TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 10, 2020

A new decade for social changes

www.techniumscience.com

ISSN 2668-7798

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

Investigating the nexus between Mobile Apps Adoption and Privacy Concerns among Users: An Empirical Analysis from Ghana

Acheampong Owusu[1], Ivy Hawah Taana[2], Akeem Soladoye Bakare[3], Daha Tijjani Abdurrahaman[4], Frederick Edem Broni Jr.[5]

[1 5]Operations and Management Information Systems Department, University of Ghana Business School, Legon, Accra, [2 3 4]Limkokwing University of Creative Technology, Cyberjaya, Malaysia,

aowusu@ug.edu.gh

Abstract. There has been a proliferation of Mobile Phones Applications commonly referred to as Mobile Apps lately due to the advancement of technology. These Mobile Apps are used for a myriad of tasks ranging from Mobile Commerce (m-commerce), healthcare, learning, social media, among others. However, with this spread of the Mobile Apps comes the issues of privacy concerns. This study, therefore, seeks to investigate why users continue to use the Mobile Apps despite the privacy concerns and what measures they have put in place to mitigate this menace. Through the Antecedents, Privacy, Concerns, and Outcome (APCO) model, the study developed a research model that was hypothesized and evaluated with 316 respondents from a tertiary institution. The data was analyzed through the partial least squares structural equation model (PLS-SEM). The results indicate that whilst antecedent variable Gender influences Privacy Concern, Experience on the other hand does not. Also, Enjoyment, Privacy Risk, and Trust influence Usage Continuance Intention. Also, Application Popularity influences Change Privacy Settings. Again, Privacy Concern influence Privacy Risk but does not influence Trust. Moreover, Enjoyment, Privacy Risk, and Trust do not influence Change Privacy Settings. This study has given the researchers insights as to why users continue to use Mobile Apps despite the Privacy Concerns that have been raised in the literature. Other implications for theory, policy, and practice are also discussed.

Keywords. Mobile Apps, Privacy Concerns, Ghana

1. Introduction

In recent times, technology has advanced which has made mobile devices parsimonious. Thus, there is a proliferation of Mobile devices such as smartphones, tablets among others globally and this is progressing steadily in most developing economies such as Ghana. The statistics show that currently, Ghana has "the highest mobile penetration in West Africa and already outperforms many of its regional peers". As at the "end of 2019, mobile adoption stood at 55 percent, higher than the regional average which is at 44.8 percent". Thus, "a huge number of people can be served through digital services, positively impacting the growth of the digital economy" (Omondi, 2020). Omondi (2020) further stated that "as of the third quarter of 2019, Ghana counted 16.7 million unique mobile subscribers, 15.1 million smartphone devices, and 10.7 million mobile internet users in the country (as of Q3 2019). 3G coverage accounts for 60 percent of the total connections, 4G has

started gaining traction and will overtake 2G services by 2023. 3G and 4G will account for nearly 95 percent of total connections by 2025" (Omondi, 2020).

A common phenomenon lately in the mobile devices' ecosystem is the development of mobile phones applications (commonly referred to as apps) for the main three mobile devices platforms i.e. iOS, android and windows (Hoehle & Venkatesh, 2015) where users can run various types of these "apps for a broad range of purposes, including searching for online information, playing games, making purchases, and staying connected with others" (Byun, Chiu, & Bae, 2018). As a result, users are downloading, installing, and using all sorts of these apps ranging from those used for m-commerce/electronic commerce (e-ecommerce) (Sun, Fang, & Hwang, 2019; Zhang, Chen, & Lee, 2013), social media/entertainment (Benamati, Ozdemir, & Smith, 2017; Lankton & Tripp, 2013; Ozdemir, Jeff Smith, & Benamati, 2017), health (Conroy, Yang, & Maher, 2014; Martínez-Pérez, De La Torre-Díez, López-Coronado, & Herreros-González, 2013), religion (Campbell, Altenhofen, Bellar, & Cho, 2014; Díez Bosch, Micó Sanz, & Sabaté Gauxachs, 2017; Richardson et al., 2020), learning and research (Pindeh, Suki, & Suki, 2016; Zydney & Warner, 2016), language learning (Godwin-Jones, 2011; Pindeh et al., 2016), sports (Byun et al., 2018; Guo et al., 2017; Hing, Russell, Li, & Vitartas, 2018; Modave et al., 2015), betting (Hing et al., 2018; Lopez-Gonzalez & Griffiths, 2018), gaming (Balakrishnan & Griffiths, 2018; Christensen & Prax, 2012; Lopez-Gonzalez & Griffiths, 2018; Merikivi, Tuunainen, & Nguyen, 2017), among others. Whilst most of these apps are free, others demand a token fee from the users. The free ones are sometimes overwhelmed with adverts, in-app purchases and also seek to exploit user's privacy by asking for access to contacts list, pictures, documents, email, among others. Naive users who consent to these sometimes find their privacy being violated.

Although, these apps are handy and have been making life more convenient for users as services that hitherto would have required users to travel to offices, etc. to transact business, can be done in one's place of convenience (Pagoto, Schneider, Jojic, Debiasse, & Mann, 2013). In Ghana for instance, lately, the government of Ghana is in a digitalization drive where many services such as acquiring Passports, Driving License, National Insurance Card, Ghana Lottery, Payment of Utility Bills (electricity, water etc.) (http://www.eservices.gov.gh/), among others are all having apps that users install and can use at their convenience. Due to the sensitivity of the data and the transactions involved, some of these apps are highly secured to prevent fraudsters from duping users. However, when it comes to the generic apps for social media, entertainment (games, etc.), among others, security may not be that strong. Thus, a user's privacy can be compromised. Some of these generic apps in some instances, demand access to the user's Phone Contact Book, Location, Pictures, Videos, Music, etc. which can highly be a violation of the user's privacy.

Thus, this study seeks to investigate why users continue to use Mobile Apps despite the privacy concerns and what measures they have put in place to mitigate this menace. Knowing these will help inform policymakers and Apps developers as to what measures they should put in place to mitigate some of the issues of privacy concerns arising from the use of Mobile Apps.

The rest of the paper is as follows. The next section introduces readers to the Literature review which discusses the concept of Mobile Apps, its applications, and benefits derived from their usage. The section further discusses the underpinning theory, related studies about Mobile Apps, and the conceptual development with the formulation of hypotheses. The next section talks about the Methodology with the survey questionnaire, sampling, and the data collection method. This is followed by the data analysis technique used and the discussions of the findings. The conclusion then follows with implications and suggestions for future studies.

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

2. Literature Review

2.1 The concept of Mobile Apps

Mobile Apps are pervasive lately and have permeated every aspect of our lives as a result of the proliferation of Smartphones which has made it easier for the development of these Apps (Statista, 2016).

The Vodafone Group (2015, p. 211) and Byun et al. (2018) defined Mobile Apps as software programs "designed to run on smartphones or tablet devices and provide a convenient means for the user to perform certain tasks". Also, Hoehle and Venkatesh (2015) in conceptualizing a Mobile Apps refers to it as "an IT software artifact that is specifically developed for mobile operating systems installed on handheld devices, such as smartphones or tablet computers". They further averred that Mobile Apps either come "preinstalled on mobile devices or can be downloaded from various mobile application stores" (e.g., Apple's iTunes store, Android Playstore, Microsoft store).

The benefits of Mobile Apps are numerous and usually depends on the purpose in which they are developed for. In most instances, the use of Mobile Apps provides convenience to end-users which can help in reducing costs. Some of the highlighted benefits in the literature include the applications of Mobile Apps for weight loss (Pagoto et al., 2013), learning and research (Zydney & Warner, 2016), getting connected (Benamati et al., 2017; Lankton & Tripp, 2013) among others.

2.2 Underpinning theory

This study is underpinned by the Antecedents, Privacy, Concerns, and Outcome (APCO) model propounded by (Smith et al., 2011). The APCO model (Smith et al., 2011) suggests antecedents variables Privacy Experience and Demographic Privacy Differences (e.g. Gender, Age, among others) will influence Privacy Concerns. They continue to declare that Privacy Concerns will influence Trust and Privacy Risk/Costs. Also, Trust, Privacy Risk, Benefits, and Perceived Application Popularity will influence user's Usage Continuance Intention and the Behavioral Reactions (e.g., self-disclosure, risks, and regulation) of the application.

Although the APCO model has been used extensively to study different phenomenon such as e-commerce/m-commerce (Sun et al., 2019; Zhang et al., 2013), social media sites (e.g. Facebook) (Benamati et al., 2017; Ozdemir et al., 2017), sharing economy (Li, Lee, & Yang, 2019) among others, little is known about it when it comes to that of Mobile Apps which have seen extensive growth lately. This study thus aims to contribute theoretically in this regard to fill the gaps left in the literature.

2.3 Related studies about Mobile Apps

In this section, we present the related studies about Mobile Apps privacy concerns in the literature.

Table 1: Related studies

Article	Theory	Methodology	Context	Findings
Alashoor, Han, and Joseph (2017)	Protection motivation theory The theory of planned behavior APCO Model	Survey Questionnaires with SEM	USA	The findings show "awareness of big data implications had a positive impact on privacy concerns. In turn, privacy concerns impacted self-disclosure concerns positively and self-disclosure accuracy negatively".
Li, Lee, Chang, and Yang (2020)	APCO Model	Conceptual	USA	
Sun et al. (2019)	APCO Model	Survey Questionnaires	China	The results "indicate that hot topic interactivity and group buying experience have

				significant negative impacts on privacy concerns and significant positive impacts on perceived benefits. Privacy concerns negatively influence the behavior of information disclosure while perceived benefits positively influence the behavior of information disclosure".
Dinev, Mcconnell, and Smith (2015)	APCO Model	Conceptual		
Ozdemir et al. (2017)	APCO Model	Survey Questionnaires with SEM	USA	The findings show that "both privacy experiences and privacy awareness are quite significant predictors of privacy concerns." The results also show that "trust, risk, benefits, and privacy concerns work together to explain a large amount (37%) of the variance in disclosure behaviors".
Benamati et al. (2017)	APCO Model	Survey Questionnaires	USA	The results suggest that "PA and gender are important explanators for CFIP, which in turn explains privacy-protecting behaviors". The results also show that "perceived risk affects trust, which in turn affects behaviors in the studied context".
Zhang et al. (2013)	APCO Model	Survey Questionnaires	USA	The results show that "the consumers' demographic differences have varying degrees of impact on their concerns for information privacy in the context of m-commerce".
Buck (2017)	APCO Model	Survey Questionnaires	German	The results show "significant correlations to the concerns users have about their privacy – an increasing future self-continuity is related with higher concerns".
Lankton and Tripp (2013)	APCO Model	Survey Questionnaires	USA	The results indicate "Experience does not influence privacy concern but gender does. Privacy concern has positive significant effects on privacy risk and change privacy settings but has no significant effects on trust, limit number friends,

			differentiate friends, and continuance intention". The results also revealed that "neither trust nor privacy risk have significant influences on the privacy behaviors but do significantly influence continuance intention". Also, "enjoyment influences continuance intention".

As indicated in Table 1, most of the studies about the APCO model have focused on Social Media, e-commerce, m-commerce, sharing economy among others. Also, in terms of the context, the focus has been on developed economies leaving the developing economies behind. Thus, this study will add up to the scanty literature in the developing country context.

2.4 Conceptual Model and Hypotheses Development

The formulation of hypotheses for the various relationships unearthed in the APCO macro model is done in this section. Table 2 presents the meanings of the constructs used in this research and illustrates how they correlate to the APCO constructs. The research model is presented in Figure 1 which was developed based on the APCO model as discussed above and extant literature.

Table 2: Constructs, their definitions and supporting literature

Construct (In this study)	**APCO Model Variable**	**Definition**	**Supporting Literature**
Experience	Privacy Experiences	Length and frequency of prior apps' use	(Dinev et al., 2015; Lankton & Tripp, 2013; Li et al., 2020, 2019; Metzger, 2007)
Gender	Demographic Differences Privacy	Gender	(Benamati et al., 2017; Lankton & Tripp, 2013; Metzger, 2007; Ozdemir et al., 2017)
Privacy Concerns	Privacy Concerns	Concerns about opportunistic behavior related to personal information that is disclosed by the respondent in particular	(Alashoor et al., 2017; Benamati et al., 2017; Dinev et al., 2015; Lankton & Tripp, 2013; Li et al., 2020, 2019; Metzger, 2007; Ozdemir et al., 2017)
Privacy Risk	Risks/Costs	Concerns about opportunistic behavior "related to personal information that is disclosed by the respondent in general"	(Benamati et al., 2017; Lankton & Tripp, 2013; Ozdemir et al., 2017; Zimmer, Arsal, Al-Marzouq, & Grover, 2010)
Enjoyment	Benefits	The extent to which using the apps are "perceived to be enjoyable in its own right, apart from any	(Buck, 2017; Dinev et al., 2015; Lankton & Tripp, 2013; Ozdemir et

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

		performance consequences that may be incurred"	al., 2017; Sun et al., 2019)
Trust	Trust	This is "being willing to depend on the website, or a volitional preparedness to make oneself vulnerable"	(Alashoor et al., 2017; Benamati et al., 2017; Dinev et al., 2015; Lankton & Tripp, 2013; Ozdemir et al., 2017; Zimmer et al., 2010)
Application Popularity		refers to the fact that many people like something or someone"	(Cambridge, 2016)
Change Privacy Settings	Behavioral Reactions	Refers to "whether the vendor-provided privacy settings have been changed"	(Lankton & Tripp, 2013)
Usage Continuance Intention		Intentions to continue using free apps	(Lankton & Tripp, 2013; Li et al., 2020, 2019; Rezaei, Shahijan, Amin, & Ismail, 2016)

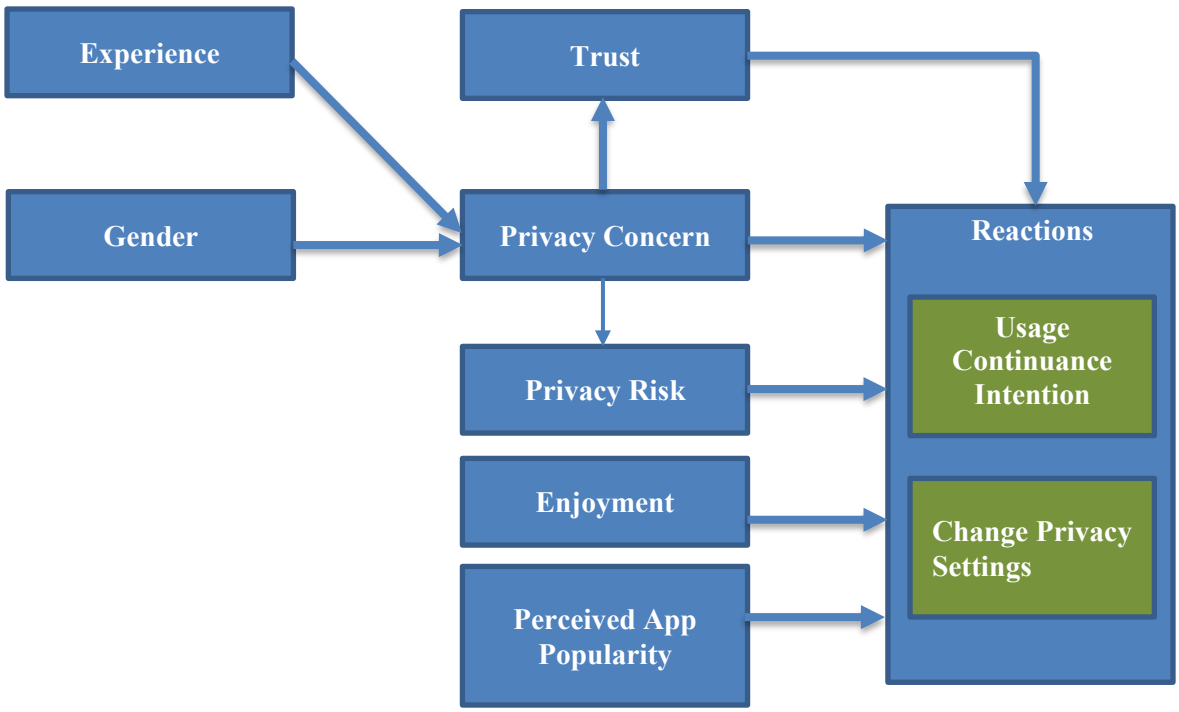

Figure 1: Conceptual model

Experience – The mobile apps "model includes privacy experience as an antecedent to privacy concern because individuals who have been exposed to or been the victim of personal information abuse should have stronger privacy concerns" (Smith et al., 2011). Additionally, Tuqfekci (2008) "finds that nonusers of a social network site had higher privacy concerns than users". We include "the prior experience to capture these effects, as users with more prior experience are more likely to have encountered privacy abuses". Besides, Sun et al. (2019) in their study find out that "the consumers' demographic differences have varying degrees of impact on their concerns for information privacy in the context of m-commerce". In another study, Ozdemir et al. (2017) established that "both privacy experiences and privacy awareness are quite significant predictors

of privacy concerns". Also, Lankton and Tripp (2013) find out that "Experience does not influence privacy concern".

Based on the above discussions, it is there hypothesized that:
H1: Experience will positively influence Privacy Concern

Gender – We use gender in our model to address population disparities as suggested by mobile apps. Researchers have found that females are more interested in privacy than males in general. Sheehan (1999) reports, for example, that females are more interested than males when an app claims its publicly identifying information is accessed by certain companies. We say that it is less relaxed for females to be in touch with unknown individuals than for males to be worried about the opportunism of those in mobile apps. Furthermore, Fogul and Nehmad (2009) identified females with much more mobile apps privacy issues than males, suggesting that females have less control over the security of their privacy than males by implicit social contracts. Also, Zhang et al. (2013) find that "the consumers' demographic differences have varying degrees of impact on their concerns for information privacy in the context of m-commerce". In another study, Lankton and Tripp (2013) find out that "Gender does not influence privacy concern".

Based on the above discussions, it is there hypothesized that:
H2: Females will have greater Privacy Concerns than Males

Privacy Concerns – Privacy concern negatively affects Trust since larger concerns may make "one less likely to feel they can rely or depend on the technology". Whilst Privacy Concern "relates to the likelihood of not having desirable results, Trust refers to the likelihood that one can depend and rely on the trustee to perform desirable actions" (Fogel & Nehmad, 2009; Owusu, Broni Jnr, & Akakpo, 2019). This implies a negative relation amongst the variables. Empirical research demonstrates that "Privacy Concern negatively influences Trust" (Eastlick et al., 2006). In another study, Lankton and Tripp (2013) established that "Privacy Concern has positive significant effects on Privacy Risk".

Based on the above discussions, it is there hypothesized that:
H3: Privacy Concern will positively influence Privacy Risk

Mobile Apps "depicts privacy risk, trust, and behavioral reactions as outcomes of Privacy Concerns" (Fogel & Nehmad, 2009). Both Privacy Concern and Privacy Risk signify "the costs of disclosing information" (Dinev & Hart, 2006). The two variables are "highly related because perceptions that one's personal information might be used opportunistically can influence one's perceptions that personal information, in general, might be used opportunistically". In a study by Lankton and Tripp (2013), they found that "Privacy concern has no significant effects on trust".

Based on the above discussions, it is there hypothesized that:
H4: Privacy Concern will negatively influence Trust

Mobile apps also predict that privacy concerns will affect behavioral reactions. The more mobile app privacy concerns "the more one is likely to exercise privacy behaviors to control their personal information and prevent bad things from happening". Privacy concerns can make mobile apps "users more likely to take action to protect their privacy". In mobile apps, "privacy behaviors can include changing vendor privacy settings" (change privacy settings) (Lankton et al., 2012), "limiting the number of friends in one's friends' list (limit number friends) and allowing only friends one has interacted with a lot in one's friends list (differentiate friends)" (Debatin et al.,

2009; Stutzman & Kramer-Duffield, 2010). These "responses to high concerns are consistent with expectancy theory's explanation that individuals are motivated to minimize negative outcomes" (Dinev & Hart, 2006). We also "include usage continuance intention in our model as a behavioral reaction to privacy concerns" because some mobile apps "users might discontinue use if their concerns are too high". A study by Lankton and Tripp (2013) established that "Privacy concern has no significant effects on continuance intention".

Based on the above discussions, it is there hypothesized that:
H5a: Privacy Concern will positively influence Usage Continuance Intention.
H5b: Privacy Concern will negatively influence Change Privacy Settings.

Trust - Mobile Apps also predict that "Trust and the Privacy Risks and benefits involved in the privacy calculus decision will influence behavioral reactions" (Fogel & Nehmad, 2009). Trust "plays an important role in predicting privacy behaviors" (Dinev & Hart, 2006). Trust lowers "the perceived concerns about revealing information making one feel that disclosure is a safe activity" (Metzger, 2004). If someone decides an app "is dependable and reliable one will be less likely to take steps to keep information private". Trust "also predicts usage continuance intentions because when one is willing to depend, one makes a conscious choice to put aside doubts and move forward with the relationship" (Holmes, 1991). Benamati et al. (2010) find that "Trust influences intention to use a bookseller website". Lankton and Tripp (2013) in their study established that "Trust has no significant influence on Change Privacy Settings but do significantly influence Continuance Usage Intention".

Based on the above discussions, it is there hypothesized that:
H6a: Trust will negatively influence Usage Continuance Intention.
H6b: Trust will positively influence Change Privacy Settings.

Privacy Risk - The final relationships that deal with mobile apps "are the effects of Privacy Risks and benefits on behavioral reactions" (Fogel & Nehmad, 2009). Similar to "Privacy Concerns, Privacy Risks should increase the likelihood of engaging in privacy behaviors to protect the opportunistic use of personal information" (Wu et al., 2012). These risks "should also make one less likely to want to continue" using mobile apps. In another study, Lankton and Tripp (2013) established that "Privacy Risk has no significant influence on change privacy settings but do significantly influence Usage Continuance Intention".

Based on the above discussions, it is there hypothesized that:
H7a: Privacy Risk will positively influence Usage Continuance Intention.
H7b: Privacy Risk will positively influence Change Privacy Settings.

According to previous studies that inspire the mobile apps model, "benefits from using technology should decrease one's privacy behaviors and increase continued use". We contemplate Enjoyment as a gain of mobile apps use because "Enjoyment is a major reason people use social networking apps" (Xu et al., 2008). The more "enjoyable using the mobile apps, the less likely one will engage in privacy behaviors because this might stifle one's ability to make use" of the app. Enjoyment is "part of the extended unified theory of acceptance and use of technology for consumers as a predictor of continuance intention" (Venkatesh et al., 2012). People will "want to continue using a technology they find enjoyable". Prior research finds "that enjoyment significantly influences the intention to continue using mobile apps" (Sledgianowski & Kulviwat, 2009). In another study, Lankton and Tripp (2013) established that "enjoyment influences continuance intention".

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

Based on the above discussions, it is there hypothesized that:
H8a: Enjoyment will positively influence Usage Continuance Intention.
H8b: Enjoyment will negatively influence Change Privacy Settings.

Popularity - The popularity of apps has a positive effect on the behavior of people to continue using the app (Ferdous, Osmani, & Mayora, 2015a). Ferdous, Osmani, and Mayora (2015b) contend that "smartphone app usage behavior is driven by factors such as the popularity of apps (e.g., how many categories of apps a user visited and how is his/her attention spread), frequency and duration of app usage (e.g., how often does a user use any application and how long is the app used), frequency of unique apps used (e.g., if the user keeps using only a few apps regularly or the list of his/her visited apps is large)". In a study by Ferdous et al. (2015a), they found out that "perceived app popularity makes them less concerned" and also "a positive effect of perceived App Popularity on download intention". Also, in another study, Shen (2015) find out that "Apps' Popularity is more effective when the app carries low perceived risk" which leads to Usage Continuance Intention.

Based on the above discussions, it is there hypothesized that:
H9: App popularity will positively influence Usage Continuance Intention.
H9: App popularity will positively influence Change Privacy Settings.

3. Methodology

The quantitative approach with the survey method was used for this study. Data was collected through a survey method with stratified and convenience sampling from 316 students from a tertiary institution in Ghana. The questionnaire comprises three sections with section one asking questions about the respondent's demographics. Section two dealt with the antecedent variables and the independent variables whilst the last section asks questions about the dependent variables. The Constructs were operationalized as follows: Experience has 2 items, Application Popularity, Trust, and Enjoyment all have 3 items each, Privacy Concerns and Privacy Risk each has 4 items. All these constructs were measured on a 5-point Likert Scale with "1" representing "Strongly Disagree" and "5" representing "Strongly Agree". The items were adapted from (Smith et al., 2011; Fuller, Serva, & Benamati, 2007; LaRose & Rifon, 2007; Smith, Milberg, & Burke, 1996)). The data was collected through a hand-delivering questionnaire where the students were given ample time to fill the questionnaire in their respective halls of residence and return them on a given date. It took almost three months to collect the data.

4. Analysis and Findings

The demographics were analyzed through SPSS version 22 and the inferential statistics done through Partial Least Squares Structural Equation Modeling (PLS-SEM) specifically with SmartPLS 3.3.2

4.1 Respondents Demographics

Table 3: Respondents Demographics

Variable	Item	Frequency	Percentage
Gender	Male	153	48.4
	Female	163	51.6
Age	Below 20	0	0
	20-29	66	20.9
	30-39	122	38.6
	40-49	74	23.4
	50-59	54	17.1
	60+	0	0

Use SmartPhone?	Yes	316	100
	No	0	0

Table 3 shows the demographic profile of the respondents. 48.4% of the respondents were males whilst 51.6% were females. Thus, the majority of the respondents were females. In terms of the Age distribution of the respondents, 38.6% of the respondents were found in the 30-39 age categories followed by 23.4% who were found in the 40-49 age categories. The greater percentage of the age distribution is above 30 years because most of the respondents were students doing their Masters's degree. Regarding the respondents' usage of Smart Phones, all of them declared they used smartphones. This is an indication of the proliferation of Smartphones in the Ghanaian economy.

4.2 Inferential statistics

The survey data collected were subjected to partial least squares structural equation modeling (PLS-SEM) where the 2-step approach of analyzing data in SEM was employed. The measurement model was assessed firstly, which was then followed by the evaluation of the structural model (Hair et al. 2017). SmartPLS 3.3.2 (Ringle et al., 2015) was used to assess both the measurement and structural models. The use of PLS-SEM is justified by its popularity lately in terms of handling of data that is not normally distributed and handling of complex research models like our conceptual model in this study (Hair et al., 2014, p. 19). Thus, PLS-SEM has been used in a lot of recent studies which includes (Abdurrahaman, Owusu, & Bakare, 2020; Owusu, 2017, 2019; Owusu, Agbemabiese, Abdurrahaman, & Soladoye, 2017; Owusu, Ghanbari-Baghestan, & Kalantari, 2017) in Information Systems and (Abdurraham, Owusu, Soladoye, & Kalimuthu, 2018; Bakare, Owusu, & Abdurrahaman, 2017) in Advertising and Marketing.

4.2.1 Assessing the Measurement Model

4.2.1.1 Reliability and Validity Test

Creswell (2012, p.159) defines Reliability as “scores from an instrument are stable and consistent.” Also, Saunders et al. (2009, p.156) defined reliability as “the extent to which your data collection techniques or analysis procedures will yield consistent findings”. Furthermore, Creswell (2014, p. 200) asserted that the “validity and reliability of scores on instruments are prime to meaningful interpretations of data”.

Reliability comes in different forms. One form is “internal consistency” which is computed by calculating the Cronbach’s alpha (Saunders et al. 2009, p.374; Hair et al. 2014, p.101). Also, “Cronbach’s alpha measures the degree to which” the items used are “internally reliable with other items” including the construct. This “takes values ranging” from “1 (which indicates the items correlate perfectly) and 0 (which denotes the items are totally inconsistent)”. An “alpha score of above 0.70 indicated internal consistency and was considered reliable” (Nunnally, 1978).

Table 4: Results of Construct Reliability and Validity Test

Constructs	Indicators	Outer Loadings	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Change_Privacy_Settings	**Change_Privacy_Settings**	**1.00**	**1.00**	**1.00**	**1.00**
Enjoyment	**Enjoyment1** **Enjoyment2**	**0.848** **0.880**	**0.832**	**0.899**	**0.748**

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

	Enjoyment3	0.868			
Exp	Exp1 Exp2	-0.553 0.694	0.712	0.716	0.693
Gender	Gender	1.00	1.000	1.00	1.00
Perc_App_Pop	Perc_App_Pop1 Perc_App_Pop2	0.493 0.832	0.702	0.805	0.678
PrivCon	Priv_Con1 Priv_Con2 Priv_Con3 Priv_Con4	0.817 0.869 0.915 0.890	0.878	0.917	0.734
Priv_Risk	Priv_Risk1 Priv_Risk2 Priv_Risk3 Priv_Risk4	0.862 0.896 0.887 0.778	0.896	0.928	0.763
Trust	Trust1 Trust2 Trust3	0.793 0.869 0.888	0.812	0.887	0.724
Usage_Cont_Int	Usage_Cont_Int1 Usage_Cont_Int2 Usage_Cont_Int3	0.938 0.949 0.903	0.923	0.951	0.866

The reliability test for this study's instrument was assessed through both Cronbach's alpha value as well as the composite reliability (Hair et al. 2014, p.98) as shown in Table 4. The data was also subjected to confirmatory factor analysis (CFA) to get insights as to the multidimensionality of the items using SmartPLS 3.3.2 (Ringle et al., 2015) and discriminant validity test. Cronbach alpha value "provides an estimate of the reliability based on the intercorrelations of the observed indicator variables" (Hair et al. 2014, p.101). Cronbach's alpha has a weakness of assuming all the indicators are equally reliable (that is "all the indicators have equal outer loadings on the construct") and it is also "sensitive to the number of items in the scale and generally tends to underestimate the internal consistency reliability" (Hair et al. 2014, p.101). However, composite reliability "takes into account the different outer loadings of the indicator variables" (Hair et al. 2014, p.101) and thus ensures more reliability on each construct.

Table 4 illustrates the summary measurement model with the "Cronbach Alpha, Composite Reliability, and the Average Variance Extracted (AVE) values" of all the constructs. As shown in Table 4, the test results revealed that all the latent "variables meet the Cronbach alpha value of 0.7 or higher" (Nunally, 1978), which "is the acceptable value for reliability". Also, the results indicate that all the "measures are robust in terms of their internal consistency reliability" which is shown by "the composite reliability". The composite reliabilities values of the different measures in the model range from 0.716 to 0.951 which well exceeds "the recommended value of 0.7" as shown in Table 4. Also, from Table 4, all the AVE values are well above 0.5. This proves that all the indicators for each construct converge very well to form the constructs (Hair et al. 2014, p.107). However, Change_Privacy_Settings and Gender each have only one indicator. As a result, the outer loadings, Cronbach alpha, Composite Reliability, and AVE all show 1. This is acceptable as indicated by Hair et al. (2014, p.).

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

Again, from Table 4, the confirmatory factor analysis illustrates acceptable factor loading on the hypothesized measurements. The outer loadings of almost all the indicators meet the acceptable value of 0.7 or higher which is recommended for indicator reliability with very few falling below 0.7. However, these indicators were maintained as (Wong, 2013) has recommended values of 0.4 or higher for exploratory research. The indicators below 0.7 have their values ranging from 0.553 (Exp1) to 0.694 (Exp2) and hence they were maintained. However, the outer loadings "Per_App_Pop3" has very low outer loading of 0.205. As a result, it was deleted.

Construct validity confirms if the items measure hypothetical constructs as planned (Creswell, 2014, p.206). This has become very helpful in recent studies and has "focused on whether the scores serve a useful purpose and have positive consequences when they are used in practice." Also, Creswell (2014, p.206) emphasized that "establishing the validity of the scores in a survey helps to identify whether an instrument might be a good one to use in survey research."

After the reliability test, the next analysis was to check the validity of the measures. This was done by the discriminant validity via the Fornell-Larcker criteria.

Table 5: Discriminant Validity - Fornell-Larcker Criterion

Constructs	Enjoyment	Exp	Gender	Perc_App_Pop	PrivRisk	Priv_Con	Trust	Usage_Cont_Int
Change_Privacy_Settings	1.00							
Enjoyment	0.865							
Exp	0.009	0.627						
Gender	-0.028	-0.084	1.000					
Perc_App_Pop	0.276	0.017	0.014	0.571				
PrivRisk	0.180	-0.059	0.102	0.064	0.857			
Priv_Con	0.197	0.045	0.119	0.100	0.607	0.873		
Trust	0.106	-0.063	0.089	0.135	0.050	0.034	0.851	
Usage_Cont_Int	0.287	0.040	0.038	0.155	0.226	0.119	0.361	0.931

From Table 5, all the constructs meet the satisfactory values for "discriminant validity based on the Fornell-Larcker Criterion" (Hair et al. 2014, p.105; Fornell & Larcker, 1981), as "the square root of each construct's AVE is greater than its highest correlation with any other construct".

4.2.1.2 Assessing the Structural Model

The structural model is assessed in the second stage only after determining that the measurement model satisfies all the acceptable values.

But before evaluating the structural model, the researchers assessed if collinearity exists among the constructs. Collinearity measures if the constructs are highly correlated and its refer to as multicollinearity if it involves more than two constructs ((Hair et al., 2014, p.218).

Collinearity issues are calculated by the computation of tolerance levels and the variance

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

inflation factor (VIF) values. The VIF is defined as the reciprocal of the tolerance (Hair et al., 2014, p.124). For PLS-SEM, Hair et al. (2014, p.125) and Hair, Ringle, and Sarstedt (2011) confirmed that "a tolerance value of 0.20 or lower and a VIF value of 5 and higher" respectively among the predictive constructs indicate a possible collinearity problem.

Table 6: Collinearity values for the predictive constructs

Constructs	Enjoyment	Exp	Gender	Perc_App_Pop	PrivRisk	Priv_Con	Trust	Usage_Cont_Int	Collinearity Problem (VIF>5)?
Change_Privacy_Settings									**No**
Enjoyment								**1.120**	**No**
Exp						**1.007**			**No**
Gender						**1.007**			**No**
Perc_App_Pop								**1.096**	**No**
PrivRisk								**1.035**	**No**
Priv_Con					**1.000**		**1.000**		**No**
Trust								**1.025**	**No**
Usage_Cont_Int									**No**

From Table 6, all the predictor constructs have their VIF values below 5, which implies that multicollinearity issues are not found among them. Therefore, the other test such as the significance of path coefficients, effect sizes, and so on can be carried on using the model.

4.2.1.3 Hypotheses testing

The bootstrapping technique was used for the testing of the hypotheses. SmartPLS 3.3.2 generates the t-value which "provides the statistical significance of the causal path between the constructs in the hypothesized model". Hair et al. (2014, p.164) declared that "for a two-tailed test, the popular critical t-values in PLS-SEM are 1.65 ($\alpha = 0.10$), 1.96 ($\alpha = 0.05$), or 2.57 ($\alpha = 0.01$)".

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

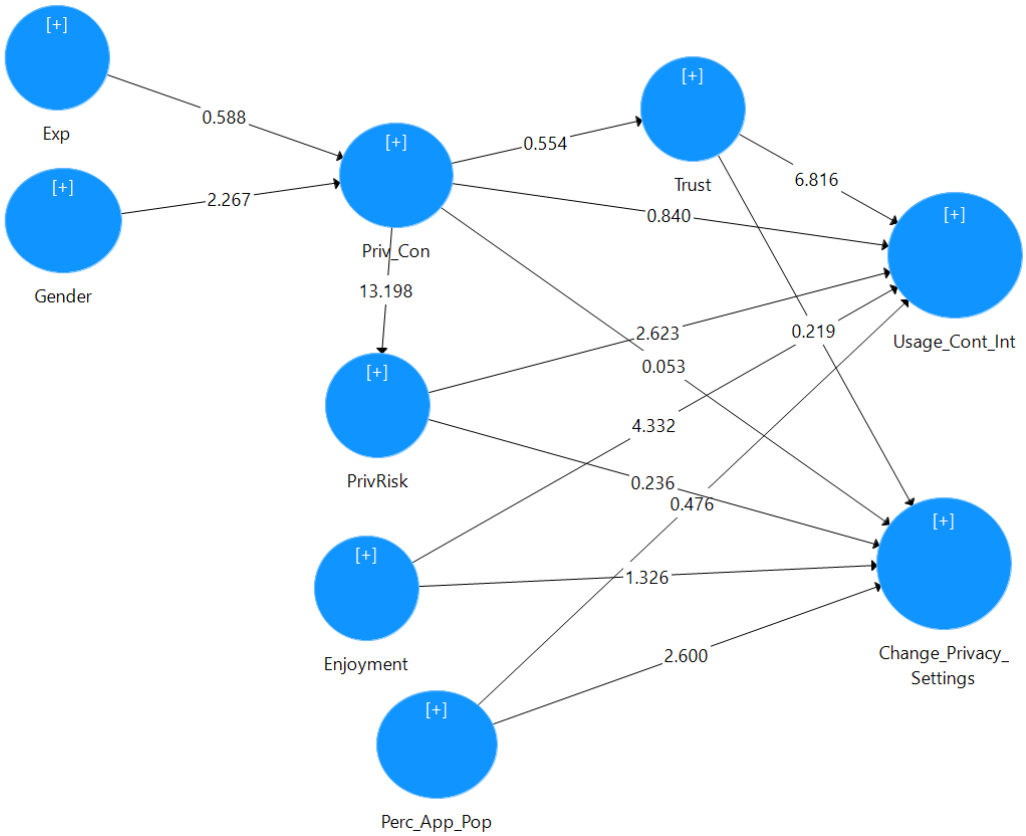

Figure 2: Structural Model

Table 7: Results of Hypotheses Testing

Paths	Hypothesis	β-value	t-values	P Values	Supported ?
Enjoyment -> Change_Privacy_Settings	H8b	-0.080	1.321	**0.186**	**No**
Enjoyment -> Usage_Cont_Int	H8a	0.237	4.423	**0.000**	**Yes**
Exp -> Priv_Con	H1	0.056	0.594	**0.552**	**No**
Gender -> Priv_Con	H2	0.124	2.225	**0.026**	**Yes**
Perc_App_Pop -> Change_Privacy_Settings	H9b	0.147	2.668	**0.008**	**Yes**
Perc_App_Pop -> Usage_Cont_Int	H9a	-0.030	0.472	**0.637**	**No**
PrivRisk -> Change_Privacy_Settings	H7b	0.016	0.230	**0.818**	**No**
PrivRisk -> Usage_Cont_Int	H7a	0.205	2.643	**0.008**	**Yes**
Priv_Con -> Change_Privacy_Settings	H5b	0.004	0.052	**0.959**	**No**
Priv_Con -> PrivRisk	H3	0.607	13.264	**0.000**	**Yes**
Priv_Con -> Trust	H4	0.034	0.554	**0.580**	**No**
Priv_Con -> Usage_Cont_Int	H5a	-0.058	0.831	**0.406**	**No**

Technium Social Sciences Journal
Vol. 10, 167-188, August 2020
ISSN: 2668-7798
www.techniumscience.com

Trust -> Change_Privacy_Settings	H6b	-0.012	0.217	**0.829**	**No**
Trust -> Usage_Cont_Int	H6a	0.332	6.743	**0.000**	**Yes**

Results from "the bootstrapping technique for the Structural Model signifying the t-values causal" links amongst the latent variables are shown in Figure 2 and Table 7, respectively. At "5% significance level (t-values ≥ 1.96)", Enjoyment-> Usage_Cont_Int (t = 4.423, p = 0.000), Gender -> Priv_Con (t=2.225, p=0.026), Perc_App_Pop -> Change_Privacy_Settings (t=2.668, p=0.008), PrivRisk -> Usage_Cont_Int (t=2.643, p=0.008), Priv_Con -> PrivRisk (t=13.264, p=0.000), and Trust -> Usage_Cont_Int (t=6.743, p=0.000) emerged significant. Therefore, hypotheses H8a, H2, H9b, H7a, H3, and H6a are accepted. However, Enjoyment -> Change_Privacy_Settings (t=1.321, p=0.186), Exp -> Priv_Con (t=0.594, p=0.552), Perc_App_Pop -> Usage_Cont_Int (t=0.472, p=0.637), PrivRisk -> Change_Privacy_Settings (t=0.230, p=0.818), Priv_Con -> Change_Privacy_Settings (t=0.052, p=0.959), Priv_Con -> Trust (t=0.554, p=0.580), Priv_Con -> Usage_Cont_Int (t=0.831, p=0.406), and Trust -> Change_Privacy_Settings (t=0.217, p=0.829) are insignificant. Therefore, hypotheses H8b, H1, H9a, H7b, H5b, H4, H5a, and H6b are all rejected.

Table 8: R^2, R^2 adjusted, f^2 and Q^2 values

Constructs	**R^2**	**R^2 Adjusted**	**f^2** Usage_Cont_Int	**f^2** Change_Privacy_Settings	**Q^2**
Change_Privacy_Settings	0.020	0.004			0.004
Enjoyment	-	-	0.051	0.006	-
Exp	-	-	0.003		-
Gender	-	-	0.015		-
Perc_App_Pop	-	-		0.019	-
PrivRisk	0.389	0.367			0.267
Priv_Con	0.017	0.011	0.584		0.008
Trust	0.001	-0.002	0.133		0.002
Usage_Cont_Int	0.223	0.213			0.184

4.2.1.4 The coefficient of determination - R square

Denoted as the $R^{2,}$ value, the coefficient of determination measures the model's predictive accuracy in PLS-SEM. The R^2 value is computed as "the squared correlation between a specific endogenous construct's actual and predicted value". The R^2 value "is the representation of all the exogenous latent variables" collective "effects on the endogenous construct". It is "also the amount of the variance in the endogenous constructs which is explained by all of the exogenous constructs linked to it" (Hair et al., 2014, pp. 174–175). The R^2 value has "a rule of thumb with values ranging from 0 to 1". Values of "0.75, 0.50, or 0.25 for endogenous latent variables have been specified as substantial, moderate, or weak, respectively" (Hair et al., 2014, p. 175).

From Table 8, the R^2 values of 0.389, 0.017, 0.001, and 0.223 indicate that the combined effects of exogenous latent variables Trust, Privacy Risk, Enjoyment, and Perceived Application Popularity explain 22.3% of "the variance of the endogenous construct" Usage Continuance Intention. Similarly, the exogenous latent variable Privacy Concern explains 38.9% on Privacy

Risk and 0.1% of Trust respectively. Also, antecedent variables Experience and Gender explain 1.7% of exogenous latent variable Privacy Concerns.

4.2.1.5 Effect sizes

Denoted as f^2, the effect size is "used to measure an exogenous latent variable's influence on an endogenous construct's" R^2 value. The f^2 value is used by researchers to measure the relevance of individual "latent variable's contribution in explaining the variance of the endogenous constructs". The rule of thumb for f^2 values ranges from "0.02, 0.15 and 0.35 indicating an exogenous construct's small, medium or large effect, respectively, on an endogenous construct" (Hair et al., 2014, p. 186).

From Table 8, with an f^2 value of 0.584, it emerged that Privacy Concern has the highest effect size on Privacy Risk. Also, with an f^2 value of 0.133, Trust has a medium effect on Usage Continuance Intention. Also, with an f^2 value of 0.051, Enjoyment has a small effect on Usage Continuance Intention. The rest have insignificant effect sizes on the Usage Continuance Intention.

4.2.1.6 Model's Predictive Relevance

The predictive relevance of the model was "assessed through the Stone–Geisser's Q^2 value" (Geisser, 1974; Stone, 1974). This "study followed the blindfolding procedure" via "the cross-validated redundancy approach as recommended by" (Hair et al., 2014, p. 183), "to calculate the Q^2 value". As shown in Table 8, the Q^2 values of 0.267, 0.008, 0.002, and 0.184 indicate the structural path model has predictive relevance as they are all above 0.

5. Discussions

This study set forth to investigate why users continue to use Mobile Apps despite the privacy concerns it brings. The findings from the analysis indicate that whilst antecedent variable Gender influences Privacy Concerns, antecedent variable Experience on the other hand does not influence Privacy Concerns. Also, Enjoyment, Privacy Risk, and Trust influence Usage Continuance Intention. Also, Application Popularity influences Change Privacy Settings. Again, Privacy Concern influence Privacy Risk but does not influence Trust. However, Enjoyment, Privacy Risk, and Trust do not influence Change Privacy Settings.

Antecedent variable Experience has been established to influence Privacy Concerns (Ozdemir et al., 2017). However, contrary to the hypothesized model, in this study, Experience does not influence Privacy Concerns. This finding is in support of the findings of (Lankton & Tripp, 2013). This may be due to the fact that the respondents sampled in this study are students who are relatively young and have not gotten much of life experience hence, in adopting mobile Apps they do not hinge their privacy concern on experience.

Research has proven that females have much more mobile apps privacy issues than males, suggesting that females have less control over the security of their privacy than males by implicit social contracts (Fogul & Nehmad, 2009). Thus, it was hypothesized that the antecedent variable (Gender) in terms of Females will have greater privacy concerns than males. Our results indeed have established the fact that females are more concerned in terms of their privacy issues in support of the findings of (Zhang et al., 2013). From this finding, it is apparent that the privacy concerns of the females who use mobile Apps should be given priority attention. This is to assure them of the protection of their information as such they will be more willing to continue using the Apps.

Privacy Concerns have been established to be a strong variable when it comes to the adoption of mobile apps. Thus, as hypothesized that Privacy Concerns will positively influence Privacy Risk, it was revealed that indeed Privacy Concerns influence Privacy Risk in this study thus confirming the findings of (Lankton & Tripp, 2013). Also, as hypothesized that Privacy Concern will negatively influence Trust, it was found out that Privacy Concern does not influence Trust in this study. This finding is in support of (Lankton & Tripp, 2013). Similarly, we hypothesized that

Privacy Concern will positively influence Usage Continuance Intention as well as Privacy Concern negatively influencing Change Privacy Settings. The findings from the analysis revealed that both hypotheses are not supported as Privacy Concerns do not influence both Usage Continuance Intention and Change Privacy Settings. Thus, the findings are in support of (Lankton & Tripp, 2013). Given these findings, it can be submitted that organizations cannot rely on Privacy Concerns to achieve Trust, Usage Continuance Intention, and Change Privacy Setting about their mobile Apps.

It has been established that Trust "plays an important role in predicting privacy behaviors" (Dinev & Hart, 2006). Thus, we hypothesized that Trust will negatively influence Usage Continuance Intention but will positively influence Change Privacy Settings. Our findings revealed that Trust has an influence on Usage Continuance Intention but not on Change Privacy Settings. Thus, this finding is in support of (Lankton & Tripp, 2013). This implies that any organization that wants to sustain the usage of its Apps by its customers should make sure that the customers are able to develop trust in the App. Organizations can achieve this by making sure that the information of the customers is highly protected.

Privacy Risks are predicted to "increase the likelihood of engaging in privacy behaviors to protect the opportunistic use of personal information" (Wu et al., 2012). These "risks should also make one less likely to want to continue using" mobile apps. Thus, we hypothesized that Privacy Risk will both positively influence Usage Continuance Intention and Change Privacy Settings. The findings show that Privacy Risk has an influence on Usage Continuance Intention but not on Change Privacy Settings. This finding is in support of (Lankton & Tripp, 2013). Privacy risk is the "potential loss of control over personal information. it is clear from these findings that having gotten the consent of customers to use their personal information, organizations that have such information must safeguard it adequately. This is what can guarantee customers' usage continuance intention.

Based on "previous research that motivates" the mobile apps "model, benefits from using technology should decrease one's privacy behaviors and increase continued use". We believe Enjoyment as a gain of Mobile Apps use because "Enjoyment is a major reason people use social networking apps" (Xu et al., 2008). The more enjoyable using mobile apps, "the less likely one will engage in privacy behaviors because this might stifle one's ability to make use of the app". Thus, we hypothesized that Enjoyment will positively influence Usage Continuance Intention but negatively influence Change Privacy Settings. The analysis indicates that Enjoyment has an influence on Usage Continuance Intention but not on Change Privacy Setting. The findings are in support of (Lankton & Tripp, 2013; Sledgianowski & Kulviwat, 2009). Enjoyment as far as technology is concerned refers to the intrinsic reward derived through the use of the technology. Therefore, going by these findings it is suggested that mobile Apps should be designed in such a way that it contains features that will enable the users to derive enjoyment while using it. In other words, features that offer hedonic value to the customers should be embedded in the mobile Apps in order to sustain their usage continuance intention.

Prior research has established that the popularity of apps has a positive effect on the behavior of people to continue using the app (Ferdous et al., 2015a). Thus, in this study, we hypothesized that App Popularity will both positively influence Usage Continuance Intention and Change Privacy Settings. Our findings revealed that App Popularity influence Change Privacy Settings but not Usage Continuance Intention. This finding is in contrast to that of (Ferdous et al., 2015a; Shen, 2015). Given these findings, it means that App Popularity is one of the factors that can be leveraged in order to influence the Change Privacy Settings of the App users. It, therefore, implies that organizations should strive to make their App popular.

6. Conclusion and Recommendations

The primary aim of this study was to investigate why users continue to use Mobile Apps despite the privacy concerns it brings. Our findings have revealed that whilst Antecedent Variable Gender influences Privacy Concern, Experience does not. Also, Privacy Concern influences Privacy Risk but not Trust, Usage Continuance Intention, and Change Privacy Settings. Also, it was established that Enjoyment, Privacy Risk, and Trust have an influence on Usage Continuance Intention but not on Change Privacy Settings. Moreover, App Popularity has an influence on Change Privacy Settings but not on Usage Continuance Intention.

In terms of contributions to theory, this study developed a conceptual model based on the APCO model which was tested with empirical data to establish the hypothesized relationships through an SEM. Thus, this study has contributed to the body of knowledge from a developing country context where there is a dearth of literature regarding the phenomenon (Mobile Apps Privacy Concerns) being discussed.

In terms of contribution to policy and practice, our findings have established that Mobile Apps users are more concerned with the Enjoyment they derived from using the Apps, yet they are more afraid of their Privacy Risk. Therefore, their continuance usage of the Apps depends largely on the Trust of the App. So, policymakers should make legislations that will guide Apps developers to make sure that the Apps being developed are highly protected of users' privacy.

This study like any other has some limitations. First, although the sample data was enough to be generalized, yet the data collection was done from only one tertiary institution which is based in Accra. Thus, it becomes difficult to generalize the findings. Future studies can stratify and collect data from not only students but the working class, as well as rural dwellers. Also, not all the variables in the APCO model was studied. Future, studies can introduce other variables especially more demographics as antecedents' variables.

References

[1]. Abdurraham, D. T., Owusu, A., Soladoye, B. A., & Kalimuthu, K. R. (2018). Celebrity-Brand Endorsement: A Study on its Impacts on Generation Y-ers in Nigeria. *Asian Journal of Scientific Research*, *11*(3), 415–427. https://doi.org/10.3923/ajsr.2018.415.427

[2]. Abdurrahaman, D. T., Owusu, A., & Bakare, A. S. (2020). Evaluating Factors Affecting User Satisfaction in University Enterprise Content Management (ECM) Systems. *The Electronic Journal of Information Systems Evaluation*, *23*(1), 1–16. https://doi.org/10.34190/EJISE.20.23.1.001

[3]. Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with Big Data, Privacy Concerns, and Self-disclosure Accuracy in Aocial Networking Websites: An APCO Model. *Communications of the Association for Information Systems*, *41*(October 2018), 62–96. https://doi.org/10.17705/1cais.04104

[4]. Bakare, A. S., Owusu, A., & Abdurrahaman, D. T. (2017). The behavior response of the Nigerian youths toward mobile advertising: An examination of the influence of values, attitudes and culture. *Cogent Business and Management*, *4*(1), 1–18. https://doi.org/10.1080/23311975.2017.1353231

[5]. Balakrishnan, J., & Griffiths, M. D. (2018). Loyalty towards online games, gaming addiction, and purchase intention towards online mobile in-game features. *Computers in Human Behavior*, *87*(February), 238–246. https://doi.org/10.1016/j.chb.2018.06.002

[6]. Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents - Privacy Concerns - Outcomes model. *Journal of Information Science*, *43*(5), 583–600. https://doi.org/10.1177/0165551516653590

[7]. Buck, C. (2017). Stop Disclosing Personal Data about Your Future Self. In *Twenty-third Americas Conference on Information Systems* (pp. 1–10).

[8]. Byun, H., Chiu, W., & Bae, J. S. (2018). Exploring the adoption of sports brand apps: An

application of the modified technology acceptance model. *International Journal of Asian Business and Information Management*, *9*(1), 52–65. https://doi.org/10.4018/IJABIM.2018010105

[9]. Campbell, H. A., Altenhofen, B., Bellar, W., & Cho, K. J. (2014). There's a religious app for that! A framework for studying religious mobile applications. *Mobile Media and Communication*, *2*(2), 154–172. https://doi.org/10.1177/2050157914520846

[10]. Christensen, C., & Prax, P. (2012). Assemblage, adaptation and apps: Smartphones and mobile gaming. *Continuum: Journal of Media & Cultural Studies*, *26*(5), 731–739. https://doi.org/10.1080/10304312.2012.706461

[11]. Conroy, D. E., Yang, C. H., & Maher, J. P. (2014). Behavior change techniques in top-ranked mobile apps for physical activity. *American Journal of Preventive Medicine*, *46*(6), 649–652. https://doi.org/10.1016/j.amepre.2014.01.010

[12]. Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*. *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*. https://doi.org/10.1007/s13398-014-0173-7.2

[13]. Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication, 15*(1), 83-108.

[14]. Díez Bosch, M., Micó Sanz, J. L., & Sabaté Gauxachs, A. (2017). Typing my Religion. Digital use of religious webs and apps by adolescents and youth for religious and interreligious dialogue. *Church, Communication and Culture*, *2*(2), 121–143. https://doi.org/10.1080/23753234.2017.1347800

[15]. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research, 17*(1), 61-80.

[16]. Dinev, T., Mcconnell, A. R., & Smith, H. J. (2015). Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, *26*(4), 639–655.

[17]. Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59*(8), 877-886.

[18]. Ferdous, R., Osmani, V., & Mayora, O. (2015a). Smartphone app usage as a predictor of perceived stress levels at workplace. *Proceedings of the 2015 9th International Conference on Pervasive Computing Technologies for Healthcare, PervasiveHealth 2015*, 225–228. https://doi.org/10.4108/icst.pervasivehealth.2015.260192

[19]. Ferdous, R., Osmani, V., & Mayora, O. (2015b). Smartphone app usage as a predictor of perceived stress levels at workplace. *Proceedings of the 2015 9th International Conference on Pervasive Computing Technologies for Healthcare, PervasiveHealth 2015*, 225–228. https://doi.org/10.4108/icst.pervasivehealth.2015.260192

[20]. Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior, 25*(1), 153-160.

[21]. Fuller, M. A., Serva, M. A., & Benamati, J. (2007). Seeing is believing: The transitory influence of reputation information on E-Commerce trust and decision making: Research Note. *Decision Sciences*, *38*(4), 675–699. https://doi.org/10.1111/j.1540-5915.2007.00174.x

[22]. Godwin-Jones, R. (2011). Emerging Technologies: Mobile APPs for Language Learning. *Language Learning and Technology*, *15*(2), 2–11.

[23]. Guo, Y., Bian, J., Leavitt, T., Vincent, H. K., Zalm, L. Vander, Teurlings, T. L., … Modave, F. (2017). Assessing the quality of mobile exercise apps based on the American college of sports medicine guidelines: A reliable and valid scoring instrument. *Journal of Medical Internet Research*, *19*(3), 1–10. https://doi.org/10.2196/jmir.6976

[24]. Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A PRIMER ON PARTIAL LEAST SQUARES STRUCTURAL EQUATION MODELING (PLS-SEM)*. SAGE Publications Inc.

[25]. Hing, N., Russell, A. M. T., Li, E., & Vitartas, P. (2018). Does the uptake of wagering inducements predict impulse betting on sport? *Journal of Behavioral Addictions*, *7*(1), 146–157. https://doi.org/10.1556/2006.7.2018.17

[26]. Hoehle, H., & Venkatesh, V. (2015). Research article Mobile application Usability : Conceptualization. *MIS Quarterly*, *39*(2), 435–472. Retrieved from https://pdfs.semanticscholar.org/8171/405b2c1538c6b2eff0eb7fb87b7b2c68eeba.pdf

[27]. Holmes, J. G. (1991). Trust and the appraisal process in close relationships.

[28]. Lankton, N., & Tripp, J. (2013). A quantitative and qualitative study of Facebook privacy using the Antecedent-Privacy Concern-Outcome Macro Model. In *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime* (Vol. 1, pp. 180–191).

[29]. LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, *41*(1), 127–149. https://doi.org/10.1111/j.1745-6606.2006.00071.x

[30]. Li, L., Lee, K. Y., Chang, Y., & Yang, S.-B. (2020). Linking Privacy Concerns for Traceable Information and Information Privacy Protective Responses on Electric Scooter Sharing Platforms. In *Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 851–857). https://doi.org/10.24251/hicss.2020.105

[31]. Li, L., Lee, K. Y., & Yang, S.-B. (2019). Do Micro-Mobility Services Take Away Our Privacy? Focusing on the Privacy Paradox in E-Scooter Sharing Platforms Research-in-Progress. In *Twenty-Third Pacific Asia Conference on Information Systems* (pp. 1–8).

[32]. Lopez-Gonzalez, H., & Griffiths, M. D. (2018). Understanding the convergence of markets in online sports betting. *International Review for the Sociology of Sport*, *53*(7), 807–823. https://doi.org/10.1177/1012690216680602

[33]. Martínez-Pérez, B., De La Torre-Díez, I., López-Coronado, M., & Herreros-González, J. (2013). Mobile apps in cardiology: Review. *Journal of Medical Internet Research*, *15*(7), 1–15. https://doi.org/10.2196/mhealth.2737

[34]. Merikivi, J., Tuunainen, V., & Nguyen, D. (2017). What makes continued mobile gaming enjoyable? *Computers in Human Behavior*, *68*, 411–421. https://doi.org/10.1016/j.chb.2016.11.070

[35]. Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of computer-mediated communication*, *9*(4), JCMC942.

[36]. Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335–361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

[37]. Modave, F., Bian, J., Leavitt, T., Bromwell, J., Harris III, C., & Vincent, H. (2015). Low Quality of Free Coaching Apps With Respect to the American College of Sports Medicine Guidelines: A Review of Current Mobile Apps. *JMIR MHealth and UHealth*, *3*(3), 1–12. https://doi.org/10.2196/mhealth.4669

[38]. Omondi, G. (2020). The state of mobile in Ghana's tech ecosystem. The Ecosystem Accelerator programme is supported by the UK Department for International Development (DFID), the Australian Government, the GSMA and its members. Retrieved from: https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-in-ghanas-tech-ecosystem/#:~:text=Ghana%20has%20the%20highest%20mobile,is%20at%2044.8%20per%20cent.&text=There%20are%2013.1%20million%20active,million%20registered)%20mobile%20money%20accounts.

[39]. Owusu, A. (2017). Business intelligence systems and bank performance in Ghana : The

balanced scorecard approach. *Cogent Business & Management*, *4*(1364056), 1–22. https://doi.org/10.1080/23311975.2017.1364056

[40]. Owusu, A. (2019). Examining the Moderating Effects of Time-Since-Adoption on the Nexus Between Business Intelligence Systems and Organisational Performance. *International Journal of Technology Diffusion*, *10*(3), 49–68. https://doi.org/10.4018/ijtd.2019070104

[41]. Owusu, A., Agbemabiese, G. C., Abdurrahaman, D. T., & Soladoye, B. A. (2017). DETERMINANTS OF BUSINESS INTELLIGENCE SYSTEMS ADOPTION IN DEVELOPING COUNTRIES: AN EMPIRICAL ANALYSIS FROM GHANAIAN BANKS. *Journal of Internet Banking and Commerce*, *22*(S8), 1–25. Retrieved from http://www.icommercecentral.com

[42]. Owusu, A., Broni Jnr, F. E., & Akakpo, P. K. (2019). PRELIMINARY INSIGHTS INTO THE CONCERNS OF ONLINE PRIVACY AND SECURITY AMONG MILLENNIALS IN A DEVELOPING ECONOMY. *Journal of Theoretical and Applied Information Technology*, *15*(11), 3063–3076. Retrieved from www.jatit.org

[43]. Owusu, A., Ghanbari-Baghestan, A., & Kalantari, A. (2017). Investigating the Factors Affecting Business Intelligence Systems Adoption. *International Journal of Technology Diffusion*, *8*(2), 1–25. https://doi.org/10.4018/ijtd.2017040101

[44]. Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642–660. https://doi.org/10.1057/s41303-017-0056-z

[45]. Pagoto, S., Schneider, K., Jojic, M., Debiasse, M., & Mann, D. (2013). Evidence-based strategies in weight-loss mobile apps. *American Journal of Preventive Medicine*, *45*(5), 576–582. https://doi.org/10.1016/j.amepre.2013.04.025

[46]. Pindeh, N., Suki, N. M., & Suki, N. M. (2016). User Acceptance on Mobile Apps as an Effective Medium to Learn Kadazandusun Language. *Procedia Economics and Finance*, *37*(16), 372–378. https://doi.org/10.1016/s2212-5671(16)30139-3

[47]. Rezaei, S., Shahijan, M. K., Amin, M., & Ismail, W. K. W. (2016). Determinants of App Stores Continuance Behavior: A PLS Path Modelling Approach. *Journal of Internet Commerce*, *15*(4), 408–440. https://doi.org/10.1080/15332861.2016.1256749

[48]. Richardson, M., Cannon, S., Teichert, L., Vance, A., Kramer, I., Barter, M., … Callahan, C. (2020). Religion-focused dating apps: A Q methodology study on the uses of mutual. *Telematics and Informatics*, (June), 1–10. https://doi.org/10.1016/j.tele.2020.101448

[49]. Ringle, C. M., Wende, S., & Becker, J.-M. (2015). SmartPLS 3. *Boenningstedt: SmartPLS GmbH*, http://www.smartpls.com.

[50]. Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. *Pearson Education* (Fifth). Pearson Education, Prentice Hall.

[51]. Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, *13*(4), 24-38.

[52]. Shen, G. C. C. (2015). Users' adoption of mobile applications: Product type and message framing's moderating effect. *Journal of Business Research*, *68*(11), 2317–2321. https://doi.org/10.1016/j.jbusres.2015.06.018

[53]. Sledgianowski, D., & Kulviwat, S. (2009). Using social network sites: The effects of playfulness, critical mass and trust in a hedonic context. *Journal of computer information systems*, *49(*4), 74-83.

[54]. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 989-1015.

[55]. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly: Management Information Systems*, *20*(2), 167–195. https://doi.org/10.2307/249477

[56]. Statista. (2016). Mobile app usage. Retrieved from https://www.statista.com/study/11559/mobile-app-usagestatista-dossier/
[57]. Stutzman, F., & Kramer-Duffield, J. (2010, April). Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 1553-1562).
[58]. Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating Privacy and Information Disclosure Behavior in Social Electronic Commerce. *Sustainability*, *11*(12). https://doi.org/10.3390/su10023311
[59]. Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 157-178.
[60]. Vodafone Group. (2015). Unifying communication, Annual Report 2015. Retrieved from http://www.vodafone.com/content/annualreport/annualreport15/assets/pdf/full_annual_report_2015.pdf
[61]. Wong, K. K. (2013). Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS. *Marketing Bulletin*, *24*(1), 1–32. https://doi.org/10.1108/EBR-10-2013-0128
[62]. Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior*, *28*(3), 889-897.
[63]. Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.
[64]. Zhang, R., Chen, J. Q., & Lee, J. C. A. (2013). Mobile commerce and consumer privacy concerns. *Journal of Computer Information Systems*, *53*(4), 31–38. https://doi.org/10.1080/08874417.2013.11645648
[65]. Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information and Management*, *47*(2), 115–123. https://doi.org/10.1016/j.im.2009.12.003
[66]. Zydney, J. M., & Warner, Z. (2016). Mobile apps for science learning: Review of research. *Computers and Education*, *94*, 1–17. https://doi.org/10.1016/j.compedu.2015.11.001