pISSN: 1906 - 6406 The Scholar: Human Sciences
eISSN: 2586 - 9388 The Scholar: Human Sciences
http://www.assumptionjournal.au.edu/index.php/Scholar

Mobile Game Players' Behavioral Intention to Use Facial Recognition Login System in Shanghai, China

Qizhen Gu*

Received: November 28, 2022. Revised: January 28, 2023. Accepted: January 31, 2023.

Abstract

Purpose: This research was designed to study the influences of perceived effectiveness of privacy policy, perceived privacy risk, perceived privacy self-efficacy, privacy concern, perceived usefulness, perceived ease of use, and the behavioral intention of mobile game players toward facial recognition login systems. **Research design, data, and methodology:** This research has applied a quantitative method to distribute questionnaires to mobile game players (n=701) in Shanghai, China. The sample techniques involve judgmental and convenience sampling. The index of item-objective congruence (IOC) and pilot test were employed before the data collection. Confirmatory factor analysis (CFA), and structural equation model (SEM) were implemented to analyze the data and test the overall model along with the proposed research hypotheses. **Result:** The analysis showed that perceived effectiveness of privacy policy, perceived privacy risk, perceived privacy self-efficacy, privacy concern, perceived usefulness, and perceived ease of use significantly impact behavioral intention. Privacy concern has the strongest impact on behavioral intention. **Conclusion:** Mobile game services need to provide a comprehensive and reliable privacy policy statement to reduce users' privacy concerns. For the system, promoters need to emphasize how facial recognition login systems are safer and more convenient than the other sign-in system.

Keywords: Facial Recognition, Behavioral Intention, Mobile Game, The Technology Acceptance Model

JEL Classification Code: M15, M21, M31, P23

1. Introduction

Facial recognition technology is one of the biometrics among voice, fingerprint, hand geometry, iris, and signature. Except for facial and fingerprint recognition, the other biometrics have yet to be wildly used, considering their drawbacks during implementation. On the one hand, fingerprint recognition possessed a high accuracy, is one of the most advanced biometrics and was easy to use. However, this technology also has certain disadvantages, such as dryness or dirt on the finger skin, could cause dysfunction, and children's fingerprints change very quickly (Bhatia, 2013). Furthermore, facial recognition uses an algorithm to recognize a person's face through his/her facial biometric characteristics (McClellan, 2020). The system would identify these characteristics or items. They were the key to distinguishing the user's face. These items usually included

1* Qizhen Gu, Ph.D. Candidate of Innovative Technology, Management, Graduate School of Business and Advanced Technology Management, Assumption University. Email: gujaystar@gmail.com

eye distance, the distance between the users' forehead to their chin, among other characteristics called "facial landmarks" to create a "facial signature" (Symanovich, 2021). The basic facial recognition system would be accomplished in five steps: First, the facial recognition machine, which requires a camera, would do digital scanning of people or existing photographs. Second, the software would detect any faces in the image. Third, once the facial recognition system software detects and targets a face, it analyzes the characteristics or features of the face. The fourth step is comparing these features with the system database to find close matches. In the final step, the system would determine the matches in step four were close enough to declare a match (Woodward Jr et al., 2003).

Governments and private companies have widely used this technology. China's Skynet Project is a national surveillance system designed to fight crime and prevent possible disasters, which possessed over 20 million surveillance cameras in public places in 2017. Certainly, facial recognition technology was implanted into the Skynet system. It allows for capturing, comparing, identifying, and monitoring the target personnel, which has played an important role in social security management (Tao, 2021).

The most used devices with facial recognition technology are smartphones and tablets. Whether the mobile device was using Apple's IOS or Google's Android operation system, they all implemented this technology. This facial recognition technology could provide an alternative option for unlocking mobile devices with a PIN code or fingerprint. Apple implemented facial recognition technology with their Face ID in their iPhone X and later models and iPad Pro models, which used A12X Bionic chip (Apple, 2021). The TrueDepth front camera would capture the user's facial information by projecting and analyzing more than 30,000 dots to create a map of the user's face. It has been designed to protect the user from spoofing by using masks or other techniques. Most Android smartphones also achieve it by using their front camera, like Xiaomi Mi Explorer Edition, Oppo Find X. Huawei's Mate 20 Pro, which used similar technology and applies 30,000 dots, whereas Oppo applies halves which were 15,000 dots (Triggs, 2021). Most mobile devices implemented the hardware and the software to satisfy the requirement of facial recognition technology, and several commonly used mobile applications started to apply this technology to their systems to improve user security.

The mobile gaming industry has grown rapidly over the last several years, with China as the top-ranked country in both market value and number of players (Venkatesh, 2021). Certainly, mobile gaming has become a very important role for players in China in terms of both money and time spent on it (Thomala, 2021). The game account has been considered a valuable and important asset to mobile game players; the traditional way to secure this asset was by using a username and password. However, the traditional way needs more guarantees to players regarding efficiency and security. A better alternative is that facial recognition technology could provide a securer and more convenient method to protect mobile game player's accounts (Prabhakar et al., 2003).

A facial recognition login system could be a perfect solution to replace the traditional mobile game login system by using usernames and passwords. Since biometrics technology is highly involved with personal information, facial recognition technology required the users to upload their facial data to the system to form a "face ID" (McClellan, 2020). The purpose of the research is to investigate the determining factors of the mobile game facial recognition login system and mobile game players' behavioral intention toward it in Shanghai, China. Since no previous research has studied this area in this specific geographic region, this study aims to fill the gap in the mobile game login system behavioral intention by using the Chinese context as sampling.

2. Literature Review

2.1 Theories Used in the Study

In this study, the theory of communication privacy management (CPM) and the technology acceptance model (TAM) were applied to establish the framework of this research. The CPM explains whether information access is a potential risk (Petronio, 2002). The theory argues that individuals with their boundaries protect their privacy and manage their boundaries by following their own rules. Any individual or organization that tries to penetrate their boundaries might be seen as a threat, and they would raise their privacy concerns (Baruh et al., 2017; Sutanto et al., 2013). CPM theory also applies to privacy issues generated by new technology (Stanton & Stam, 2003; West et al., 2004). The TAM is about individuals' acceptance of a certain technology. Within the proposed model, perceived ease of use and usefulness were the major predictors of people's behavioral intention or acceptance of using this technology (Davis, 1989). Tan et al. (2012) extended the model and included privacy concerns as a third predictor.

2.2 Introduction of Variables

2.2.1 Perceived Effectiveness of Privacy Policy (PEPP)

The perceived effectiveness of a privacy policy could be defined as how strongly the customers believe the privacy notice posted by the firm (online service provider) could provide reliable information about how this firm practices

its customers' data (Xu et al., 2011). The privacy policy represents a long-term commitment to the customers (Anton et al., 2007); in general, this statement could fulfill the information gap between the customers and the service provider by providing a message about how the service provider would practice with the information (Zhu et al., 2020). In this study, the perceived effectiveness of privacy policy refers to how strongly the users believe the privacy notice posted by the mobile game operator could practice users' data properly.

Xu et al. (2011) determined that perceived effectiveness was negatively related to users' privacy risk perception. Wang (2019) supported this statement in the study "Effect of Brand Awareness and Social Norms on User-Perceived Cyber Privacy Risk," which mainly focused on how external factors would affect users' perceptions of online privacy risk. These external factors included the perceived effectiveness of a privacy policy and the perceived controls over the user's information disclosure. The data indicated that a negative relationship between perceived effectiveness and privacy risk was also identified.

Acquisti et al. (2015) stated in the relationship between users and online service providers (social media vendors) that the users were at the side of disadvantage, especially after when the users shared their personal information with the service provider. Wang (2019) studied the relationship between the perceived effectiveness of privacy policies and perceived privacy self-efficacy and stated that the perceived effectiveness of privacy policies significantly and positively impacted perceived privacy self-efficacy. Therefore, in this research, we hypothesize:

H1: Perceived effectiveness of privacy policy has a significant impact on perceived privacy risk.

H2: Perceived effectiveness of privacy policy has a significant impact on perceived privacy self-efficacy.

2.2.2 Perceive Privacy Risk (PPR)

Featherman and Pavlou (2003) generally conceptualized this term as a significant perceived risk factor. They defined it as a potential losing control of personal information. Malhotra et al. (2004) and Xu et al. (2011) also defined perceived privacy risk as customers' expectation of losing their released personal information to mobile applications. Since the facial recognition of mobile game applications needs to be required to access users' private data, allowing mobile applications to access users' personal information could easily compromise users' privacy (King & Jessen, 2010), and this private information could be misused; sold to the market; accessed without authorized, and information theft (Dinev & Hart, 2006). In this study, the perceived privacy risk refers to the degree of users' expectation of losing their facial information to the mobile game login system.

Zhu and Bao (2018) stated that when a user's privacy concern is deep, he/she feels less control over personal information. How the user perceives risk is also related to the platform's capability and enough righteousness to ensure user information privacy. The unawareness of how the platform practices user information was the perceived risk that might occur users' high privacy concern, and when users already had a high privacy concern, they would doubt whether the service provider (platform) collected too much personal information and practices this information without informing the user (Zhou, 2020). Wang et al. (2019) studied the linkages between CPM theory and privacy concerns moreover defined that perceived privacy risk has a positive relationship with privacy concerns. Therefore, in this research, we hypothesize:

H3: Perceived privacy risk has a significant impact on privacy concern.

2.2.3 Perceive Privacy Self-Efficacy (PPSE)

Perceived self-efficacy generally could be defined as people's beliefs about their abilities to certain events that might influence their lives. These beliefs about their self-efficacy were mainly developed from four information sources (Bandura et al., 2010). Previous research pointed out that people believe their performance could produce the expected results; otherwise, they might lack the motivation to perform or persist when facing certain difficulties (Bandura et al., 2010). Since the term "perceived privacy self-efficacy" in this study was highly related to the mobile application. Therefore, it is conceptualized as the degree of users' perception of their ability to control the privacy boundaries for protecting their personal information on their mobile devices (Lee & Hill, 2013; Youn, 2009). In this study, perceived privacy self-efficacy refers to the degree of users' knowledge and confidence in protecting the facial information they provide to the mobile game login system.

Mohamed and Ahmad (2012) defined internet self-efficacy as the degree of user's confidence or abilities in applying internet skills, furthermore, found that internet self-efficacy and privacy concerns were significantly related. Previous research showed that users with high self-efficacy were more confident about reaching certain goals, including managing their privacy. These high self-efficacy users viewed themselves as more capable of solving problems when using online services. On the other hand, those with low self-efficacy lacked the capabilities and felt less confident in managing their private information (Akhter, 2014). Wang et al. (2019) researched CPM theory and privacy concerns and stated that perceived privacy self-efficacy was negatively associated with privacy concerns regarding social media use. Therefore, in this research, we hypothesize:

H4: Perceived privacy self-efficacy has a significant impact on privacy concern.

2.2.4 Privacy Concern (PC)

In information technology use, the term privacy refers to how the users provide their personal information to the service provider and how the provider and the users keep this information confidential (Phelps et al., 2000). Since it is almost impossible to measure privacy, the studies moved to privacy concerns as a measurable term instead of privacy (Malhotra et al., 2004; Smith et al., 1996). Generally, privacy concerns could be conceptualized as the belief that a user's privacy may face risks (Culnan & Armstrong, 1999). Gu et al. (2016) define privacy concerns of mobile applications refer to the user's overall assessment of the application and perceived permission sensitivity as one of the important aspects of this assessment. In the context of this study, the privacy concern refers to before the mobile game login system has collected the facial information, how strong the users' beliefs of the potential privacy risk they were facing.

The term privacy concern was not directly included with TAM. However, privacy concerns might be another predictor of behavioral intention influencing a user's acceptance of new technology. In other words, privacy concern was just like perceived usefulness and perceived ease of use as one of the behavioral beliefs which affect user's attitudes (Tan et al., 2012). Anic et al. (2019) defined there was a negative relationship between privacy concerns and intention to use new technology, considering the new technologies were often linked with a high level of privacy threats; they also pointed out that users' privacy concerns were exerted as a predictor of general behavior toward new technologies or services or applications. Therefore, in this research, we hypothesize:

H6: Privacy concern has a significant impact on behavioral intention.

2.2.5 Perceived Usefulness (PU)

Perceived usefulness is one of the fundamental elements of the TAM (technology acceptance model), Davis (1989) defined the term as an individual who believes that using certain IT (information technology) or systems would be useful or would improve his/her performance. Later on, this definition was extended into many areas. In online shopping, this term has been defined as the degree of customers' perception of the benefits and advantages of online shopping (Moslehpour et al., 2018). In the area of mobile payment, this term has been defined as users' overall cognitive evaluation of the advantage of the mobile payment service (Wu et al., 2017). In this study, perceived usefulness refers to how strongly users believe that using mobile game facial recognition would be convenient or improve their game login process.

The linkage between perceived usefulness and perceived ease of use was defined by Davis (1989) in the Technology acceptance model (TAM) research, in which the perceived ease of use was the predictor of perceived usefulness. Abdullah et al. (2017) defined a significant relationship between perceived ease of use and perceived usefulness towards the user's intention on online hotel booking. Kim and Bernhard (2014) conducted a study to examine the customers' intention to use the fingerprint system service in a hotel. They resulted in the perceived ease of use significantly influencing the perceived usefulness.

The relationship between perceived usefulness and behavioral intention was another link stated by Davis (1989) in the model of TAM, and the model showed that perceived usefulness was the protector of the user's behavioral intention. Lai (2018) applied the extended TAM model to examine the consumers' use intention for a single platform E-payment and found that the perceived usefulness was positively associated with consumers' use intention. A similar result showed in the research on Chinese consumers' use intention for mobile commerce (Chi, 2018). Therefore, in this research, we hypothesize:

H7: Perceived usefulness has a significant impact on behavioral intention.

2.2.6 Perceived Ease of Use (PEU)

The term perceived ease of use as another fundamental element of the TAM, refers to the degree to which an individual believes that by using certain information technology or system effortlessly, "ease" has been defined as freedom from difficulty or putting great effort to study this technology or system (Davis, 1989). To test the element of perceived ease of use, investigate the necessity of this technology (Burton-Jones & Hubona, 2005). Specifically, a certain technology was easier or more advantageous than another (Moslehpour et al., 2018). Prior study shows that ease of use was directly and significantly determinant of user acceptance for Chinese people in the early phases of using certain information technology innovations (Dong, 2011). In this study, the perceived ease of use refers to the degree to which users believe using the mobile game facial recognition system would be free of effort.

The perceived ease of use and the behavioral intention was the third fundamental linkage defined by Davis (1989) in the model of TAM. Hansen et al. (2018) applied and extended the TAM model to test customers' use intention of social media for transactions and verified the significant relationship between the perceived ease of use and the behavioral intention to use. Koul and Eydgahi (2018) used the TAM model to adopt driverless car technology. The result showed that perceived ease of use positively impacted behavioral intention toward such technology. Therefore, this research hypothesizes:

H6: Perceived ease of use has a significant impact on perceived usefulness.
H8: Perceived ease of use has a significant impact on behavioral intention.

2.2.7 Behavioral Intention (BI)

In TAM, behavioral intention was the central concept of the model. Davis (1989) defined behavioral intention as the intention to perform a certain behavior. Moreover, it has been determined by an individual's attitude toward the system. In the context of mobile learning, behavioral intention refers to the degree to which an individual is willing to plan a specific future behavior which in this case was to accept and adapt to mobile learning (Chao, 2019). Tsou et al. (2019) state that behavioral intention is an individual's willingness to engage in a particular behavior. This term has been extensively used to predict a customer's future behavior or explain a customer's actual behavior. In this study, behavioral intention refers to the individual's willingness to use the mobile game facial recognition system.

3. Research Methods and Materials

3.1 Research Framework

The research framework was established according to four previous studies and their theoretical frameworks. The first theoretical framework was from Davis (1989). The study proposed perceived usefulness and perceived ease of use to predict users' intention to use and usage behavior of information technology. The second theoretical framework was from James et al. (2006). The study proposed the perceived need for security, perceived need for privacy, perceived physical invasiveness, perceived usefulness, perceived ease of use, and how the variables influenced users' intention to use biometrics devices. The third theoretical framework was from Tan et al. (2012). The study proposed that privacy concerns, perceived usefulness, and perceived ease of use could impact users' behavioral intention toward social networking websites. The fourth theoretical framework was from Wang et al. (2019). The study proposed privacy invasion experience, perceived effectiveness of privacy protection technology, perceived effectiveness of privacy policy, perceived privacy risk, and perceived self-efficacy that would influence users' privacy concerns.

This study aimed to investigate whether the variables: perceived effectiveness of privacy policy; perceived privacy risk; perceived privacy self-efficacy; privacy concern; perceived ease of use; perceived usefulness could impact mobile game players' behavioral intention toward facial recognition login system. The research framework is illustrated in Figure 1.

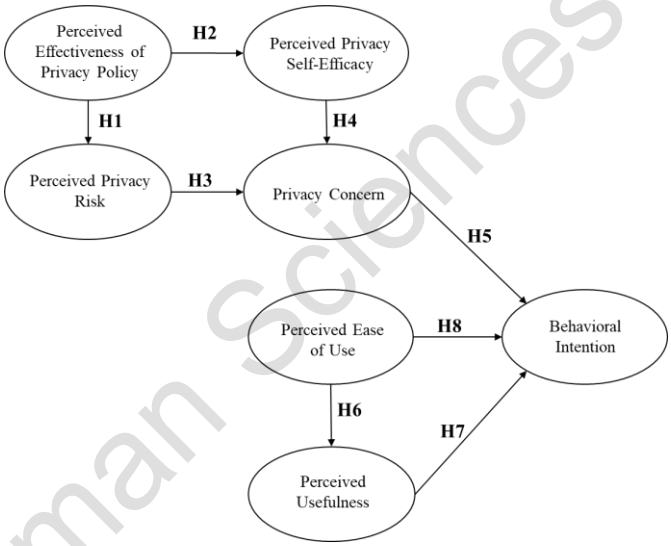

Figure 1: Conceptual Framework

H1: Perceived effectiveness of privacy policy has a significant impact on perceived privacy risk.
H2: Perceived effectiveness of privacy policy has a significant impact on perceived privacy self-efficacy.
H3: Perceived privacy risk has a significant impact on privacy concern.
H4: Perceived privacy self-efficacy has a significant impact on privacy concern.
H5: Privacy concern has a significant impact on behavioral intention.
H6: Perceived ease of use has a significant impact on perceived usefulness.
H7: Perceived usefulness has a significant impact on behavioral intention.
H8: Perceived ease of use has a significant impact on behavioral intention.

3.2 Research Methodology

In this study, the quantitative research used questionnaire distribution through online channels of the Internet platform. The data were collected from target groups and analyzed. Before data collection, to ensure reliability and validity, the Item Objective Congruence (IOC) Index is used by the rating of three experts with all scale items reserved at a score of 0.6 and over. Cronbach's alpha was used to test to ensure the validity of the content with all constructs were passed at value greater than 0.70 (Zikmund, 2008). After collecting data, confirmatory factor analysis (CFA) was conducted for validity and reliability. The baseline variables of the

structural equation model (SEM) are used to verify the structural nature of the relationship between variables.

3.3 Population and Sample Size

The target population is considered to have common characteristics (Zikmund et al., 2013). They pointed out that the target population refers to the main population of the study and is a part of the overall population (Saunders et al., 2016). They comprise a group of related elements which participated in the test and possessed the information designed and collected by researchers (Ali et al., 2016). Cooper and Schindler (2011) pointed out that the sample size for complex model should be between 200 to 500. Therefore, the sample size of this study is 800 mobile gamers who are 25 to 34 years old in Shanghai Province, China. However, the returned questionnaire after the screening was 701 respondents.

3.4 Sampling Technique

Tolmie et al. (2011) defined the sampling unit as the basic unit for modeling a sample, which can be set as a single element or a group of elements from the crowd. Zikmund et al. (2013) defined the sampling unit as a group of elements based on sample selection. In addition, besides being accurately defined, identifiable and observable, sampling units can be regarded as basic units or groups of basic units suitable for sequencing purposes (Kabir, 2016). Therefore, each unit element is independent and indivisible when selected (Sharma et al., 2005). The sample techniques involve judgmental and convenience sampling. For judgmental sampling, the sampling unit comprises mobile gamers who are 25 to 34 years old in Shanghai Province, China. The convenience sampling method was conducted using the mobile social application (Wechat, QQ, Weibo) to distribute the questionnaires.

4. Results and Discussion

4.1 Demographic Information

In Table 1, the demographic profile of 701 respondents shows that 52.6% were male, and 47.4% were female. The age range between 25 to 27 was slightly more than other age ranges. For education, 72.3% of the respondents have Bachelor's degree. Nearly 46% of the respondents would play mobile games 2 to 4 times a week. More than 90% of the respondents would not spend over 75$ each month on mobile games, and the majority group was willing to spend 15$ to 45$ per month.

Table 1: Demographic Profile

Demographic and General Data (N=701)		Frequency	Percentage
Gender	Male	369	52.6%
	Female	332	47.4%
Age	25 to 27	269	38.4%
	28 to 31	228	32.5%
	32 to 34	204	29.1%
Education	Bachelor's Degree & Below	507	72.3%
	Master's Degree	167	23.8%
	Doctorate Degree	27	3.9%
Frequency of mobile gaming (weekly)	Less than 2 times	110	16%
	2 to 4 times	324	46%
	5 to 7 times	167	24%
	More than 7 times	100	14%
Monthly Spending	Less than 15$	184	26.2%
	15$ to 45$	287	40.9%
	46$ to 74$	180	25.7%
	75$ to 149$	46	6.6%
	Higher than 150$	4	0.6%

4.2 Confirmatory Factor Analysis (CFA)

The confirmatory factor analysis (CFA) could examine whether the measurement model was acceptable by testing the relationship between the observed and latent variables (Ramlall, 2017). CFA could confirm the convergent validity (including composite reliability, factor loading, average variance extracted, and multicollinearity) and discriminant validity. According to the findings in Table 2, the constructs have exhibited the coefficient of internal consistency sufficed the requirements of Cronbach's Alpha value greater than 0.70 (Zikmund, 2008); and the value of factor loading greater than 0.5 and the composite reliability greater than 0.7 (Gravetter & Wallnau, 2000; Hair et al., 2010). In this study, each variable satisfied each of the indicators. In table 3, the square root of each AVE in the diagonal with the correlation coefficients for each construct in the relevant rows and columns was identified as having a larger value than the correlations with other constructs (Hair et al., 2016). Therefore, the discriminant validity was accepted.

Table 2: Confirmatory Factor Analysis Result, Composite Reliability (CR) and Average Variance Extracted (AVE)

Variables	Source of Questionnaire	No. of Items	Cronbach's Alpha	Factors Loading	CR	AVE
1. Perceived effectiveness of privacy policy (PEPP)	Wang et al. (2019)	3	0.896	0.750-0.763	0.947	0.856
2. Perceived privacy risk (PPR)	Wang et al. (2019)	4	0.873	0.787-0.820	0.959	0.854
3. Perceived privacy self-efficacy (PPSE)	Wang et al. (2019)	4	0.921	0.780-0.800	0.956	0.846
4. Privacy Concern (PC)	Chang et al. (2015)	4	0.833	0.810-0.833	0.960	0.858
5. Perceived ease of use (PEU)	Liebana-Cabanillas et al. (2015)	5	0.794	0.763-0.807	0.951	0.796
6. Perceived usefulness (PU)	Liebana-Cabanillas et al. (2015)	4	0.908	0.692-0.758	0.936	0.786
7. Behavioral Intention (BI)	Tan et al. (2014)	4	0.930	0.810-0.845	0.953	0.836

As seen in Table 3 below, the square root of the AVE of each variable is more prominent than its correlation coefficient with other variables, indicating that the discriminant validity of the model is perfect. In addition, CMIN/DF, GFI, AGFI, NFI, CFI, TLI, and RMSEA are used as indicators of model fitting in CFA testing.

Table 3: Goodness of Fit for Measurement Model

Index	Acceptable Values	Statistical Values
CMIN/df	≤ 2.00 (Schreiber et al., 2006)	1.833
GFI	≥ 0.90 (Bagozzi & Yi, 1988)	0.941
AGFI	≥ 0.90 (Hair et al., 1998)	0.927
TLI	≥ 0.95 (Hu & Bentler, 1999)	0.987
NFI	≥ 0.90 (Hair et al., 1998)	0.976
CFI	> 0.95 (Hu & Bentler, 1999)	0.989
RMSEA	≤ 0.05 (Hair et al., 2010)	0.034
Model Summary		**Acceptable Model Fit**

Remark: CMIN/DF = The ratio of the chi-square value to degree of freedom, GFI = Goodness-of-fit index, AGFI = Adjusted goodness-of-fit index, TLI = Tucker-Lewis index, NFI = Normed fit index, CFI = Comparative fit index, and RMSEA = Root mean square error of approximation,
Source: Created by the author.

As shown in Table 4, the value obtained in this study is greater than the acceptable value, which verifies the good fitting effect of the model. In addition, the measurement results of these models consolidate the effectiveness of discrimination and verify the effectiveness of subsequent structural model estimates.

Table 4: Discriminant Validity

	PEPP	PPR	PPSE	PC	PEU	PU	BI
PEPP	**0.925**						
PPR	-0.845	**0.924**					
PPSE	0.852	-0.861	**0.920**				
PC	-0.751	0.762	-0.817	**0.927**			
PEU	0.005	0.004	0.038	-0.144	**0.892**		
PU	0.008	-0.018	0.045	-0.172	0.854	**0.887**	
BI	0.650	-0.616	0.682	-0.863	0.331	0.354	**0.915**

Note: The diagonally listed value is the AVE square roots of the variables
Source: Created by the author.

4.3 Structural Equation Model (SEM)

Henseler (2011) stated that Structural Equation Modeling (SEM) could test the latent variables of the constructed model, correcting the error of measurements among specific errors with covariance structures and evaluating the entire theoretical structure simultaneously. Table 5 illustrates the statistical value of the model fitness and compares it with the recommended values. The original model of this study was identified as lacking fitting, therefore after the modification, the results acquired from SEM of the goodness of fit of this model were CMIN/df = 1.944, GFI = 0.936, AGFI = 0.924, TLI(NNFI) = 0.986, NFI = 0.974, CFI = 0.987, and RMSEA = 0.037. as a result, all 7 indicators reached the recommended value and showed a good fit for the structural model.

Table 5: Goodness of Fit for Structural Model

Index	Acceptable Values	Statistical Values
CMIN/df	≤ 2.00 (Schreiber et al., 2006)	1.944
GFI	≥ 0.90 (Bagozzi & Yi, 1988)	0.936
AGFI	≥ 0.90 (Hair et al., 1998)	0.924
TLI	≥ 0.95 (Hu & Bentler, 1999)	0.986
NFI	≥ 0.90 (Hair et al., 1998)	0.974
CFI	> 0.95 (Hu & Bentler, 1999)	0.987
RMSEA	≤ 0.05 (Hair et al., 2010)	0.037
Model Summary		**Acceptable Model Fit**

Remark: CMIN/DF = The ratio of the chi-square value to degree of freedom, GFI = Goodness-of-fit index, AGFI = Adjusted goodness-of-fit index, TLI = Tucker-Lewis index, NFI = Normed fit index, CFI = Comparative fit index, and RMSEA = Root mean square error of approximation,
Source: Created by the author.

4.4 Research Hypothesis Testing Result

Table 6: Hypothesis Testing Result

Hypothesis	Standardized Estimate (β)	t-Value	p-Value	Result
H1: PEPP →PPR	-0.844	-29.257	***	Supported
H2: PEPP→PPSE	0.854	29.480	***	Supported
H3: PPR→PC	0.241	4.735	***	Supported
H4: PPSE→PC	-0.609	-11.650	***	Supported

H5: PC→BI	-0.827	-30.724	***	Supported
H6: PEU→PU	0.858	28.247	***	Supported
H7: PU→BI	0.123	2.603	0.009	Supported
H8: PEU→BI	0.113	2.399	0.016	Supported

Remark: ***p<0.001

The path analysis result of the SEM also shows the result of the hypothesis testing of the proposed structural model. The results were based on the regression and standardized regression weights, and the indicators showed that all eight hypotheses were supported. Moreover, the variable privacy concern positively impacted mobile players' behavioral intention toward facial recognition login systems. The hypotheses testing results are presented in table 5, and the structural path is presented in figure 2.

H1: The standardized estimate between the perceived effectiveness of privacy policy and perceived privacy risk was equal to -0.844 (t-value = -29.257, p-value <0.001). Therefore, the perceived effectiveness of privacy policy impacts perceived privacy risk, and Ha1 was supported. It indicated that mobile game players perceived that an effective privacy policy announcement would decrease their perceived privacy risk when using the facial recognition login system. Previous studies' results were aligned with the finding (Culnan & Bies, 2003; Wang et al., 2019; Xu et al., 2011).

H2: The standardized estimate between the perceived effectiveness of privacy policy and perceived privacy self-efficacy was equal to 0.854 (t-value = 29.480, p-value <0.001). Therefore, the perceived effectiveness of privacy policy impacts perceived privacy self-efficacy, and H2 was supported. It indicated that the mobile game players perceived that an effective privacy policy announcement would help them to build their perceived privacy self-efficacy. Previous studies' results were aligned with the finding (Miller et al., 2017; Steinfeld, 2016; Wang et al., 2019).

H3: The standardized estimate between perceived privacy risk and privacy concern was equal to 0.241 (t-value = 4.735, p-value <0.001). Therefore, the perceived effectiveness of privacy policy impacts perceived privacy self-efficacy, and H3 was supported. It indicated that when the mobile game players possessed a high perceived privacy risk to the facial recognition login system, it would increase their privacy concerns. Previous studies' results were aligned with the finding (Li, 2012; Zhu et al., 2020).

H4: The standardized estimate between perceived privacy self-efficacy and privacy concern was equal to -0.609 (t-value = -11.650, p-value <0.001). Therefore, the perceived effectiveness of privacy policy impacts perceived privacy self-efficacy, and H4 was supported. It indicated that when mobile game players possessed a high level of privacy self-efficacy, it would reduce their privacy concerns towards the facial recognition login system. Previous studies' results were aligned with the finding (Akhter, 2014; Aljukhadar et al., 2010; Lee et al., 2017; Li, 2012).

H5: The standardized estimate between privacy concern and the behavioral intention was equal to -0.827 (t-value = -30.724, p-value <0.001). Therefore, the perceived effectiveness of privacy policy impacts perceived privacy self-efficacy, and H5 was supported. It indicated that when mobile game players have more privacy concerns about the facial recognition login system, it lowers their behavioral intention of using the system. Previous studies' results were aligned with the finding (Anic et al., 2019; Awad & Krishnan, 2006; Nam et al., 2006).

H6: The standardized estimate between perceived ease of use and perceived usefulness was equal to 0.858 (t-value = 28.247, p-value <0.001). Therefore, the perceived effectiveness of privacy policy impacts perceived privacy self-efficacy, and H6 was supported. It indicated that mobile game players would perceive the facial recognition login system useful when they perceived it was easy to learn and operate. Previous studies' results were aligned with the finding (Abdullah et al., 2017; Al-Sharafi et al., 2017; Kim & Bernhard, 2014).

H7: The standardized estimate between perceived usefulness and the behavioral intention was equal to 0.123 (t-value = 2.603, p-value = 0.009). Therefore, the perceived effectiveness of privacy policy impacts perceived privacy self-efficacy, and H7 was supported. It indicated that when mobile game players perceived the facial recognition login system was useful, they would have behavioral intentions of using it. Previous studies' results were aligned with the finding (Chi, 2018; Lai, 2018; Venkatesh & Davis, 2000)

H8: The standardized estimate between perceived ease of use and the behavioral intention was equal to 0.113 (t-value = 2.399, p-value = 0.016). Therefore, the perceived effectiveness of privacy policy impacts perceived privacy self-efficacy, and H8 was supported. It indicated that mobile game players would have the behavioral intention to use the facial recognition login system when they perceived it was easy to learn and operate. Previous studies' results were aligned with the finding (Aslam et al., 2017; Hansen et al., 2018; Nayanajith et al., 2019).

5. Conclusions and Recommendation

5.1 Conclusion and Discussion

This study investigated the factors that might affect mobile game players' behavioral intention to use facial recognition login systems in Shanghai, China. The target population of this study was mobile game players aged between 25 to 34 and currently living in Shanghai. The study applied the theory of CPM and TAM to facial recognition. A

total of eight hypotheses among seven variables have been studied, including the perceived effectiveness of privacy policy; perceived privacy risk; perceived self-efficacy; privacy concern; perceived ease of use; perceived usefulness, and behavioral intention. The researcher applied a quantitative method and collected 701 valid questionnaire data sets, and all data were analyzed using SEM.

The constructs were established based on the communication privacy management (CPM) theory and the technology acceptance model (TAM). In the previous studies (Anic et al., 2019; Arpaci, 2016; Awad & Krishnan, 2006; Nam et al., 2006), privacy concern was found to significant affecting behavioral intention. Therefore, this research proposed and testified a conceptual framework that combines CPM and TAM theories.

In the part of the CPM theory, privacy concern was significantly influenced by perceived privacy risk and perceived privacy self-efficacy. Perceived privacy self-efficacy possessed a relatively stronger negative impact on privacy concerns, and perceived privacy risk possessed a weak positive impact on privacy concerns. Perceived privacy risk and perceived effectiveness of the privacy policy strongly influenced privacy self-efficacy. The difference was that the perceived effectiveness of the privacy policy was negatively associated with perceived privacy risk, and the perceived effectiveness was positively associated with perceived privacy self-efficacy.

In the part of the TAM theory, privacy concern was found to possess the strongest negative influence on behavioral intention, with perceived usefulness as the second-ranked positive influence, with perceived ease of use providing the least positive influence. Additionally, perceived ease of use also possessed a strong positive influence on perceived usefulness. In conclusion, the study gives academics and professionals a better understanding of which aspects are important and to what degree of priority.

5.2 Recommendation

The overall result showed that all eight hypotheses were supported. The privacy concern had been identified as the strongest impact on mobile game players' behavioral intention of using facial recognition login systems. Perceived privacy risk and perceived privacy self-efficacy impacted mobile game players' privacy concerns. Both perceived privacy risk and perceived effectiveness of the privacy policy impacted privacy self-efficacy. Perceived usefulness possessed the second strongest impact on mobile game players' behavioral intention and was also impacted by perceived ease of use. Perceived ease of use possessed the least strong impact on mobile game players' behavioral intention. In general, for promoting or encouraging mobile game players to use facial recognition login systems, privacy concern was the primary factor that should be focused on, followed by their perceived usefulness, and perceived ease of use of the systems.

Based on the result of this research, practically, to improve mobile game players' behavioral intention toward facial recognition systems was to dispel their privacy concerns. By following the degree of priority, the first practical way should be: the system needs to provide a relatively comprehensive and trustworthy privacy policy statement that the users could depend on. Subsequently, making the user believe that the service provider was honest with them and that they have control of the data they provided, by doing it would enhance their perceived privacy of self-efficacy. In the meantime, a good privacy policy could reduce users' perceived privacy risk of the data they provide to the system. Based on the founding and the privacy paradox theory (Awad & Krishnan, 2006), the more privacy self-efficacy they possessed, the lower the privacy concerns they perceived. In other words, they would worry less and perceive fewer risks about the information they provided to the system. As a result, they achieved the purpose of dispelling their privacy concern and improving behavioral intention. The second practical way was to optimize the process of the facial recognition login systems and make them easier to learn for the users, which could improve their perception of the system's usefulness and increase their behavioral intention to use it in the future. The third practical way to increase behavioral intention was to emphasize that using a facial recognition login system was a better approach than using a username and password.

5.3 Limitations for Future Study

First, this paper studies mobile game players' behavioral intention toward using facial recognition login systems; it might not be suitable for other areas, such as facial recognition payment systems or biometric recognition systems. Furthermore, this study only focused on game players' behavioral intentions on mobile devices and other devices like PC or console game machines. The result might be different. Second, behavioral intentions in different nations might be perceived differently. Since this study was conducted in Shanghai, China, the result could be from a different nation, even a different province, and this study did not consider the respondents' nationality could cause the result to be different.

References

Abdullah, D., Jayaraman, K., Shariff, D. N., Bahari, K. A., & Nor, N. M. (2017). The Effects of Perceived Interactivity, Perceived Ease of Use and Perceived Usefulness on Online Hotel Booking Intention: A Conceptual Framework. *International Academic Research Journal of Social Science, 3*(1), 16-23.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Akhter, S. H. (2014). Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing, 31*(2), 118-125.

Ali, F., Zhou, Y., Hussain, K., Nair, P. K., & Ragavan, N. A. (2016). Does Higher Education Service Quality Effect Student Satisfaction, Image and Loyalty? A Study of International Students in Malaysian Public Universities. *Quality Assurance in Education, 24,* 70-94. https://doi.org/10.1108/QAE-02-2014-0008

Aljukhadar, M., Senecal, S., & Ouellette, H. (2010). Can the media richness of a privacy disclosure enhance outcome? A multifaceted view of trust in rich media environments. *International Journal of Electronic Commerce, 14*(4), 103-126.

Al-Sharafi, M. A., Arshah, R. A., Herzallah, F. A., & Alajmi, Q. (2017). The effect of perceived ease of use and usefulness on customers intention to use online banking services: the mediating role of perceived trust. *International Journal of Innovative Computing, 7*(1), 9-14.

Anic, I.-D., Budak, J., Rajh, E., Recher, V., Skare, V., & Skrinjaric, B. (2019). Extended model of online privacy concern: what drives consumers' decisions?. *Online Information Review, 43*(5), 799-817. https://doi.org/10.1108/oir-10-2017-0281

Anton, A. I., Bertino, E., Li, N., & Yu, T. (2007). A roadmap for comprehensive online privacy policy management. *Communications of the ACM, 50*(7), 109-116.

Apple. (2021, April 26). Retrieved from About Face ID advanced technology: https://support.apple.com/en-us/HT208108

Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior, 58*, 150-157.

Aslam, W., Ham, M., & Arif, I. (2017). Consumer behavioral intentions towards mobile payment services: An empirical analysis in Pakistan. *Trziste Market, 29*(2), 161-176.

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly, 30*(1), 13-28.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the academy of marketing science, 16*(1), 74-94.

Bandura, A., Weiner, I. B., & Craighead, W. E. (2010). Self-Efficacy. In I. B. Weiner & W. E. Craighead (Eds.), *The Corsini Encyclopedia of Psychology. Published Online* (pp. 1-3). John Wiley. https://doi.org/10.1002/9780470479216.corpsy0836

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53.

Bhatia, R. (2013). Biometrics and Face Recognition Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 93-99.

Burton-Jones, A., & Hubona, G. S. (2005). Individual differences and usage behavior: Revisiting a technology acceptance model assumption. *ACM SIGMIS Database, 36*(2), 58-77.

Chang, Y., Wong, S. F., & Lee, H. (2015). *Understanding perceived privacy: A privacy boundary management model* [Paper presentation]. The 19th Pacific Asia Conference on Information Systems (PACIS 2015), Singapore.

Chao, C.-M. (2019). Factors determining the behavioral intention to use mobile learning: An application and extension of the UTAUT model. *Frontiers in psychology, 10*, 1652.

Chi, T. (2018). Understanding Chinese consumer adoption of apparel mobile commerce: An extended TAM approach. *Journal of Retailing and Consumer Services, 44,* 274-284.

Cooper, D., & Schindler, P. (2011). *Business Research Methods.* (11th ed.). McGraw Hill.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323-342.

Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science, 10*(1), 104-115.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

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

Dong, J. Q. (2011). User acceptance of information technology innovations in the remote areas of China. *Journal of Knowledge-based Innovation in China, 3*(1), 44-53.

Featherman, M., & Pavlou, P. (2003). Predicting E-Services Adoption: A Perceived Risk Facets Perspective. International *Journal of Human-Computer Studies, 59*(4), 451-474.

Gravetter, F., & Wallnau, L. (2000). *Statistics for the behavioral sciences.* Wadsworth /Thomson Learning.

Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2016). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94,* 19-28. https://doi.org/10.1016/j.dss.2016.10.00

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th ed.). Pearson Prentice Hall.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2016). Advanced Issues in Partial Least Squares Structural Equation Modeling. *London: SAGE Publication, 8*(6), 1-10.

Hair, J. J., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate data analysis* (1st ed.). Prentice Hall.

Hansen, J. M., Saridakis, G., & Benson, V. (2018). Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions. *Computers in Human Behavior, 80,* 197-206.

Henseler, J. (2011). Why generalized structured component analysis is not universally preferable to structural equation modeling. *Journal of the Academy of Marketing Science, 40*(3), 402-413.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. *Journal of Organizational and End User Computing, 18*(3), 1-24.

Kabir, S. M. (2016). Measurement Concepts: Variable, Reliability, Validity, and Norm. *Basic Guidelines for Research: An Introductory Approach for All Disciplines, 10*(1), 72-110.

Kim, J., & Bernhard, B. (2014). Factors influencing hotel customers' intention to use a fingerprint system. *Journal of Hospitality and Tourism Technology, 5*(2), 98-125.

King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer-Privacy concerns when behavioural advertisers target mobile phones-Part I. *Computer Law & Security, 26*(5), 455-478.

Koul, S., & Eydgahi, A. (2018). Utilizing technology acceptance model (TAM) for driverless car technology adoption. *Journal of Technology Management & Innovation, 13*(4), 37-46.

Lai, P. C. (2018). Security as an Extension to TAM Model: Consumers' Intention to Use a Single Platform E-Payment. *Asia-Pacific Journal of Management, 13*(3-4), 110-119.

Lee, H. H., & Hill, J. T. (2013). Moderating effect of privacy self-efficacy on location-based mobile marketing. International. *Journal of Mobile Communications, 11*(4), 330-350.

Lee, W. Y., Tan, C.-S., & Siah, P. C. (2017). The Role of Online Privacy Concern as a Mediator between Internet Self-Efficacy and Online Technical Protection Privacy Behavior. *Sains Humanika, 3*(2), 37-43.

Li, Y. (2012). Theories in online information privacy research: a critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.

Liebana-Cabanillas, F., Ramos de Luna, I., & Monroto-Rios, J. F. (2015). User behavior in QR mobile payment system: the QR Payment Acceptance Model. *Technology Analysis & Strategic Management, 27*(9), 1031-1049.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems, 15*(4), 336-355.

McClellan, E. (2020). Facial Recognition Technology: Balancing the Benefits and Concerns. *Journal of Business & Technology Law, 15*(2), 363-380.

Miller, V. A., Feudtner, C., & Jawad, A. F. (2017). Children's decision-making involvement about research participation: associations with perceived fairness and self-efficacy. *Journal of Empirical Research on Human Research Ethics, 12*(2), 87-96.

Mohamed, N., & Ahmad, I. H. (2012). Information Privacy Concerns, Antecedents, And Privacy Measure Use in Social Networking Sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366-2375.

Moslehpour, M., Pham, V., Wong, W. K., & Bilgiçli, I. (2018). E-purchase intention of Taiwanese consumers: Sustainable mediation of perceived usefulness and perceived ease of use. *Sustainability, 10*(1), 234.

Nam, C., Song, C., Lee, E., & Park, C. I. (2006). Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online. *Advances in Consumer Research, 33,* 212-217.

Nayanajith, G., Damunupola, K. A., & Ventayen, R. J. (2019). Impact of Innovation and Perceived Ease of Use on E-Learning Adoption. *Asian Journal of Business and Technology, 2*(1), 19-27.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure* (1st ed.). Suny Press.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric Recognition: Security and Privacy Concerns. *IEEE Security & Privacy Magazine, 1*(2), 33-42.

Ramlall, I. (2017). *Applied Structural Equation Modelling for Researchers and Practitioners, Using R and Stata for Behavioral Research* (1st ed.). Emerald Group Publishing Limited.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (7th ed.). Pearson.

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting structural equation modeling and confirmatory factor analysis results: A review. *The Journal of educational research, 99*(6), 323-338.

Sharma, S., Pradhan, K., Satya, S., & Vasudevan, P. (2005). Potentiality of earthworms for waste management and in other uses - a review. *Journal of American Science, 1*(1), 4-16.

Smith, H. J., Milburg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Stanton, J. M., & Stam, K. R. (2003). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance & Society, 1*(2), 152-190.

Steinfeld, N. (2016). I agree to the terms and conditions:(How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior, 55*, 992-1000.

Sutanto, J., Palme, E., Tan, C., & Phang, C. W. (2013). Addressing the personalization privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37*(4), 1141-1164.

Symanovich, S. (2021, April 25). *How does facial recognition work?*. Norton Life Lock Inc. https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

Tan, G. W.-H., Ooi, K.-B., Leong, L.-Y., & Lin, B. (2014). Predicting the drivers of behavioral intention to use mobile learning: A hybrid SEM-Neural Networks approach. *Computers in Human Behavior, 36,* 198-213.

Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking website. *Internet Research, 22*(2), 211-233.

Tao, L. (2021, April 25). *The facial recognition company that supplies China's Skynet surveillance system.* https://www.scmp.com/tech/science-research/article/3005733/what-you-need-know-about-sensenets-facial-recognition-firm

Thomala, L. L. (2021, March 20). *Average monthly mobile game playing frequency in China from April 2018 to June 2020.* Statista. https://www.statista.com/statistics/1036019/china-monthly-mobile-gaming-frequency/

Tolmie, A., Muijs, D., & Mcateer, E. (2011). *Quantitative methods in educational and social research using SPSS.* (1st ed.). Open University Press.

Triggs, R. (2021, April 26). *Facial recognition technology explained.* Android Authority. https://www.androidauthority.com/facial-recognition-technology-explained-800421/

Tsou, H. T., Chen, J. S., Chou, Y., & Chen, T. W. (2019). Sharing Economy Service Experience and Its Effects on Behavioral Intention. *Sustainability, 11*(18), 5-15.

Venkatesh, C. R. (2021, July 16). *Recent Mobile Game Market Trends.* https://www.dotcominfoway.com/blog/infographic-mobile-game-market-trends-2020/

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science, 46*(2), 186-204.

Wang, E. S. (2019). Effects of Brand Awareness and Social Norms on User-Perceived Cyber Privacy Risk. *International Journal of Electronic Commerce, 23*(2), 272-293.

Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H.-H. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology & People, 32*(6), 1679-1703.

West, R. L., Turner, L. H., & Zhao, G. (2004). *Introducing Communication Theory: Analysis and Application.* McGraw-Hill.

Woodward, J. D., Horn, C., Gatune, J., & Thomas, A. (2003). *Biometrics: A look at facial recognition* (1st ed.). Rand Corp.

Wu, J., Liu, L., & Huang, L. (2017). Consumer acceptance of mobile payment across time: Antecedents and moderating role of diffusion stages. *Industrial Management & Data Systems, 117*(8), 1761-1776.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information System, 12*(12), 798-824.

Youn, S. (2009). Determinants of online privacy concerns and Its Influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389-418.

Zhou, T. (2020). The effect of information privacy concern on users' social shopping intention. *Online Information Review, 44*(5), 1119-1133. https://doi.org/10.1108/OIR-09-2019-0298

Zhu, R., Srivastava, A., & Sutanto, J. (2020). Privacy-deprived e-commerce: the efficacy of consumer privacy policies on China's e-commerce websites from a legal perspective. *Information Technology & People, 4*(5), 1119-1133. https://doi.org/10.1108/ITP-03-2019-0117

Zhu, Y., & Bao, Z. S. (2018). The role of negative network externalities in SNS fatigue: an empirical study based on impression management concern, privacy concern, and social overload. *DataTechnologies and Applications, 52*(3), 313-328.

Zikmund, W. G. (2008). *Business research methods* (8th ed.). South-Western Cengage Learning.

Zikmund, W. G., Carr, B. J. C., Griffin, M., & Babin, B. J. (2013). *Business Research Method* (8th ed.). Dryden Press.