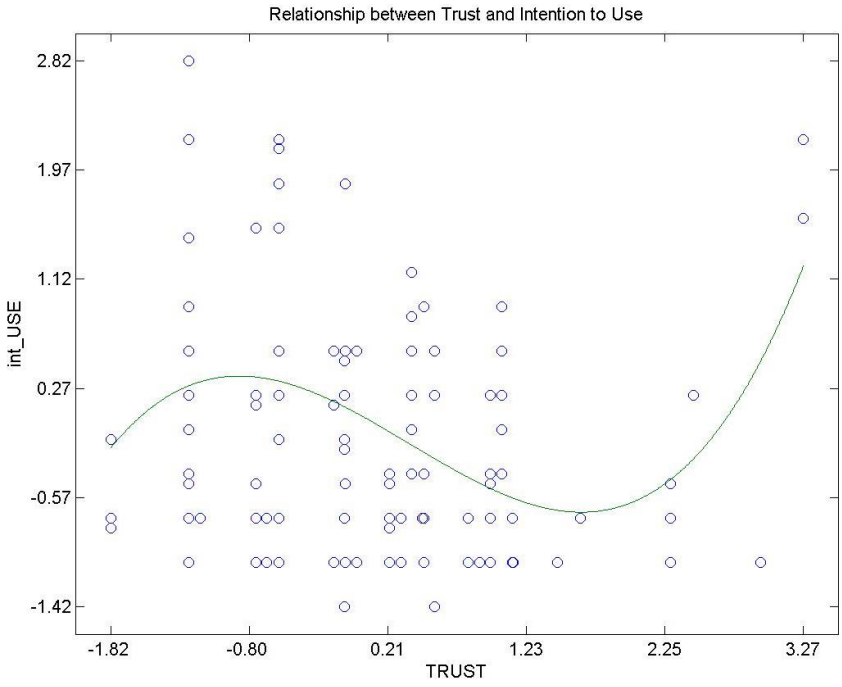


Figure 5.6 Relationships between Trust and Intention to Use

vi. Relationship between Perceived Risk and Intention to Use

Consistent with prior research, it was notable that, perceived risk had a negative effect on intention to use as evident from Figures 5.6. This can be due to the fact that, when users perceive more risky situations on how their information is used, they may fear using such systems, contributing to a decline in levels of usage intention for every increase in perceived risk.

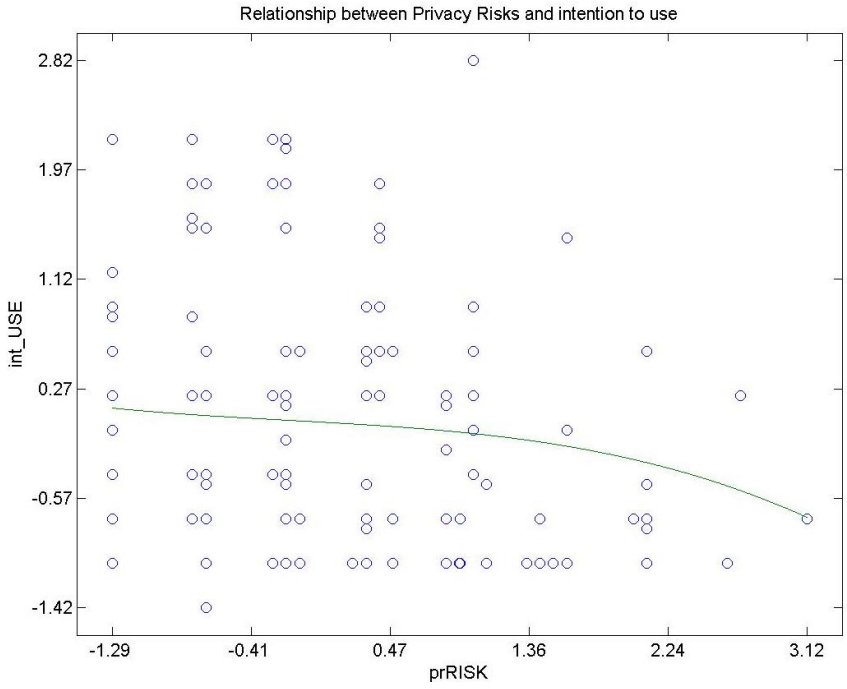


Figure 5.6 Relationships between Perceived Risk and Intention to Use

5.7 Comparative Model Analysis

To investigate research questions using structural equation modeling, it was more appropriate to analyze and compare results of several competing models as opposed to analyzing a single model (Werner & Schermelleh-Engel, 2010). These authors argue that, the proposed model may fit the data well, but there could be competing models based on different hypotheses which can explain the observed relationships as well; of which should be rejected if their data fit the worse compared to the proposed model. They assert that differences in model fit should be the only criteria to decide which model to prefer.

Accordingly, (Werner & Schermelleh-Engel, 2010) proposed the following model fit comparisons: 1) A model with an additional path compared to an otherwise identical

model without this path: Is there an effect between two latent variables or not? Is there a direct effect of factor **ξ1**-variable on a η-variable, or an indirect effect only? 2) A model assuming a relationship between two latent variables compared to a model where these latent variables are presumed to be unrelated: Are the factors **ξ1** and **ξ1** independent of each other or not? 3) A model with an additional loading of a manifest variable on a latent variable, compared to a model without such an additional loading: Is the manifest variable x1 an exclusive indicator of construct **ξ1**, or does it also measure aspects of a different latent variable **ξ2** at the same time? A decision between competing models may be clear-cut if there are completely obvious differences in model fit criteria, or if a parameter in question turns out to be both insignificant ($|t| < 1.96$) and of marginal size .

Different models can be compared with regard to their model fit by computing a $\chi 2$ difference test; meaningful only if the models in question are nested models, that is, one of the models can be obtained simply by fixing and or eliminating parameters in the other model (Werner & Schermelleh-Engel, 2010). Similarly , this research adopted their strategy by having additional path in the structural model of which we called a **saturated model**; additional loadings in a measurement model of which we called a **default model** (those factors that loaded poorly were trimmed); and an additional correlation/covariance between latent variables as proposed by (Werner & Schermelleh-Engel, 2010).

To compute $\mathbf{X^2}$ difference test, the difference of the $\mathbf{X^2}$ values of the two models in question were taken and the difference of the degrees of freedom as shown below:

$$X^2_{diff} = X^2_s - X^2_l \quad \text{and} \quad df_{diff} = df_s - df_l$$

Here, $_s$ denotes the "smaller" model with fewer parameters and therefore more degrees of freedom, whereas $_l$ denotes the "larger" model with more parameters and thus fewer degrees of freedom. The X^2_{diff} value is distributed with df_{diff} degrees of freedom and can be checked manually for significance using a X^2 table (shown in Appendix B). According to (Werner & Schermelleh-Engel, 2010), if the X^2_{diff} value is significant, the larger model (saturated model) with more freely estimated parameters fits the data better than the "smaller" model (default model) in which the parameters in question are fixed.; "paying off" to prefer "larger" model. In case the X^2_{diff} is insignificant both models fits equally well statistically, so the parameters in question can be eliminated from the model (fixed to zero) and the "smaller" model can be accepted just as well.

Table 4.29: Comparative Model Analysis

N0.	MODEL TYPE	X^2	df	X^2_{diff}	*p-value*	*Recommendation*
1	Saturated Model	0	0		.000	
2	Default Model	33.34	10	18.307	.000	Insignificant
3	Proposed Model	52.265	39	54.572	.000	Significant

On one hand the calculated Chi-Square for X^2 **(2),** 33.34 is less than the X^2_{diff} value, 18.307, the results fails to support goodness of fit; hence not significant. On the other hand, the Chi-Square Test for Goodness of Fit for X^2 **(3),** 52.265, were statistically significant since it was less than its X^2_{diff}, 54.572.

5.8 Summary

In this chapter, a location-based privacy-preserving model based on the findings of this research in chapter four is presented. The research was based on works by (Liao et al, 2011; Zhou, 2012) who ascertained Perceived risk, Privacy Concerns and Trust as factors manipulating behavioral intention. This research added the concept of privacy awareness and endeavored to establish its impact on usage intention as well as the correlation with other variables.

The model developed was tested using extant recommended indices for goodness of fit, whereby it was found to fit well. Besides this the research employed pseudo F-test (f^2 effect size), which allows a scholar to evaluate the independent variable's incremental explanation of a dependent variable. This is rarely used by existing studies on prediction and model estimations that only use the coefficient of determination (R^2 values) to characterize the ability of the model to explain and predict the endogenous latent variables. The model perfectly met this test therefore, exhibiting acceptable predictive and explanatory quality.

CHAPTER SIX

CONCLUSION AND FUTURE WORK

6.0 Conclusion

Through empirical research, it was found that location-based privacy affects usage intention of m-learning systems; and that extant models fail to address learners' location-based privacy, inspiring the development of a model to evaluate behavioral intention to use location-aware m-learning systems for distance education. The measurement model fit was assessed by a confirmatory factor analysis whereas, the individual items reliability, internal consistency, convergent and discriminant validity was scrutinized for goodness of fit. It was therefore established that Perceived risk, Privacy concerns, Trust and Privacy awareness had profound impact on behavioral intention to use m-learning systems for distance education.

6.1 Implication

This research has accomplished both academic and practical contributions. In terms of the academic contributions, an overall literature review of mobile learning systems was conducted with focus on location-based service's security and privacy aspects. The model's verification of goodness of fit is a sound evidence of a theoretical and practical contribution. From a theoretical perspective, this research integrated both perspectives of UTAUT and privacy risk to examine LBS user adoption in the context of mobile learning. As noted earlier, extant research had always focused on the effect of privacy concerns, Trust and privacy risk on user behavioral intention; but did

not fully address learners' location privacy awareness, making it unable to completely disclose user decision process of adopting LBS, especially for learning purposes. This research came in handy to fill that gap. Therefore, this research revealed that location privacy awareness had a profound effect on intention to use m-learning systems, an addition of new knowledge to the existing body of knowledge.

6.2 Future Work

Future research shall explore the effects of moderating variables in relation to the identified constructs in the present research. The research will also be extended to include societal and cultural factors beyond Kenyan context to ascertain generalizability of the research to other countries. Future research can also address the age groups and their perception on location based mobile learning. Future work can also explore the possibility of an m-learning application and use it for prototype demonstration.

REFERENCES

Ackerman, M. S., Cranor, L. F., & Reagle. , J. (1999.). Privacy in e-commerce: Examining user scenarios and privacy preferences. *1st ACM conference on Electronic Commerce,* (pp. 1–8). ACM Press,.

Abu-Al-Aish, A., Love, S., Hunaiti, Z., & Al-masaeed, S. (2013). Toward A Sustainable Deployment of M-learning: A conceptual Model in Higher Education. *International Journal of Mobile Learning and Organization*, 7(4), 253-276.

Adams, A., & Blandford, A. (2003). Security and Online Learning: To Protect or Prohibit. In C. e. Ghaoui, *Usability of Olnine Learning Programs* (pp. 331-359). UK: IDEA Publishing.

Ardagna, C., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., & Samarati, P. (2007). Location privacy protection through obfuscation-based techniques. *the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*. Redondo Beach, CA, USA .

Australian Government. (2014, September). *Australian Government. Privacy act. 1988.* Retrieved from Australian Government: http://www.privacy.gov.au/act/,

Bagozzi , R., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science,* 16(1), 74–94.

Bansal et al. (2010). "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems,* 49(2), 138-150,.

Bartley, S., & Golek, J. (2004). Evaluating the Cost Effectiveness of Online a nd Face-to-Face Instruction. . *Educational Technology & Society,* 7(4) , 167-175. .

Beldad, A., de Jong, M., & Steehoulder, M. (2010). How shall i Trust the Faceless and the Intangible? A literature review on the Antecedents of online Trust. *Computers in Human Behaviors*, 857-869.

Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing,* 2(1), 46–55.

Best, P., & Khan, L. (2009). *Research in Education (10th Ed.).* New Delhi: PHI Puplishing.

Bettini, C., Wang, X., & Jajodia, S. (2005). Protecting privacy against location-based personal identification. In W. Jonker, & M. Petkovic, *Secure Data Management. Volume 3674 f Lecture Notes in Computer Science.* (pp.185–199). Springer : Berlin / Heidelberg.

Buthpitiya, S., Zhang, Y., Dey, A., & Griss, M. (2011). n-gram geo-trace modeling. *Proceedings of Ninth International Conference on Pervasive Computing.* San Francisco, CA,.

Charbaji, A., & Mikdashi, T. (2003). A path analytic study of the attitude toward e-government in Lebanon. *Corporate Governance, 3*(1) , 76-82.

Chatschik , B., & Murat , S. (2013). *Trust and Obfuscation Principles for Quality of Information in Emerging Pervasive Environments.*

Chow, W., & Angie, N. (2006). A study of trust in e-shopping before and after first-hand experience is gained. *Journal of Computer Information Systems,* 46(4), 125–130.

Cohen, L., Manion, L., & Morrison, K. (2008). *Research methods in education.* New York: Routledge. .

Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* SAGE.

Cranor, L. F. (2001). P3P: The platform for privacy preferencesproject. In S. Garfinkel, & G. Spafford , *Web Security, Privacy, and Commerce, 2nd edition,* (pp. 699-707.). Sebastopol, CA, : O'Reilly, .

Cvrcek, D., Kumpost, M., Matyas, V., & Danezis, G. (2006). A study on the value of location privacy. *WPES '06 Proceedings of the 5th ACM workshop on Privacy in electronic society* (pp. 109-118). New York, USA: ACM.

Damiani, M. L., Bertino, E., & Silvestri, C. (2009). Protecting location privacy against spatial inferences: the probe approach. . *the 2nd SIGSPATIAL ACM GIS 2009*

International Workshop on Security and Privacy in GIS and LBS. SPRINGL '09, (pp. 32–41). New York, USA: ACM.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research, 17*(1), 61-80 .

Dinev , T., & Hart , P. (2006). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact,. *International Journal of Electronic Commerce ,10*(2), 7–29.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the AIS, 8*(7), 386-408.

Duckham , M., & Kulik, L. (2005). Simulation of obfuscation and negotiation for location privacy. In D. M. Mark , & A. G. Cohn, *COSIT 2005, volume 3693 ofLecture Notes in Computer Science,* (pp. 31–48). Berlin,: Springer,.

Duckham , M., & Kulik, L. (2006). *Location privacy and location-aware Computing.* Australia: University of Melborne.

Duckham , M., & Kulik, L. (2005). A formal model of obfuscation and negotiation for location privacy. In H. W. Gellersen, R. Want, & A. Schmidt, *Pervasive 2005, volume 3468 of Lecture Notes in Computer Science* (pp. 152–170). Berlin: Springer.

Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez , R., Singh, M., & Tang, J. M. (2002). Framework for security and privacy in automotive telematics. *2nd International Workshop on Mobile Commerce*, (pp. 25–32). ACM Press.

Espinoza, F., Persson, P., Sandin, A., Nystr¨ om, H., Cacciatore, E., & Bylund, M. (2001). GeoNotes: Social and navigational aspects of location-based information sysstems. In G. Abowd, B. Brumitt, & S. Shafer, *editors, Ubicomp 2001:Ubiquitous Computing, volume 2201 of Lecture Notes in Computer Science*, (pp. 2–17). Springer.

Gruteser , M., & Grunwald, D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. . *MobiSys '03* , (pp. 31–42).

Faruq , M., & Hartini , B. (2013). The Moderating Effect of Technology Awareness on the Relationship between UTAUT Constructs and Behavioural Intention to Use Technology: A Conceptual Paper. *Australian Journal of Business and Management Research, 3* (2), 14-23.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. . *Journal of Marketing Research, 18*(1), 39-50.

Fraenkel, J., & Wallen, N. (2009). *How to Design and Evaluate Research in Education (7th ed.).* New York: McGraw-Hill.

GovTech. (2009). Survey Raises Consumer Online Privacy Awareness. *Government Technology Magazines, Government Technology*.

Greene , S., & Kamimura , M. (2003). Ties that Bind: Enhanced Social Awareness Development Through Interactions with Diverse Peers. *Annual Meeting of the Association for the Study of Higher Education.* Portland, Oregon: Michigan University.

Gunter, C. A., May, M. J., & Stubblebine, S. G. (2004). A formal privacy systems and its application to location-based services. *Workshop on Privacy Enhancing Technologies.* Toronto, Canada.

Hair, J., Hult, G., Ringle, C., & Sarstedt, M. (2013). *A primer on partial least squares structural equation modeling (pls-sem).* Thousand Oaks, California: Sage.

Hawaii. (2015). *Sampling Strategies and their Advantages and Disadvantages*. Retrieved from hawaii.edu: http://www2.hawaii.edu/~cheang/Sampling%20Strategies%20and%20their%20Advantages%20and%20Disadvantages.htm

Hoyle , G. (2014). *What is Distance Education and Distance Learning?* Retrieved from Distance Learning on the Net: http://www.hoyle.com/distance/define.htm

Hong , J. I., & Landay. , J. A. (2004). An architecture for privacy-sensitive ubiquitous computing. *2nd International Conference on Mobile Systems, Applications, and Services,* (pp. 177–189). ACM Press.

Hwang, G. J., Tsai, C. C., & Yang, S. H. (2008). Criteria, Strategies and research issues of Context-aware ubiquitous learning. *Educational Technology & Society*, 81-91.

Ivec, S. (2015). *Mobile Learning Lockdown: Is Your Data Secure?* Retrieved from elearningindustry.com: https://elearningindustry.com/mobile-learning-lockdown-data-secure

Junglas, I., & Watson, R. (2008). Location-based services. *Communications of the ACM, 51*(3), 65-69.

Kambourakis, G. (2013). Security and Privacy in m-Learning and Beyond:challenges and state of the Art . *International Journal of u- and e- Service, Science and Technology*, 67-84.

Kido, H., Yanagisawa, Y., & Satoh, T. (2005). An anonymous communication technique using dummies for location-based services. *the International Conference on Pervasive Services (ICPS '05).*, 88–97.

Kim, D., Ferrin, D., & Rao, H. (2008). A trust-based consumer decision making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564.

Kim, M., & Ahn, J. (2006). Comparison of trust sources of an online market-maker in the e-marketplace: buyer's and seller's perspectives. *Journal of Computer Information Systems, 47*(1) , 84–94.

Kock , N. (2015). *WarpPLS 3.0 User Manual,*. Retrieved from ScriptWarp Systems: http://www.scriptwarp.com/BBFB2E30-7E6A-4086-B7F8-A134A1745029/FinalDownload/DownloadId-EB35805702C247E12080F78E66A03D0E/BBFB2E30-7E6A-4086-B7F8-A134A1745029/warppls/UserManual_WarpPLS_V3_Redirect.pdf

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1-10.

Kombo, C., & Tromp, R. (2006). *Proposal and Thesis writing: An Introduction. .* Nairobi: Pauline's Publication of Africa.

Kumar et al. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 46*(1), 254-264.

Kurkovsky, S., & Syta, E. (2010). Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. *InProceedings of the IEEE International Symposium on Technology and Society (ISTAS),* (pp. 441-449).

Langheinrich. , M. (2002). A privacy awareness system for ubiquitous computing environments. In G. Borriello, & L. E. Holmquist, *UbiComp 2002: Ubiquitous Computing, volume 2498 of Lecture Notes in Computer Science,* (pp. 237–245.). Springer.

Li, Y. (2011.). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(3), 453-496.

Liao et al. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications, 10(6),* 702-715.

Liu et al. (2012). A unified risk-benefit analysis framework for investigating mobile payment adoption. *2012 International Conference on Mobile Business.*

Lowry, P. B., Cao, J., & Everrard, A. (2011). Privacy Concerns versus Desire for Interpersonal Awareness in Driving the sue of Self-Disclosure Technologies: The Case of Instaant Messaging in Two Cultures. *Journal of Management Information Systems,* 163-200.

Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. . *Electronic Commerce Research and Applications, 8*(3), 130–141.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly, 10,1*, 4-12.

Mayer et al. (1995). An integrative model of organizational trust . *The Academy of Management Review, 20*(3), 709-734.

(2016). *Mobile Security Report.* NowSecure.

Mugenda, O., & Mugenda, A. (2003). *Research Methods:Quantitative and Qualitative Aapproaches.* Nairobi: Act Press.

Ng, W., & Nicholas, H. (2013). A Framework for Suistainable Mobile Learning in Schools. *British Journal of Educational Technology, 44 (5*), 695-715.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy,and the Integrity of Social Life.* Stanford University Press.

Okazaki, S., Li , H., & Hirose, M. (2009). Consumer privacy concerns and preference or degree of regulatory control. . *Journal of Advertising, 38(4),* 63-77.

Omar, K., Ala'a, & Al-Nasrallah. (2011). Determinants of e-Gov Adopt in Kuwait: The Case of the Traffic Violation E-payment System (TVEPS) . *the Second Kuwait Conference on e-Services and e-Systems,*. Kuwait.

Pan, Y., & Zinkhan, G. (2006). Exploring the impact of online privacy disclosures on onsumer trust. . *Journal of Retailing, 82*(4) , 331-338 .

Park., C. (2014). *Location-based information service due next year.* Retrieved from Korea Times 2 July 2004.: http://times.hankooki.com,

Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. *MIS Quarterly* , 105–136.

Peterson., J. (2014). *A presence-based GEOPRIV location objectformat.* Retrieved from ietf: http://www.ietf.org/proceedings/59/I-D/draft-ietf-geopriv-pidf-lo-01.txt

Pfitzmann , A., & K¨ ohntopp., M. (2001.). Anonymity, unobservability, and pseudonymity a proposal for terminology. ,. In H. Federrath, *Designing Privacy Enhancing Technologies, volume 2009 of Lecture Notes in Computer Science,* (pp. 1–9.). Springer.

Philips, R., McNaught, C., & Kennedy, G. (2010). Towards a genelized conceptual Framework for learning: the learning environment, learning procesess and learning outcomes (LEPO) framework. In L. H. Montgomerie, *Proceeding s of Edmedia:World conference on educational Media and Technology* (pp. 2495-2504). Association of Advancement of Computing in Education.

Podsakoff, P., MacKenzie, S., & Podsakoff, N. (2003). Common Method Biases in Behavioral Research: A Critical Review of theLiterature and Recommended Remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Rahman, M., Esichaikul, V., & Kamal, M. (2012). Factors influencing e-government adoption in Pakistan. *Transforming Government: People, Process and Policy, 6(3),* 258-282.

Russello, G., Crispo, B., Fernandes, E., & Zhauniar, Y. (2011). Yaase: Yet another android security extension. In privacy, security, risk and trust (PASSAT). *IEEEThird Inernational Conference on Social Computing (SocialCom),* (pp. 1033-1040).

Ringle, C., Sarstedt, M., & Straub, D. (2012). EDITOR'S COMMENTS:A Critical Look at the Use of PLS-SEM in MIS Quarterly. *MIS Quarterly*, *36*(1), 3-14.

Shonola , S., & Joy, M. (2016). Enhancing mobile learning security. *International Journal on Integrating Technology in Education (IJITE), 5*(3), 1-15.

Strassman , M., & Collier., C. (2004). Case study: Development of the Find Friend application. . In J. Schiller , & A. Voisard, *Location-based services,chapter 2,* (pp. 27–39). Morgan Kaufmann.

Schilit, B. N., Hong, J. I., & Gruteser, M. (2003). Wireless location privacy protection. *IEEE Computer*, *36*(12), 135–137.

Shankar, P., Ganapathy, V., & Iftode, L. (2009). Privately querying location-based services with sybilquery. . *International Conference on Ubiquitous Computing (UbiComp 2009)*, (pp. 31–40).

Shonola, S., & Joy, M. (2014). Learners' perception on security issues in m-learning (NigerianUniversities case study) . *Exchanges: the Warwick Research Journal, 2(1*), 107 – 128.

Tabachnick, B., & Fidell, L. (2007). *Using Multivariate Statistics, Fifth Edition.* . Boston: Pearson Education, Inc. .

Thelwall, M. (2011). Privacy and gender in the Social Web. . In L. R. In: Sabine Trepte, *Privacy online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 255-269). New York: Springer.

Thietart, R. (2007). *Doing management research: a comprehensive guide.* Paris: SAGE.

U.S. Department of Justice, Office of Information and Privacy. (2014). U.S. Department of Justice, Office of Information and Privacy. *Overview of the Privacy Act of 1974,*.

Urbach, N., & Ahlemann, F. (2010). Structural Equation Modelling in Information Systems Using Partial Least Squares. (W. Hui, Ed.) *Journal of information technology theory and application*, 5-40.

Values of the Chi-squared distribution. (2015). Retrieved from www.medcalc.org: https://www.medcalc.org/manual/chi-square-table.php

Wagner, E. D. (2008). Realizing the Benefits of Mobile L.earning. *Journal of Computing in Higher Education*, 4-14.

Wang, Y.-S., Wu , M.-C., & Wang, H.-Y. (2009). Investigating the determinants and age and gender differences in the acceptance of mobile learning. *British Journal of Educational Technology, 40*(1) , 92–118.

Werner, C., & Schermelleh-Engel, K. (2010). Deciding Between Competing Models: Chi-Square Difference Tests. In C. Werner, & K. Schermelleh-Engel, *Introduction to Structural Equation Modeling with LISREL – Version February 2010.* Frankfurt: Goethe University.

Westin, A. F. (1967). *Privacy and Freedom.* New York: Antheneum.

Williams, P. W. (2009). *Assessing Mobile Learning Effectiveness and Acceptance.*

Wernke, M., Skvortsov, P., D¨urr, F., & Rothermel, K. (2008). A Classification of Location Privacy Attacks and Approaches. *Personal and Ubiquitous Computing*.

Yamane , T. (1967). *Statistics, An Introductory Analysis,* (2nd Ed.), New York: Harper and Row.

Zafar, A., Hasan, S., & Trigui, M. (2014). Towards Secure m-Learning: An Analysis . *MAGNT Research Report (ISSN. 1444-8939), 2 (5),* 148-159 .

Zhou , T. (2012). Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. *Journal of Electronic Commerce Research, 13*(2).

Zhu , J., & Zhang, Y. (2011). Towards accountable mobility model: A language approach on user behavior modeling in office wifi networks. *Proceedings of The IEEE International Conference on Computer Communications and Networks (ICCCN 2011).* Maui, Hawaii.

APPENDICES

Appendix I: Questionnaire

A Location-Based Privacy-preserving Model for M-Learning Adoption to Enhance Distance Education in Kenya

The advent of smart mobile devices equipped with sensing technology into education realm has made large scale collection of personal specific data possible without the consent of the user. The purpose of this questionnaire is to explore the need for secure location-based privacy-preserving m-learning model to enhance distance education in Kenya. The data you provide would be kept confidential and stored anonymously. Also note that the Department's ethical rules and procedures have been followed, and ethical consent has been granted for this questionnaire.

Section 1: Personal Information & Demographics

Regional Centre

Course *

School

Level of Study

Year of Study

Age Group

Gender

- Male
- Female

This is a required question

Section 2: Location Privacy for Mobile Learning

NOTE: For the purpose of this research, Location privacy is a special type of information privacy which concerns the right of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others.

1. How important is location privacy to you? (Select one box only)

- Very important
- Important
- Not Important
- I'm not sure

2. Has your location privacy been breached before? (If YES, briefly explain)

(Please type either: YES, NO or NOT SURE (whichever is applicable))

3. What are the privacy aspects you may have when using mobile devices for learning?

Select all that apply (If other, please specify)

- ☐ Theft of mobile device with sensitive data
- ☐ Virus / Malware attack
- ☐ Data Interception
- ☐ Unauthorized access to mobile device
- ☐ Denial of Service
- ☐ Other: _____

4. What do you think are the damaging effect(s) of mobile learning location privacy threats to the learners?

Select all that apply (If other, please specify)

- ☐ Personal Safety due to Intrusive inferences
- ☐ Loss of confidential information
- ☐ Denial of Service
- ☐ Loss of control (e.g. Over online assessment)
- ☐ Loss of content quality
- ☐ Psychological damage
- ☐ Loss of study hours (e.g. due to downtime)
- ☐ Other: _____

5. What do you think are the damaging effect(s) of mobile learning privacy threats to the Higher Education Institution?

Select all that apply (If other, please specify)

- ☐ Loss of confidential information

- ☐ Loss of goodwill / integrity
- ☐ Loss of reliability
- ☐ Loss of person's hours
- ☐ Other: ____

6: How do you think the mobile learning privacy threats or issues are assessed?

Select all that apply (If other, please specify)

- ☐ Report by users of unusual behavior of device
- ☐ System monitoring/Alert
- ☐ Frequency of Denial of Service
- ☐ Log file analysis
- ☐ Other: ____

On a scale of 1-5 (1=Strongly Agree, 2=Agree, 3=neither Agree nor Disagree, 4= Disagree, 5=Strongly Disagree), rate the level of your agreement for each of the following questions when using your mobile device for educational purposes.

(Please tick one circle on each row)

7. M-learning systems seeking information should disclose how data are collected, processed, and used.

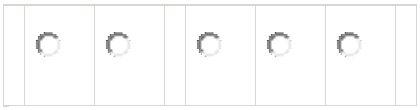
	1	2	3	4	5
	○	○	○	○	○

8. Good learners' online privacy should have a clear and visible disclosure.

	1	2	3	4	5

9. It is very important that I am aware of how my personal information will be used.

1 2 3 4 5



10. I am concerned that information collected by location- aware m-learning systems could be misused.

(1=Strongly Agree, 2=Agree, 3=neither Agree or Disagree, 4= Disagree, 5=Strongly Disagree)

1 2 3 4 5

11. I am concerned that others can find my private information from location- aware m-learning systems

1 2 3 4 5

12. I am concerned of my personal information in the m-learning systems as it could be used in a way that I do not foresee.

1 2 3 4 5

13. M-learning service provider keeps learners' interests in mind (i.e would not intentionally endanger learner's privacy)

1 2 3 4 5

14. M-learning service provider keeps its promise on protecting learners' privacy

1 2 3 4 5

15. M-learning service provider is trustworthy in preserving learner's location privacy

(1=Strongly Agree, 2=Agree, 3=neither Agree or Disagree, 4= Disagree, 5=Strongly Disagree)

1 2 3 4 5

16. Providing m-learning service provider with my personal information would involve many unexpected outcomes.

1 2 3 4 5

17. It would be risky to disclose my personal information to m-learning service provider

1 2 3 4 5

18. There would be high potential for loss in disclosing my personal information to m-learning service provider

1 2 3 4 5

19. Given the chance, I intend to use location aware mobile equipment for learning

1 2 3 4 5

20. I expect my use of location aware mobile gadget for learning to continue in the future.

(1=Strongly Agree, 2=Agree, 3=neither Agree or Disagree, 4= Disagree, 5=Strongly Disagree)

1 2 3 4 5

22. I have intention to use location aware mobile equipment for learning

1 2 3 4 5

23. Protecting learners' location privacy will improve the sustainability of M-learning

1 2 3 4 5

24. To evaluate the impact of m-learning systems in meeting needs of learners' location privacy will promote sustainability.

1 2 3 4 5

Appendix II: Chi-square distribution table

Adopted from (Values of the Chi-squared distribution, 2015)

	P										
DF	**0.995**	**0.975**	**0.20**	**0.10**	**0.05**	**0.025**	**0.02**	**0.01**	**0.005**	**0.002**	**0.001**
1	0.0000393	0.000982	1.642	2.706	3.841	5.024	5.412	6.635	7.879	9.550	10.828
2	0.0100	0.0506	3.219	4.605	5.991	7.378	7.824	9.210	10.597	12.429	13.816
3	0.0717	0.216	4.642	6.251	7.815	9.348	9.837	11.345	12.838	14.796	16.266
4	0.207	0.484	5.989	7.779	9.488	11.143	11.668	13.277	14.860	16.924	18.467
5	0.412	0.831	7.289	9.236	11.070	12.833	13.388	15.086	16.750	18.907	20.515
6	0.676	1.237	8.558	10.645	12.592	14.449	15.033	16.812	18.548	20.791	22.458
7	0.989	1.690	9.803	12.017	14.067	16.013	16.622	18.475	20.278	22.601	24.322
8	1.344	2.180	11.030	13.362	15.507	17.535	18.168	20.090	21.955	24.352	26.124
9	1.735	2.700	12.242	14.684	16.919	19.023	19.679	21.666	23.589	26.056	27.877
10	2.156	3.247	13.442	15.987	18.307	20.483	21.161	23.209	25.188	27.722	29.588
11	2.603	3.816	14.631	17.275	19.675	21.920	22.618	24.725	26.757	29.354	31.264
12	3.074	4.404	15.812	18.549	21.026	23.337	24.054	26.217	28.300	30.957	32.909
13	3.565	5.009	16.985	19.812	22.362	24.736	25.472	27.688	29.819	32.535	34.528
14	4.075	5.629	18.151	21.064	23.685	26.119	26.873	29.141	31.319	34.091	36.123
15	4.601	6.262	19.311	22.307	24.996	27.488	28.259	30.578	32.801	35.628	37.697
16	5.142	6.908	20.465	23.542	26.296	28.845	29.633	32.000	34.267	37.146	39.252
17	5.697	7.564	21.615	24.769	27.587	30.191	30.995	33.409	35.718	38.648	40.790
18	6.265	8.231	22.760	25.989	28.869	31.526	32.346	34.805	37.156	40.136	42.312
19	6.844	8.907	23.900	27.204	30.144	32.852	33.687	36.191	38.582	41.610	43.820
20	7.434	9.591	25.038	28.412	31.410	34.170	35.020	37.566	39.997	43.072	45.315
21	8.034	10.283	26.171	29.615	32.671	35.479	36.343	38.932	41.401	44.522	46.797
22	8.643	10.982	27.301	30.813	33.924	36.781	37.659	40.289	42.796	45.962	48.268
23	9.260	11.689	28.429	32.007	35.172	38.076	38.968	41.638	44.181	47.391	49.728
24	9.886	12.401	29.553	33.196	36.415	39.364	40.270	42.980	45.559	48.812	51.179
25	10.520	13.120	30.675	34.382	37.652	40.646	41.566	44.314	46.928	50.223	52.620
26	11.160	13.844	31.795	35.563	38.885	41.923	42.856	45.642	48.290	51.627	54.052
27	11.808	14.573	32.912	36.741	40.113	43.195	44.140	46.963	49.645	53.023	55.476
28	12.461	15.308	34.027	37.916	41.337	44.461	45.419	48.278	50.993	54.411	56.892
29	13.121	16.047	35.139	39.087	42.557	45.722	46.693	49.588	52.336	55.792	58.301
30	13.787	16.791	36.250	40.256	43.773	46.979	47.962	50.892	53.672	57.167	59.703
31	14.458	17.539	37.359	41.422	44.985	48.232	49.226	52.191	55.003	58.536	61.098
32	15.134	18.291	38.466	42.585	46.194	49.480	50.487	53.486	56.328	59.899	62.487
33	15.815	19.047	39.572	43.745	47.400	50.725	51.743	54.776	57.648	61.256	63.870
34	16.501	19.806	40.676	44.903	48.602	51.966	52.995	56.061	58.964	62.608	65.247
35	17.192	20.569	41.778	46.059	49.802	53.203	54.244	57.342	60.275	63.955	66.619
36	17.887	21.336	42.879	47.212	50.998	54.437	55.489	58.619	61.581	65.296	67.985

37	18.586	22.106	43.978	48.363	52.192	55.668	56.730	59.893	62.883	66.633	69.346
38	19.289	22.878	45.076	49.513	53.384	56.896	57.969	61.162	64.181	67.966	70.703
39	19.996	23.654	46.173	50.660	54.572	58.120	59.204	62.428	65.476	69.294	72.055
40	20.707	24.433	47.269	51.805	55.758	59.342	60.436	63.691	66.766	70.618	73.402
41	21.421	25.215	48.363	52.949	56.942	60.561	61.665	64.950	68.053	71.938	74.745
42	22.138	25.999	49.456	54.090	58.124	61.777	62.892	66.206	69.336	73.254	76.084

Appendix III: Operational Definitions and Survey Items

Construct	Operational Definition	Survey Items	References
Privacy Awareness	The individuals' knowledge on the privacy risks, privacy concerns, privacy policies associated with the Internet, and the legal implications of privacy invasions and identity theft	7. M-learning systems seeking information should disclose how data are collected, processed, and used (AWARE1)	(Liao et al., 2011).
		8. Good learners' online privacy should have a clear and visible disclosure (AWARE2).	
		9. It is very important that I am aware of how my personal information will be used (AWARE3).	
Privacy Concerns	The degree to which an individual is concerned about the collection, improper access, errors, and secondary use of their personal location information	10. I am concerned that information collected by location- aware m-learning systems could be misused (CONC1).	(Xu, 2007)
		11. I am concerned that others can find my private information from location- aware m-learning systems (CONC2).	
		12. I am concerned of my personal information in the m-learning systems as it could be used in a way that I do not foresee (CONC3).	
Trust	The willingness of a party to be vulnerable to the actions of another party	13. M-learning service provider keeps learners' interests in mind (i.e would not intentionally endanger learner's privacy)	(Chow and Angie, 2006)
		14. M-learning service provider keeps its promise on protecting learners'	

		privacy	
		15. M-learning service provider is trustworthy in preserving learner's location privacy	
Perceived Risk	The degree to which an individual is able to anticipate negative outcomes in the future due to improper collection, access, errors, and secondary use of their personal location information	16. Providing m-learning service provider with my personal information would involve many unexpected outcomes	(Liu, 2012), (Liao et al., 2011).
		17. It would be risky to disclose my personal information to m-learning service provider	
		18. There would be high potential for loss in disclosing my personal information to m-learning service provider	
Intention to Use	A person's perceived likelihood or "subjective probability that he or she will engage in a given behavior".	19. Given the chance, I intend to use location aware mobile equipment for learning	(Venkatesh et al. 2003); (Venkatesh & Morris, 2000); (Committee on Communication for Behavior Change in the 21st Century, 2002, p. 31).
		20. I expect my use of location aware mobile gadget for learning to continue in the future.	
		22. I have intention to use location aware mobile equipment for learning	
		23. Protecting learners' location privacy will improve the sustainability of M-learning	
		24. To evaluate the impact of m-learning systems in meeting needs of learners' location privacy will promote sustainability.	
		19. Given the chance, I intend to use location aware mobile equipment for learning	