J. Comput. Educ. (2017) 4(2):147–169
DOI 10.1007/s40692-017-0079-4

A location-based privacy-preserving m-learning model to enhance distance education in Kenya

Peter B. Obiria[1] · Micheal W. Kimwele[1]

Received: 27 October 2016 / Revised: 10 February 2017 / Accepted: 13 February 2017 /
Published online: 23 February 2017

Abstract Developments in mobile learning have seen the adoption of high-power, location-aware mobile gadgets in distance education. Unauthorized user's location data collected by these devices could hamper sustainable adoption of m-learning systems. There is the need, therefore, to develop a secure location-based privacy-preserving model to evaluate learners' behavioral intention to use location-aware mobile systems for distance education. The study employed descriptive design, and using a questionnaire, data were collected from a population enrolled for distance learning. Using SPSS version 20 and WarpPLS 5.0, data were statistically analyzed to validate or refute the intended objectives. The model would provide the university management with informed approach to consider privacy-preserving aspects in m-learning implementation. It will provide enlightened guidance to mobile-learning-application developers on the need to cater for learners' privacy.

Keywords Location-based privacy · m-learning · m-learning systems · Distance education

Introduction

Rapid technological advancement in the recent past has led to emergence of new specialties into computing and communication service provision (Musau and Obiria 2013). One such discipline is mobile learning (m-learning). The need to position students in real-world learning scenarios has also accelerated the delivery of technology-enhanced learning that enables students to access digital-learning

✉ Peter B. Obiria
obpeters@gmail.com

[1] Department of Computer Science, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

resources from anywhere and at any time (Hwang 2015). The popularity of mobile and wireless communication technologies has provided a good opportunity to accomplish these objectives with various strategies and tools having been proposed to help learners more effectively learn with mobile devices (Hwang 2015). In addition, m-learning helps to link what students learn from textbook to what they experience in real life, providing support to individual students to deal with real-world problems and enable them afford seamless learning (Hwang 2017). The upsurge of mobile devices and their capabilities thereof has made m-learning establish itself as a learning tool to be 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 (Hwang et al. 2008).

Therefore, with the advent of smart phones equipped with mobile-sensing technology into the education realm, a large-scale collection of personal specific data is now possible. Typical sensor information, which includes GPS, Location, WLAN, cell tower ID, browsing history, and microphone, makes it easy to infer a user’s home address, office location, the period, and means of movement among others from the personal Big Data collected. Through statistical modeling over the sensor data time-series, it is possible to infer behavioral patterns of the user such as their outdoor (Buthpitiya et al. 2011) and indoor (Zhou 2011) mobility patterns. Consequently, such personal data if not protected can lead to serious privacy-intrusion implications, including a hindrance to seamless adoption of mobile-learning technologies.

Preserving location privacy of the learner while sensitive data are stored or processed in m-learning systems is a nontrivial concern (Obiria et al. 2015a). Therefore, a secure location-based privacy mechanism is essential to retain users’ trust, the key to influencing the usage intention of any new technology. This is because any risk to users’ privacy can have drastic effects on the users’ perceptions of a system’s reliability and trustworthiness (Adams and Blandford 2003). In the context of m-learning, the provision of privacy-preserving mechanisms is key to safeguard private sensitive data (Pfitzmann and Ohntopp 2001), and Kukulska-Hulme (2013), in her presentation at a UNESCO mobile-learning symposium, revealed several challenges facing m-learning implementations, among them being data security, privacy, and trust. It is therefore the endeavor of this study to establish a location-based privacy-preserving framework that can be used to evaluate user-location privacy aspects in m-learning domain.

Kenya like other developing countries in the world is grappling with an upsurge in its university distance-learning enrolment, fueled by the increased need for education and social-economic factors (Obiria et al. 2015a). 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 to m-learning. Universities have developed a great interest on how to engage mobile technologies in making learning for 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 (Obiria et al. 2015a).

Problem statement

Developments in mobile learning have seen the adoption of high-power, location-aware mobile gadgets like smart phones and iPads in distance education which offer additional freedom through service mobility. However, lack of security and privacy awareness on unauthorized user's location data collected by these devices could hamper sustainable adoption of m-learning systems. This is because data collected can be used by ruthless businesses to overwhelm a mobile device with spam related to that individual's location, leading to overload of m-learning device already known to contain low processing power, resulting in denial of service. In addition, the data collected can lead to stalking and intrusive inferences that could result in the abuse of user profiling which is generally unacceptable.

Justification

Security and privacy aspects in m-learning are quite different from those tackled in e-learning context. As a result, users are worried on the abuse of sensitive personal data collected without their implicit consent (Obiria et al. 2015a). Those authors assert that mobile devices have the ability to expose their user's location, and consequently, track their movement in space. Vulnerability issues in mobile technologies have become common due to lots of ad-hoc mobile networks, high penetration of mobile devices, and lack of user's security and privacy awareness (Greene and Kamimura 2003; Obiria et al. 2015a).

Research objectives

- To determine how secure location-based privacy relates to intention to use m-learning systems;
- To develop a secure location-based privacy-preserving model for evaluating learners' behavioral intention to use location-aware m-learning systems.
- To evaluate the effects of the identified constructs on the intention to use m-learning systems for distance education.

In this research, we make the following contributions:

- We build an integrated model germane to location-based privacy derived from the existing theories to examine the effects of antecedent variables on the intention to use m-learning systems to enhance distance education.
- We verify the model with and without moderating variables to lend this study both a theoretical significance and a practical significance.

Related work

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) (Chow and Angie 2006). 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, in the context of m-learning, further argue that, while security is a methodology of ensuring integrity of data and protecting policies of the institution, privacy is that of maintaining 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 cited 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 could 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 learner‘s 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. Hence, 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 and Kulik 2006). Therefore, control of location information is a key concern in location privacy. Location privacy is fundamental to this study due to recent developments in mobile learning that has seen adoption of high-power, location-aware mobile gadgets like smart phones and iPads in distance education.

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 domain.

Learners' location-based 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 his or 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 a location-based news feed service. Preserving temporal information is one other expectation that learners would want protected.

Challenges germane to location-based privacy

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

- *Location-Based Spam:* Location could be used by unscrupulous businesses to bombard an individual with unsolicited marketing of 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 in denial of service.
- *Personal Well-being and Safety:* Location is indivisibly linked to personal safety. Unrestricted access to information about an individual's location could potentially lead to harmful encounters, for example, stalking or physical attacks. Personal safety and well-being could affect adoption in that, the moment learners realize that their whereabouts can easily be tracked and the obtained data used to cause physical injury, then few people will be willing to adopt m-learning.
- *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. Most people would want their information kept private and confidential, and on such occasions, when their location data can be accessed and even more information deduced, it

becomes a fundamental concern that could hamper seamless adoption of m-learning strategy in education.

Effects of unsecured location-based privacy to m-learning adoption

Failure to protect location privacy within a location-aware computing environment could result in a number of negative effects. For instance, a porous location could be used by ruthless businesses to overwhelm an individual with unsolicited marketing of products or services related to that individual's location. This could lead to overload of an m-learning device which is already known to contain low processing power, eventually resulting in denial of service. Uncontrolled access to information about an individual's location could potentially lead to harmful encounters, like stalking or physical attacks. This could 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 constrains 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 hence, a fundamental concern that could hamper seamless adoption of m-learning in education.

Our location privacy-preserving framework

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. Consistently, our study follows the direction of technology adoption literature as described in Faruq and Hartini (2013) and Lee (2009a, b) 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.

(1) *Behavioral Intention*

The main variable of interest in this study is Behavioral intention to use location-aware m-learning system. 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 and Hartini (2013). In the listing, this study focuses on works by Faruq and Hartini (2013) and Liao et al. (2011), which have proposed Perceived risk, Privacy Concerns, and Trust as factors influencing behavioral intention. This study adds the concept of privacy awareness and endeavors to establish its impact on usage intention as well as the correlation with other variables.

(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 and 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 has long been discussed in the literature (Mason 1986). 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 will be to affect those perceptions. The study by Dinev and Hu (2007) found that technology awareness leads 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 users' 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. However, the multiplied risk of this information may be lost on many users. Hence, a need to establish a means to hide some if not all of these vital identifiers of user's personal information.

A study on factors influencing e-government adoption among Lebanese postgraduate students has found that awareness significantly influences behavioral intention (Charbaji and Mikdashi 2003). A similar study by Rahman et al. (2012) confirmed these findings. Other studies on the relationship between independent variable and dependent variable have also found that awareness perfectly affects relationships between variables (Omar 2011).

(3) *Privacy Concerns*

Privacy concerns indicate user's concern on personal information disclosure (Li 2011). There have since then been many concerns such as (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 purpose 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's 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. In addition, numerous extant studies have treated the construct of privacy concerns as a precursor to various behavior-related variables. Assertions by Dinev and Hart (2006a) confirm 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 and Sin 2005). Similarly, we expect 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. Research by Okazaki et al. (2009) found that privacy concerns were a significant predictor of trust and perceived risk in mobile advertising.

(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 and Angie 2006). It is hoped that an exchange partner will not engage in opportunistic behavior (Kim and Ahn 2006). Finally, Kim and Ahn (2006) assert that trust is the willingness to depend. It often includes three beliefs: ability, integrity, and benevolence (Dinev and Hart 2006a). Ability means that service providers have the knowledge and skills to fulfill their tasks. 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 the 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).

(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 2012). For example, Lee (2009a, b) employs five subdimensions 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 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 become reluctant to adopt and use m-learning systems that are already location-aware.

Methodology

This methodology adopted quantitative design due to its particular value to establish topic-related occurrences, trends, comparisons, and statistical relationships (Thietart 2007). The target population comprised students enrolled for distance learning using mobile gadgets in a selected university. The researcher used the Yamane (1967, p. 886) formula, with a 95% confidence level to identify appropriate sample size.

Data analysis and findings

The study aimed at validating the research model shown in Fig. 1 based on the perception of actual users of location-aware mobile-learning systems for distance education. An online survey based on Google Docs was conducted. The URL link was sent via e-mail to 336 University students registered for Distance Learning, and replies were obtained from 323 learners, representing 96.13% respondents. The demographic characteristics of the sample are shown in Table 1.

Statistical findings analysis

Partial Least Squares (PLS) approach was adopted for statistical analysis in this study. 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 and Ahlemann

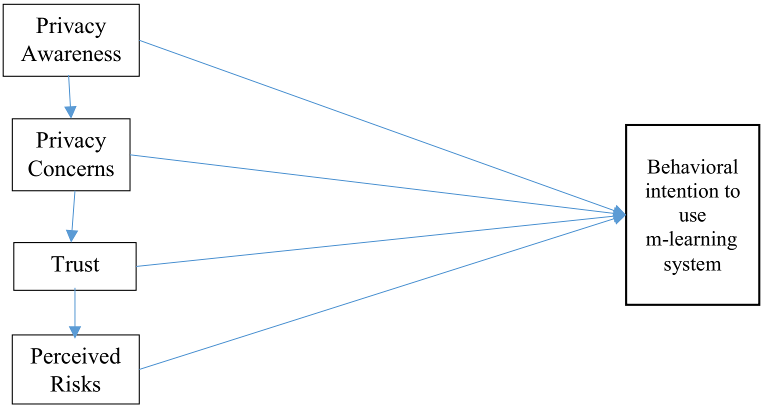

Fig. 1 Conceptual Model

Table 1 The demographic distributions of data findings

	Frequency		Percent	Valid percent
Cumulative percent				
Year of study				
Year 1	111	34.4	34.4	34.4
Year 2	109	33.7	33.7	68.1
Year 3	103	31.9	31.9	100.0
Age group				
18–24 years	44	13.6	13.6	13.6
25–30 years	26	8.0	8.0	21.7
31–35 years	25	7.7	7.7	29.4
36–40 years	80	24.8	24.8	54.2
41–45 years	64	19.8	19.8	74.0
46–50 years	84	26.0	26.0	100.0
Gender				
Male	187	57.9	57.9	57.9
Female	136	42.1	42.1	100
Importance of location privacy				
Very important	103	31.9	31.9	31.9
Important	141	43.7	43.7	75.5
Not sure	79	24.5	24.5	100.0

(2010). The CBSEM, on the one hand, is applicable for testing of the theory and is parameter-oriented, and hence, optimal for parameter accuracy. PLS on the other hand is prediction-oriented, optimal for prediction accuracy, and thus, a more appropriate technique for theory development studies (Urbach and Ahlemann 2010).

WarpPLS5.0 (Ringle et al. 2012) was used to test the measurement model and the structural model. 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 study based on our objectives, reflective model was adopted for this research. This is because the evaluation of formative measurement models give rise to concerns such as redundancy analysis, where as a review by Ringle et al. (2012) reveals that PLS-SEM studies are usually built on satisfactory evaluations that ensure the reliability and validity of the reflective measurement model construct.

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 3. 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 modeling (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 were scrutinized to ensure appropriate measurement model.

Structural model

In the structural model, also called inner model, the latent variables (LVs) are related to each other according to substantive theory. This study 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. 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.

In addition, Ringle et al. (2012) assert that none of the studies in their findings use (Stone 1974)'s cross-validated redundancy measure Q^2, which allows assessing the model's predictive relevance. 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. According to Kock (2015a, b), acceptable predictive validity in connection with an endogenous latent variable is suggested by a Q-squared coefficient greater than zero. In accordance with Ringle et al. (2012), who urge researchers to use statistical criteria such as f^2, Q^2, and q^2, this study incorporated these measures to make a stronger case for model's predictive capabilities.

While assessing the pseudo F-test (f^2 effect size), we run the warpPLS5.0 that provides an option to view both the direct and indirect effects along various paths making up the structural model. This study found that the result supports a direct effect on all variables as shown embolden in Table 2. The indirect effect was also significant with respect to some variable

To assess the prediction quality, q^2, we used warpPLS5.0 as well. The result showed a substantial prediction ability of our proposed model as shown in the Table 2.

Table 2 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)

Model-fit validation from results

After the analysis process, the results of the model could be represented as shown in Fig. 2, 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.

To assess the model fit with the 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 (Kock 2015a, b). In addition, the average variance inflation factor (AVIF) should be lower than 5. Table 3 provides the model fit indices with p values of the estimated model. It was found that, all the three fit criteria were met and can reasonably assume that the model has acceptable predictive and explanatory qualities as the data are well represented by the model.

Another aspect used to determine model fit is item loadings. The items are 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 a general rule of thumb, loadings above 0.71 are excellent, 0.63 very

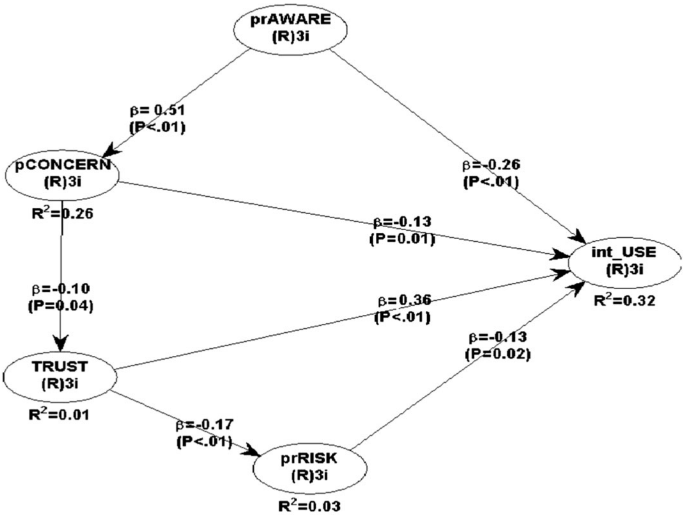

Fig. 2 Results of PLS analysis

Table 3 Model-fit and 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)	1.90	≤ 5
Average full collinearity VIF (AFVIF)	1.603	≤ 5
Tenenhaus GoF (GoF)	0.283	Small $\geq$ 0.1
		Medium $\geq$ 0.25
		Large $\geq$ 0.36
Simpson'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

good, 0.55 good, 0.45 fair, and 0.32 poor (Tabachnick and Fidell 2007). In this study, the indicators loaded highly where they are supposed to load, as shown in Table 4 (loadings shown in bold).

Table 5 shows the items' mean, standard deviation, composite reliability, average variance extracted (AVE), and square root of the AVE, as well as the correlations between the constructs. According to Kock (2015a, b), 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

Table 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	−0.9	**0.857**
USE5	−0.192	−0.023	0.095	0.06	**0.844**

Table 5 Correlations among latent variables with sq. roots of AVEs in diagonal

No.	Constructs	No. 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	−0.97	**0.69**			
3	Trust	3	1.75	0.86	0.719	0.91	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**

of the correlations between that latent variable and other latent variables. To test the discriminant validity, we compared the square roots of AVE and factor correlation coefficients. As listed in Table 5, for each variable, the square root of AVE is significantly larger than its correlation coefficients with other variables, suggesting good discriminant validity.

The same table also shows that the composite reliability (CR) measures are all greater than 0.71, which is above the recommended value of 0.7 for construct reliability (Bagozzi and Yi 1988). A satisfactory level of convergent validity is maintained since the AVE values of most of the constructs are above the suggested threshold value of 0.50.

Discussion

This study was designed to develop a secure location-based privacy-preserving model from the existing theories for m-learning adoption; to enhance distance education by evaluating learners' behavioral intention to use location-aware m-learning systems. Through a literature review, the study 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 aforementioned factors on behavioral intention is lacking, adding much complexity to our understanding of the perception-versus-behavior relationship for this online learning activity. This study offers 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 will help in discussing the results, case by case.

Relationship between privacy awareness and privacy concerns

Privacy awareness is seen to positively relate to privacy concerns, a finding consistent with Dinev and Hart (2006b). 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 Fig. 3.

Relationship between privacy awareness and intention to use

Previously, Obiria et al. (2015a) discovered that new studies indicated growing user online privacy awareness. It was also found that many users of LBS are quite aware that there are privacy risks, the majority of which do not understand how unprotected location data can be potentially used against them. In line with this, this study endeavored to investigate learners' behavioral usage intention, should they know the effects of their unsecured location-based information. This study found

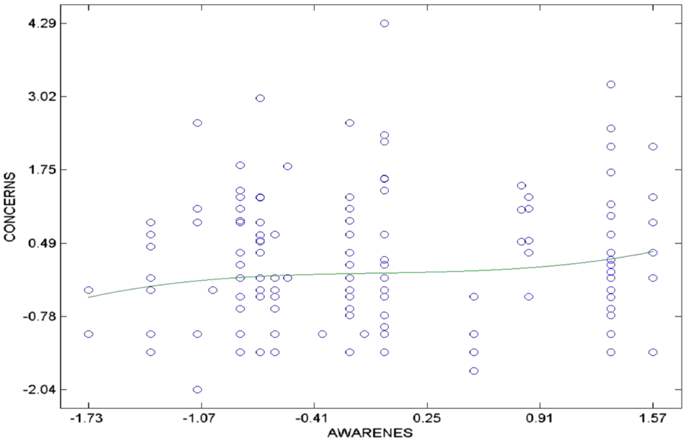

Fig. 3 Relationship between Privacy awareness and privacy concerns

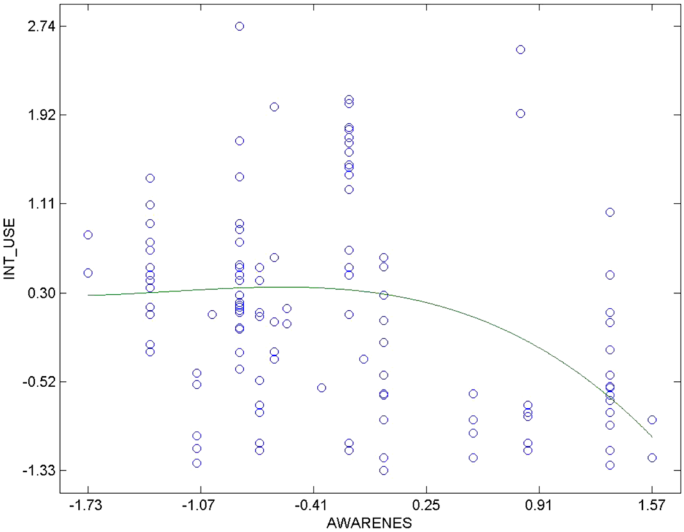

Fig. 4 Relationship between Privacy awareness and Intention to Use

out that privacy awareness negatively relates to intention to use location-aware m-learning systems as shown in Fig. 4.

Relationship between privacy concerns and trust

The results are consistent with extant findings by Bansal et al. (2010). Privacy concern reflects user concern on personal information disclosure willingly or personal information discovery unaware through location-aware mobile systems. If service providers cannot ensure that users' personal information is properly

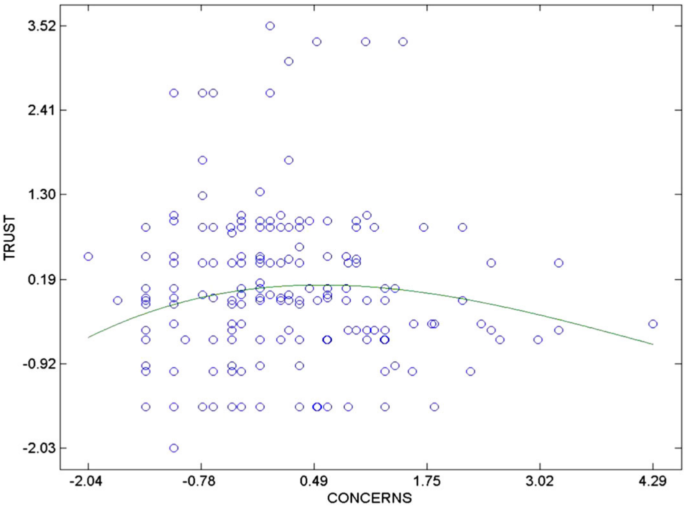

Fig. 5 Relationship between privacy concerns and Trust

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 study found that privacy concerns has significant effects on trust as shown in Fig. 5. Therefore, service providers need to implement effective measures to reduce users' privacy concerns 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.

Relationship between trust and perceived risk

In the same vein, Trust was found to affect perceived risk, and both factors affect usage intention as shown in Fig. 6. Trust provides a guarantee that users acquire positive outcomes in future. Consistent with the extant studies, trust is seen to mitigate perceived risk.

Relationship between trust and intention to use

Findings from this study also exhibited a significant effect of trust on intention to use as shown on Fig. 7. This can be explained from the fact that, when users trust a system, their willingness to or continue using it improves accordingly.

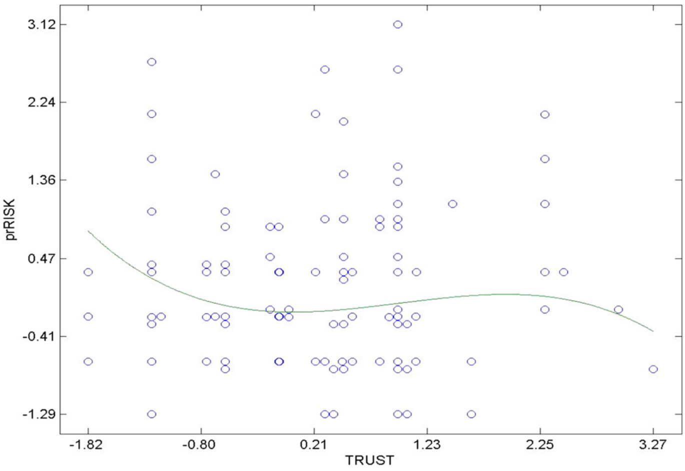

Fig. 6 Relationship between Trust and Perceived Risk

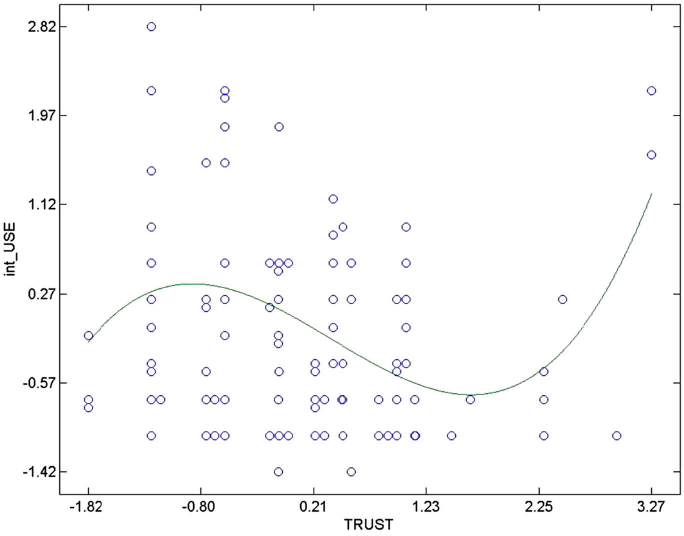

Fig. 7 Relationship between Trust and Intention to Use

Relationship between perceived risk and intention to use

Consistent with prior research, it was notable in this study that perceived risk had a negative effect on intention to use as evident from Fig. 8. This could be due to the fact that, when users perceive more risky situations on how their information is used, they tend to have fear using such systems, contributing to a decline for every increase in perceived risk.

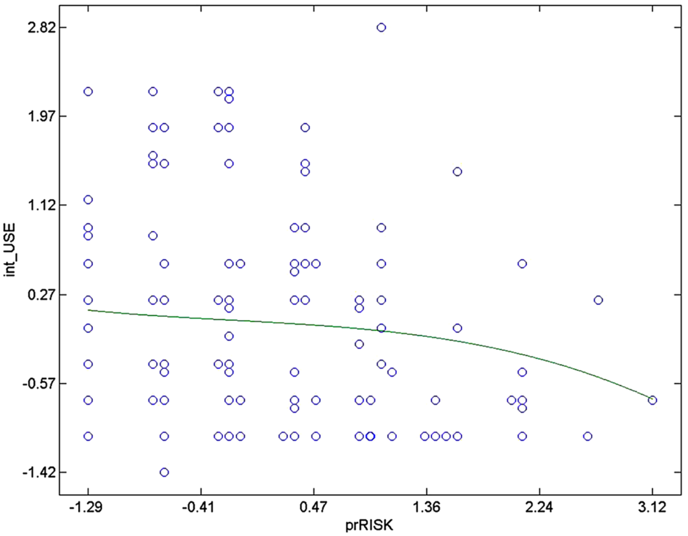

Fig. 8 Relationship between Perceived Risk and Intention to Use

Comparative model analysis

To investigate research questions using structural equation modeling, it is more appropriate to analyze and compare results of several competing models as opposed to analyzing a single model (Werner and 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 could explain the observed relationships as well, which should be rejected if their data fit was worse compared with the proposed model. They assert that differences in model fit should be the only criteria to decide which model to prefer.

Accordingly, Werner and Schermelleh-Engel (2010) propose the following model-fit comparisons: (1) A model with an additional path is compared with an otherwise identical model without this path: Is there an effect between two latent variables or not? Is there a direct effect of ξ1-variable on a η-variable, or an indirect effect only? (2) A model assuming a relationship between two latent variables is compared with 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 with 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 fits by computing a χ^2 difference test, meaningful only if the models in question are nested models, i.e.

Table 6 Comparative model analysis

No.	Model type	X^2	df	X^2_{diff}	p value	Recommendation
1	Saturated model	0	0		0.000	
2	Default model	33.34	10	18.307	0.000	Insignificant
3	Proposed model	52.265	39	54.572	0.000	Significant

one of the models could be obtained simply by fixing/eliminating parameters in the other model (Werner and Schermelleh-Engel 2010). Similarly, this study adopted their strategy by having additional path in the structural model, which we called a saturated model; additional loadings in a measurement model 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 and Schermelleh-Engel (2010).

To compute a X^2 difference test, the difference in the X^2 values of the two models in question is taken as well as the difference in the degrees of freedom as shown in the equation given 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 with more degrees of freedom, whereas l denotes the "larger" model with more parameters and thus with 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. According to Werner and 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 fit 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 6).

On the one hand, the calculated Chi-square score for X^2 (2), 33.34, is greater than the X^2_{diff} value, 18.307, and this result fails to support the goodness of fit, and hence not significant. On the other hand, the Chi square test score for the Goodness of Fit for X^2 (3), 52.265, was statistically significant since it was less than that for X^2_{diff}, 54.572.

Conclusion and future work

m-learning systems carry similar risks as other information systems do, and hence, compliance officers have to be diligent with respect to privacy aspects. In this study, we proposed, developed, and validated a model for a secure location-based privacy-preserving mobile learning in distance education. This was achieved through a thorough research on the existing theories for m-learning adoption and by evaluating learners' behavioral intention to use location-aware m-learning systems. This study has affirmed the prior literature that indeed perceived risk, privacy concerns, and Trust affects the behavioral intention to use new technology. In addition, we established through empirical evidence that privacy awareness has profound impact on behavioral intention to use m-learning systems for distance education.

In light of the Internet usage, globalization, and rapid uptake of location-aware mobile gadgets among individuals in educational setup, it will also be of great interest to extend this study to include societal and cultural factors in the future.

References

Adams, A., & Blandford, A. (2003). Security and online learning: To protect or prohibit. *Usability of online learning programs* (pp. 331–359). UK: IDEA Publishing.

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.

Beldad, A., de Jong, M., & Ateehoulder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behaviors, 26*(5), 857–869.

Bettini, C., Wang, X., & Jajodia, S. (2005). Protecting privacy against location-based personal identification. In *Secure data management. Volume 3674 of Lecture Notes in Computer Science* (pp. 185–199). Berlin/Heidelberg: Springer.

Buthpitiya, S., Zhang, Y., Dey, A., & Griss, M. (2011). n-gram geo-trace modeling. In *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.

Chellappa, R., & Sin, R. (2005). Personalization versus privacy: An empirical examination of the online consumer's Dilemma. *Information Technology and Management, 6,* 181–202.

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, 9*(4), 125–130.

Dinev, T., & Hart, P. (2006a). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7–29.

Dinev, T., & Hart, P. (2006b). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

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. (2006). *Location privacy and location-aware computing*. Australia: University of Melbourne.

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*(02), 14–23.

Glover, S., & Benbasat, I. (2011). A comprehensive model of perceived risk of e-commerce transactions. *International Journal of Electronic Commerce, 15*(2), 47–78.

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. In *Annual meeting of the association for the study of higher education.* Portland: Oregon.

Hwang, G.-J. (2015). Mobile technology-enhanced learning. In Z. Yan (Ed.), *Encyclopedia of mobile phone behavior* (Vol. 1, pp. 541–548). IGI Global.

Hwang, G.-J. (2017, February 10). *Mobile Learning research in specific disciplines.* Retrieved from ouhk.edu.hk: http://www.ouhk.edu.hk/URC/Seminar_Prof%20Gwo-Jen%20Hwang.pdf

Hwang, G., Tsai, C., & Yang, S. (2008). Criteria, strategies and research issues of Context-aware ubiquitous learning. *Educational Technology & Society, 11*(1), 81–91.

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, 6*(3), 67–84.

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, July 20). *WarpPLS 3.0 User Manual.* Retrieved from 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. (2015b). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1–10.

Kukulska-Hulme, A. (2013). Aligning migration with mobility: Female immigrants using smart technologies for informal learning show the way. *UNESCO Mobile Learning Symposium.* Paris. Retrieved from unesco.org: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/ED/ICT/pdf/Kukulska-Hulme.pdf

Kumar, et al. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems, 9*(1), 254–264.

Lee, M.-C. (2009a). 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.

Lee, M.-C. (2009b). 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.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review. *Communications of the Association for Information Systems.*

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, Y., et al. (2012). A unified risk-benefit analysis framework for investigating mobile payment adoption. In: *2012 international conference on mobile business.*

Lowry, P., Cao, J., & Everrard, A. (2011). *Privacy concerns versus desire for interpersonal awareness in driving the sue of self-disclosure technologies: The case of instant messaging in two cultures. Journal of Management Information Systems, 27*(4), 163–200.

MacCarthy, M. (2014). Student privacy: Harm and context. *International Review of Information Ethics, 21,* 11–24.

Mason, R. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), 4–12.

Musau, F., & Obiria, P. (2013). *Transparent computing: A new paradigm for increased user friendliness in service sharing*. Kenyatta University Institutional Repository.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

Obiria, P., Kimwele, M., & Cheruiyot, W. K. (2015a). A secure location-based privacy preserving framework for M-learning adoption to enhance distance education in Kenya: Work in progress. *International Journal of Advanced Studies in Computer Science and Engineering (IJASCSE), 4*(9), 1–7.

Obiria, P., Kimwele, M., Cheruiyot, W., & Mwangi, G. (2015b). A location-based privacy preserving framework for M-learning adoption to enhance distance education in Kenya: Literature review. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), 4*(10), 7–14.

Okazaki, S., Hairong, L., & Morikazu, H. (2009). *Consumer privacy concerns and preferences for degree of regulatory control. Journal of Advertising, 38*(4), 63–77.

Omar, K., Aláa, & Al-Nasrallah. (2011). Determinants of e-Gov adopt in Kuwait: The case of the traffic violation E-payment system (TVEPS). In *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.

Pfitzmann, A., & Ohntopp, M. (2001). Anonymity, unobservability, and pseudonymity a proposal for terminology. In *Designing privacy enhancing technologies, volume 2009 of Lecture Notes in Computer Science* (pp. 1–9). Springer.

Podsakoff, P., MacKenzie, S., & Podsakoff, N. (2003). Common method biases in behavioral research: A critical review of the literature 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.

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), iii–xiv.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society, 36,* 111–147.

Tabachnick, B., & Fidell, L. (2007). *Using multivariate statistics* (5th ed.). Boston: Pearson Education Inc.

Thietart, R. (2007). *Doing management research: A comprehensive guide*. Paris: Sage.

Urbach, N., & Ahlemann, F. (2010). Structural equation modelling in information systems using partial least squares. *Journal of Information Technology Theory and Application, 11*(2), 5–40.

Wagner, E. (2008). Realizing the benefits of mobile learning. *Journal of Computing in Higher Education, 20*(2), 4–14.

Werner, C., & Schermelleh-Engel, K. (2010). Deciding between competing models: Chi square difference tests. In *Introduction to structural equation modeling with LISREL—version February 2010.* Frankfurt: Goethe University.

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

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. (2011). 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).

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), 135–144.

Peter B. Obiria is a Research Scholar in the School of Computer Science and Information Technology at the Jomo Kenyatta University and Agriculture. He is a PhD candidate at the same institution and holds a master of science in computer systems. His research interests include pervasive computing, privacy in information systems, Big Data, and location-aware mobile systems.

Micheal W. Kimwele is a Senior Lecturer and Deputy Director in the School of Computer Science and Information Technology at the Jomo Kenyatta University and Agriculture. He is a PhD holder in Information Technology and his research interests include mobile computing, ubiquitous computing, and security in information systems among others.