ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 2, 469-475 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Comparison Analysis Between Mobile Banking and Mobile Payment as Determinant Factors of Customer Privacy

Yakob Utama Chandra[*,1], Bahtiar Saleh Abbas[2], Agung Trisetyarso[2], Wayan Suparta[3], Chul-Ho Kang[4]

[1]*Information Systems Department, School of Information Systems, Bina Nusantara University, Jakarta 11480, Indonesia*

[3]*Computer Science Department, Bina Nusantara University, Jakarta, 11480, Indonesia*

[3]*Department of Informatics, Faculty of Design and Technology Pembangunan Jaya University, South Tangerang, Indonesia*

[4]*Department of Electronics and Communication Engineering, Kwangwoon University, Seoul, South Korea*

ARTICLE INFO

Article history:
Received: 15 December, 2019
Accepted: 25 February, 2020
Online: 04 April, 2020

Keywords:
Perceived Privacy
Privacy Concern
Trust
Mobile Banking
Mobile Payment

ABSTRACT

Mobile banking and mobile payment are currently always used by customers for financial payments. With customer payments, it is usually easier to make payments with mobile payment, because it is more practical and direct than mobile banking. However, is the privacy of both platforms understood by the customer? Research questions to be answered: 1) What are the factors that influence privacy issues in mobile banking? 2) What are the factors that influence privacy issues with mobile payments? 3) What are the factors that influence confidence in mobile banking? 4) What are the factors that influence confidence in mobile payments? 5) Does the privacy factor influence the perceived privacy? 6) Does the confidence factor influence the perceived privacy? There are two research models and 12 (twelve) hypotheses for each model. Privacy risk, subjective norm, information management factors positive influence on privacy interest, and trust. Care about privacy and trust have a positive influence on mobile payment.

1. Introduction

Smartphones can now have a variety of applications, ranging from standard applications on a smartphone itself, such as telephone, message, internet browser, to applications that customers download to meet customer needs. Most customers currently use mobile payment and mobile banking applications as applications that must be on smartphones in addition to social media applications [1][2].

Customer privacy is an essential factor in an application on a smartphone that aims to give customers confidence in the application company by maintaining privacy on every element of the customer. The customer feels safe about using the application if the application company on the smartphone can give customer privacy rights. The most important in terms of privacy in a smartphone application is the flow of information to the customer. The customer's concern about the ownership of data, and the customer does not want data on smartphones to be in circulation without the customer's knowledge [3].

The privacy of customers can depend on the factors of institutions and the environment in the application itself. The more closely related to customer personal information, the higher the privacy issue for the safety and comfort of customer information. Underlying the existence of customer privacy is anticipating the prevention of problems that are more related to management practices. When customers want to care more about privacy, customer information can be better monitored. Therefore, the role of maintaining privacy is not only the regulation of the application but also the awareness of the privacy of the customer. In the privacy of customers themselves, there are two (two) concerns that affect the privacy of customers, namely internal drivers and external drivers. Internal drivers are something that influences customers because of privacy considerations from within the customer, and external drivers are something that

* Yakob Utama Chandra, Email : yakob@binus.ac.id

influences customers because of privacy considerations from outside the customer and usually looks at the environment that exists in the customer [3], [4].

Applications that are of concern in this study are mobile banking and mobile payment applications from financial institutions. Mobile banking is a bank product that gives customers easy access to customers 'savings at the bank so that mobile banking customers can easily do non-financial and financial transactions because they have access to customers' savings. While mobile payments, customers do not have savings at the financial institution, but the customer deposits money at the financial institution to facilitate transactions. Mobile payments are generally used to make payments for convenience in non-bank transactions [5]–[7].

With both platforms, namely mobile banking and mobile payment, the research questions in this study are 1) What are the factors that influence the privacy issues in mobile banking? 2) What are the factors that influence privacy issues with mobile payments? 3) What are the factors that influence confidence in mobile banking? 4) What are the factors that influence confidence in mobile payments? 5) Does the privacy factor influence the perceived privacy? 6) Does the confidence factor influence the perceived privacy?

To answer the research question above, this study will use a model, and there are two models, one for the mobile banking and mobile payment, with 12 (twelve) hypotheses for this research for each model:

- H1: Privacy Risk (PR) positive influence on the Privacy Concern (PC)
- H2: Propensity to Value Privacy (PVP) positive influence on the Privacy Concern (PC)
- H3: Subjective Norm (SN) positive influence on the Privacy Concern (PC)
- H4: Privacy Awareness (PA) positive influence on the Privacy Concern (PC)
- H5: Information Quality (IQ) positive influence on the Privacy Concern (PC)
- H6: Privacy Risk (PR) positive influence on the Trust (TR)
- H7: Propensity to Value Privacy (PVP) positive influence on the Trust (TR)
- H8: Subjective Norm (SN) positive influence on the Trust (TR)
- H9: Privacy Awareness (PA) positive influence on the Trust (TR)
- H10: Information Quality (IQ) positive influence on the Trust (TR)
- H11: Privacy Concern (PC) positive influence on the Perceived Privacy (PP)
- H12: Trust (TR) positive influence on the Perceived Privacy (PP)

This research used a quantitative approach by distributing questionnaires to 210 respondents.

2. Literature Review

2.1. Mobile Banking

Mobile banking or sometimes referred to as online banking is an application built by banks aimed at offering alternative channels to customers so that customers have access rights to use savings that are owned by customers. Customers can, therefore, be more satisfied with the use of the existing service facilities at the bank. For banks, operating costs will also be reduced by the existence of a mobile banking application, as banks do not have to provide the people needed to provide services to customers, but are represented by a mobile banking application [8][9].

2.2. Mobile Payment

Mobile payment, or better known as e-wallet or e-payment, is a breakthrough in non-bank financial institutions that strive to offer facilities or services to the public to make payments quickly. Customers only have to enter the balance of this mobile payment and then make a payment using a smartphone via QR Code or EDC available at the payment service, and the customer can quickly enter the customer pin to complete the payment. Mobile payment is generally more practical compared to mobile banking because, with mobile payments, it is not necessary to open a savings account, only by registering on the application and filling in money balances, it can be used directly for the execution of payments [9][10][11].

2.3. Perceived Privacy

Perceived privacy is something that the customer can accept for the privacy of current personal information when the customer registers with mobile banking and mobile payment. Perceived privacy means accepting all kinds of negative possibilities that result from the use of the application [12][13]. This perceived privacy is the goal to be pursued in this study, whereby privacy considerations and trust influence perceived privacy. Because the customer can accept any existing privacy, this influences the way the customer receives a real privacy issue and along with the trust that the customer understands. The customer can then prepare if there is a risk that arises because of the information collected about the application used by the customer [14].

2.4. Privacy Concern

Customers must understand that every application has a privacy setting, especially in applications that request data or smartphone settings from the customer. With the client's privacy issue, the client can feel comfortable and safe when using the application because the application has settings that can be made by the client and the client can adapt to the needs of the client in terms of different types of privacy that exist in the customer's smartphone application. Moreover, in highly sensitive applications such as mobile banking and mobile payment, it contains sensitive data that relates explicitly to customer money. The privacy problem is, therefore, something that the customer must take into account [15][16].

2.5. Trust

An essential factor in this research is trust, where trust is a condition that the customer believes that the application on the

smartphone can function correctly according to what the application developer has promised and ensures that all transactions can go smoothly. Besides, trust also in the sense that the client understands the business well how the business processes in the business can be carried out and by the promises made when the client reads or sees before the client installs the application on the client's smartphone and ensuring registration by providing data about the application is installed by the customer and is a sign that the customer uses the application well from start to finish [17][10].

2.6. Privacy Risk

Customers must be able to understand that every application installed on a smartphone sometimes requires customer information data to be entered into the application, and the customer must realize that the customer may lose information input or the data may be used by people who are not interested in the use of the application. Customers should realize that the risk to privacy can arise at any time because the data in each application can be taken by someone else or unknown to someone who has taken over the data [18][19].

2.7. The propensity to Value Privacy

Customers must respect the privacy created by the application developer to understand how privacy settings are made in the application. Customers are more likely to use the application without looking at the privacy settings in the application so that the customer cannot complain if something happens to the customer. Therefore, customers must understand and respect how privacy is created in applications by application developers [20].

2.8. Subjective Norm

Currently, more customers to see the terms of other customers and the behavior of other customers when using the same application for a specific purpose. In this way, the subjective norm can see how customers want to adapt to others who use the same application in psychological terms. It can be seen that customer factors follow what other people do and then psychologically apply to themselves [21].

2.9. Privacy Awareness

Customer awareness of privacy is certainly a concern and need when using applications, especially in applications where there are financial transactions. This is because privacy awareness forms the basis for the safety and ease of transactions such as mobile banking or mobile payment. Because customers with privacy awareness can make the necessary privacy settings when they start transactions in the previous phase to ensure that application developers always maintain privacy. The customer experience at the time of the transaction thus becomes positive and the absence of a negative thing that will happen to the customer, especially on the customer's psychological factors [22].

2.10. Information Control

Every customer has the right to control the information submitted in the online application. With the Information Control factor, the customer can easily set what is a priority for sharing or not. Because the client does not know that the entered data is being taken somewhere by the application developer so that the client can use the information check to adapt to the privacy policy that is available from a government or country in the client's area and also find out how the information is useful for the customer himself. Openness to information is very vulnerable to the privacy of customers. Therefore, the information check of the application can be beneficial when you perform specific online transactions [21][22].

3. Research Methodology

In this study, researchers wanted to discover which factors influence privacy interests and trust in perceived privacy. The privacy interest and trust factors in this study are five factors, namely privacy risk (PR), the propensity to value privacy (PVP), subjective norm (SN), privacy awareness (PA), and information control (IC). With figure 2 above, this model is tested simultaneously on respondents who both use mobile banking and mobile payment. Researchers conducted the same respondents to find out how privacy is felt when using mobile banking and mobile payment in terms of privacy when using the application. With this model, the aim of this study can be achieved by looking at how consumers feel about the perceived privacy of mobile banking and mobile payment.

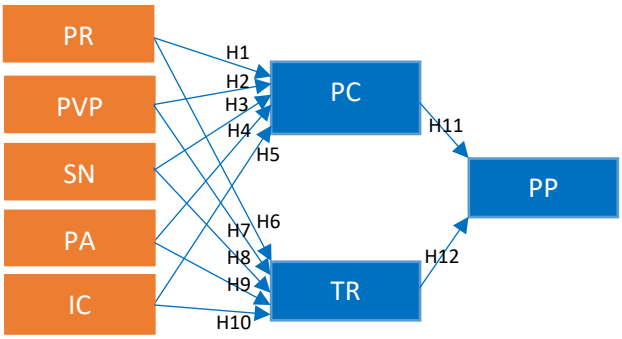

Figure 1. Research Model

3.1. Research Instrument

In this research in quantitative research, 31 statements are the same for mobile banking and mobile payment. So there are 62 statements in total. Respondents must complete all these statements in order to be able to measure the perceived privacy of respondents with a Likert scale. On this comparable scale, there are six choices of feelings felt by consumers, starting with number 1 the feeling of disagreeing with the statement until number 6 is a feeling that they strongly agree with the statement. Thirty-one statements to know perceived privacy, there are eight factors with details as follows: privacy risk (4 statements), propensity to value privacy (3 statements), subjective norm (3 statements), privacy awareness (3 statements), information control (4 statements), privacy concern (5 statements), trust (6 statements), and perceived privacy (3 statements). In addition to 31 statements for mobile banking and 31 statements for mobile payments, the questionnaire also asked about the identity of the respondents, namely the age of the respondents and the occupation of the respondents.

3.2. Data Collection Procedure

By using the sampling of the snowball technique, the data collection procedure is distributed online with Google Forms. The researcher used snowball sampling because the researcher did not know the exact population when questionnaires were distributed that started in September 2019 for 1 (one) a full month. With the use of Google Forms, the researcher has set the form if the

respondent who opens the online questionnaire is not a user of both applications on mobile banking and mobile payment, then the respondent is not counted as a respondent or invalid so that 31 answer statements in mobile banking and mobile payment. This is because there is a choice on Google Forms whether respondents use mobile banking and mobile payment? If both are not used, the respondent answers "no" and is then asked to end the form. So, it is beneficial for researchers to find out which are valid in this study. From the results obtained in this study, 210 respondents actively used mobile banking and mobile payment. Respondents' ages and occupations are shown in Table I.

Table 1. Number of Respondents

Description	Total Answer	%
N Total	210	100%
Ages of Respondent		
17 – 23 years old	167	80%
24 – 30 years old	8	4%
31 – 37 years old	11	5%
38 – 44 years old	13	6%
45 – 51 years old	9	4%
More than 51 years old	2	1%
Occupation of the Respondent		
Entrepreneur	2	1%
Employee	23	11%
Professional	16	8%
Higher Education Students	163	78%
High School Students	1	1%
Housewife	4	1%

4. Result and Discussion

Correct respondent data are respondents who use mobile banking and mobile payment, a total of 210 respondents. Of the 210 respondents, 80% (167 respondents were 17-30 years old. The remaining 20% were older than 30 years and older. Because the respondents in this study were 17-30 years old, the profession of respondents was at most students in higher education as much as 78% (163 respondents) With the identity of these respondents it can be concluded that the observed privacy will be assessed earlier in this study, especially more at the age of 17-30 and older professions as students in higher education, the results of this research are more focused on identity.

After knowing the identity of the respondent, we will look at how the test model designed in Chapter 3 is used to calculate the results of the questionnaire in this study, a statistical calculation tool to make the calculation more accurate. Researchers using the partial least squares of Smart Equations (PLS-SEM) [23]. This application is used to find the outer load for each indicator, the composite reliability for each indicator, and the extracted average variance (AVE) for each indicator. The results of the calculation of each indicator are shown in Table II for the use of mobile banking and Table III for the use of mobile payment.

Table 2: Outer Loading, Validity, and Reliability of Mobile Banking Privacy

Latent Variables	Indicators	Loading	CA	CR	AVE
Privacy Risk (PR)	PR1	0.805	0.874	0.914	0.727
	PR2	0.883			
	PR3	0.860			
	PR4	0.860			
The propensity to Value Privacy (PVP)	PVP1	0.783	0.716	0.831	0.622
	PVP2	0.786			
	PVP3	0.796			
Subjective Norm (SN)	SN1	0.842	0.790	0.878	0.705
	SN2	0.878			
	SN3	0.798			
Privacy Awareness (PA)	PA1	0.880	0.737	0.852	0.658
	PA2	0.783			
	PA3	0.765			
Information Control (IC)	IC1	0.825	0.797	0.867	0.623
	IC2	0.846			
	IC3	0.845			
	IC4	0.716			
Privacy Concern (PC)	PC1	0.777	0.919	0.940	0.758
	PC2	0.866			
	PC3	0.916			
	PC4	0.883			
	PC5	0.904			
Trust (TR)	TR1	0.836	0.925	0.941	0.728
	TR2	0.874			
	TR3	0.760			
	TR4	0.892			
	TR5	0.890			
	TR6	0.860			
Perceived Privacy (PP)	PP1	0.913	0.900	0.938	0.834
	PP2	0.904			
	PP3	0.922			

In Table 2 above, based on 210 respondents who use mobile banking about outer loading is valid because it is more than 0.7.

Also, with the composite reliability valid because the composite reliability value is higher than 0.6. Furthermore, the AVE (Average Variance Extracted) also valid because the value is higher than 0.5, so it can be concluded that all statements from using mobile banking are all valid.

Table 3: Outer Loading, Validity, and Reliability of Mobile payment Privacy

Latent Variables	Indicators	Loading	CA	CR	AVE
Privacy Risk (PR)	PR1	0.773	0.871	0.912	0.722
	PR2	0.875			
	PR3	0.854			
	PR4	0.891			
The propensity to Value Privacy (PVP)	PVP1	0.751	0.721	0.829	0.618
	PVP2	0.768			
	PVP3	0.836			
Subjective Norm (SN)	SN1	0.806	0.779	0.872	0.694
	SN2	0.879			
	SN3	0.812			
Privacy Awareness (PA)	PA1	0.882	0.728	0.847	0.650
	PA2	0.790			
	PA3	0.742			
Information Control (IC)	IC1	0.761	0.795	0.868	0.624
	IC2	0.869			
	IC3	0.852			
	IC4	0.762			
Privacy Concern (PC)	PC1	0.826	0.925	0.944	0.770
	PC2	0.867			
	PC3	0.893			
	PC4	0.924			
	PC5	0.876			
Trust (TR)	TR1	0.830	0.927	0.943	0.733
	TR2	0.879			
	TR3	0.804			
	TR4	0.873			
	TR5	0.898			
	TR6	0.848			
Perceived Privacy (PP)	PP1	0.933	0.914	0.946	0.854
	PP2	0.896			
	PP3	0.943			

After calculating statistics on mobile banking users, on Table III above shows the result of 210 respondents of mobile payment on the same respondents. In Table III in the outer loading, all statements are valid because the outer loading is more than 0.7. The composite reliability is also valid because the composite reliability value is higher than 0.6. And in the AVE (Average Variance Extracted), are all higher than 0.5, so it can be concluded that all statements about respondents who use mobile payment is all valid.

The SmartPLS application, there is a process called bootstrapping to test internal and external models. This application increases the total number of 210 respondents to 1000 samples for this research, and the alpha error is 5%. The level of proximity for general information can be achieved with the use of bootstrapping.

The bootstrapping for testing the values for hypothesis or path correlation with values of original samples, T statistics, and P values. According to the T-Table, the valid or acceptable T-Statistics is above 1.96. While P Values should below 0.05. The results of the hypothesis for mobile banking can be seen in Table IV and Figure 3. Then, the result of the hypothesis for mobile payment can be seen in Table V and Figure 4.

Table 4: Result of Mobile Banking Hypothesis

Hypothesis	Paths	Original Sample	T-Statistic	P Values	Result
H1	PR→ PC	0.424	5.386	0.000	Significant
H2	PVP → PC	0.193	1.912	0.056	Not Significant
H3	SN → PC	0.150	2.015	0.044	Significant
H4	PA → PC	-0.015	0.166	0.868	Not Significant
H5	IC → PC	0.048	0.575	0.565	Not Significant
H6	PR → TR	-0.011	0.187	0.852	Not Significant
H7	PVP → TR	-0.043	0.494	0.621	Not Significant
H8	SN → TR	0.333	3.918	0.000	Significant
H9	PA → TR	0.177	1.957	0.051	Not Significant
H10	IC → TR	0.337	3.542	0.000	Significant
H11	PC → PP	-0.051	1.438	0.151	Not Significant
H12	TR → PP	0.855	33.679	0.000	Significant

The results of Table IV about mobile banking users indicate that there is 5 (five) path correlation that significant in using mobile banking. They are privacy risk (PR) to privacy concern (PC), subjective norm (SN) to privacy concern (PC), subjective norm (SN) to trust (TR), information control (IC) to trust (TR), and trust (TR) to perceived privacy (PP).

The results of Table V about mobile payment users indicate that there are 6 (six) path correlations that significant in using mobile banking. They are privacy risk (PR) to privacy concern (PC), subjective norm (SN) to privacy concern (PC), subjective norm (SN) to trust (TR), information control (IC) to trust (TR), privacy concern (PC) to perceived privacy (PP), and trust (TR) to perceived privacy (PP).

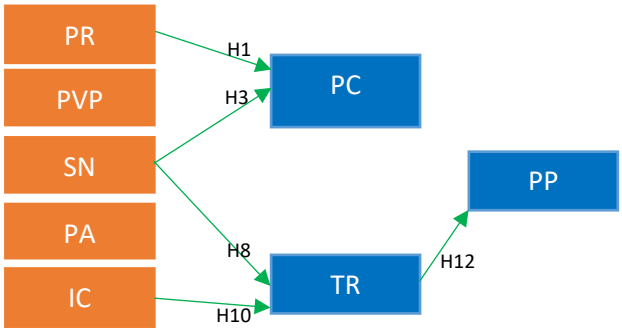

Figure 2. Result of mobile banking hypotheses

Table 5: Result of Mobile payment Hypothesis

Hypothesis	Paths	Original Sample	T-Statistic	P Values	Result
H1	PR → PC	0.405	4.876	0.000	Significant
H2	PVP → PC	0.221	1.828	0.068	Not Significant
H3	SN → PC	0.216	2.707	0.007	Significant
H4	PA → PC	-0.005	0.055	0.956	Not Significant
H5	IC → PC	-0.052	0.625	0.532	Not Significant
H6	PR → TR	0.024	0.336	0.737	Not Significant
H7	PVP → TR	-0.121	1.404	0.161	Not Significant
H8	SN → TR	0.268	3.058	0.002	Significant
H9	PA → TR	0.078	0.911	0.363	Not Significant
H10	IC → TR	0.523	6.483	0.000	Significant
H11	PC → PP	-0.085	2.177	0.030	Significant
H12	TR → PP	0.865	32.629	0.000	Significant

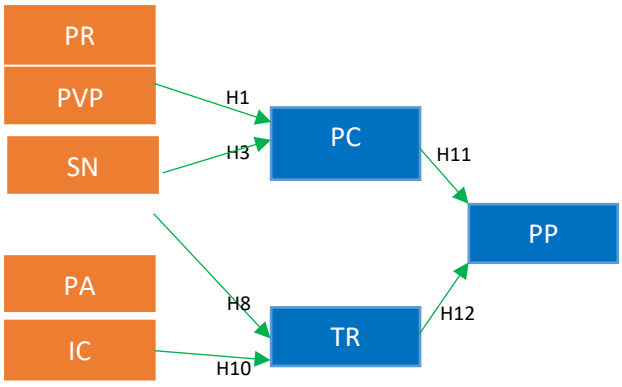

Figure 3. Result of mobile payment hypotheses

5. Conclusions

There is an exciting uniqueness in this study. The results obtained show that in the hypothesis, there are almost similarities that are statistically calculated for the same respondents as the use of mobile banking and mobile payment. In general, the same essential factors between mobile banking and mobile payment are privacy risk and subjective norm regarding privacy, subjective norms, and information control for trusts. This shows the similarity between mobile banking and mobile payment.

However, the difference that occurs is in mobile banking; privacy considerations do not have a significant effect on perceived privacy, while mobile payments for privacy and trust have a significant effect on perceived privacy. So the unique feature of this study is that privacy is significantly more critical for consumers to feel the perceived privacy.

In short, mobile banking is a product issued by a bank with a good reputation and building new electronic channels to facilitate consumers' use of bank access. Consumers will, therefore, have more confidence in the use of mobile banking issued by banks trusted by consumers. The bank also has an explicit agreement for consumers to use every product and service available in mobile banking. Such as the general terms and conditions that consumers must agree on when using mobile banking. This makes consumers feel comfortable with financial transactions with mobile banking.

That is why trust is perceived as valuable by consumer trust. The confidence that consumers have in the use of mobile banking also comes from important factors, namely the subjective standard and information control. The subjective norm is to follow what is driven or created by the social environment of consumers so that consumers also see from the perspective of others. An information check is a consumer who can easily use mobile banking with a check on the privacy of information about a consumer. Regarding privacy issues that are not significant to the perceived privacy. Concerning privacy issues, consumers who use mobile banking come from significant privacy risk and subjective standards. This is because consumers are still concerned about their privacy when using mobile banking, particularly concerning monitoring the risk of privacy and also subjective standards based on an understanding of the social environment of mobile banking for consumers.

With mobile payment, the same applies to mobile banking because of privacy and trust. Where privacy considerations are also significantly influenced by privacy risk and subjective norm. This is because consumers understand the privacy risks to be understood, and consumers also know that there are restrictions on the use of mobile payments so that consumers do not overthink about the risks that arise, so that consumers have understood the privacy risk. Moreover, on the subjective norm, consumers have been influenced by the social environment on the use of mobile payment and see from environmental factors that everything can go according to procedures agreed between the consumer and the manager of the mobile payment.

With mobile payment, however, privacy concerns significantly affect perceived privacy, which is what distinguishes between mobile payment and mobile banking. What has been explained above is that privacy issues in mobile banking do not affect perceived privacy. For the trust, the same thing with mobile banking is that there are subjective standards and information control factors that significantly affect trust. Moreover, the trust

factor has a significant effect on the perceived privacy. Viewed from the same two fields in financial technology, consumers will feel the same in terms of confidence in mobile payment. Because of the subjective norm that consumers feel in the social environment and also information management, that gives consumers more freedom to control the receipt and provision of information on the mobile payment platform.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] S. Rathore, "Adoption of digital wallet by consumers," *BVIMSR's J. Manag. Res.*, vol. 8, pp. 69–75, 2016.

[2] T. T. T. Pham and J. C. Ho, "The effects of product-related, personal-related factors and attractiveness of alternatives on consumer adoption of NFC-based mobile payments," *Technol. Soc.*, vol. 43, pp. 159–172, 2015.

[3] V. Kumar and W. Reinartz, "Customer Privacy Concerns and Privacy Protective Responses," pp. 285–309, 2018.

[4] P. Su, L. Wang, and J. Yan, "How users' Internet experience affects the adoption of mobile payment: a mediation model," *Technol. Anal. Strategy. Manag.*, vol. 30, no. 2, pp. 186–197, 2018.

[5] A. C. Teo, G. W. H. Tan, K. B. Ooi, T. S. Hew, and K. T. Yew, "The effects of convenience and speed in m-payment," *Ind. Manag. Data Syst.*, vol. 115, no. 2, pp. 311–331, 2015.

[6] A. Upadhayaya, "Electronic Commerce and Mobile payment," vol. I, no. March, pp. 37–41, 2012.

[7] K. B. Ooi and G. W. H. Tan, "Mobile technology acceptance model: An investigation using mobile users to explore smartphone credit card," *Expert Syst. Appl.*, vol. 59, pp. 33–46, 2016.

[8] M. A. Shareef, A. Baabdullah, S. Dutta, V. Kumar, and Y. K. Dwivedi, "Consumer adoption of mobile banking services: An empirical examination of factors according to adoption stages," *J. Retail. Consum. Serv.*, vol. 43, no. December 2017, pp. 54–67, 2018.

[9] Y. U. Chandra, "Bank vs Telecommunication Mobile payment : System Analysis , Purchase , and Payment Method of GO- Mobile CIMB Niaga and T-Cash Telkomsel," no. November, pp. 165–170, 2017.

[10] Y. U. Chandra, D. M. Kristin, J. Suhartono, F. S. Sutarto, and M. Sung, "Analysis of Determinant Factors of User Acceptance of Mobile Payment System in Indonesia (A Case Study of Go-Pay Mobile Payment)," *Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, no. September, pp. 454–459, 2018.

[11] M. Karsen, Y. U. Chandra, and H. Juwitasary, "Technological factors of mobile payment: A systematic literature review," *Procedia Comput. Sci.*, vol. 157, pp. 489–498, 2019.

[12] Y. Chang, S. F. Wong, C. F. Libaque-Saenz, and H. Lee, "The role of privacy policy on consumers' perceived privacy," *Gov. Inf. Q.*, vol. 35, no. 3, pp. 445–459, 2018.

[13] Y. Yang, Y. Liu, H. Li, and B. Yu, "Understanding perceived risks in mobile payment acceptance," *Ind. Manag. Data Syst.*, vol. 115, no. 2, pp. 253–269, 2015.

[14] A. Rauzzino and J. C. Correa, "Diferencias por sexo de los «Millenials» sobre la privacidad percibida en Snapchat," *Suma Psicol.*, vol. 24, no. 2, pp. 129–134, 2017.

[15] K. Degirmenci, "Mobile users' information privacy concerns and the role of app permission requests," *Int. J. Inf. Manage.*, vol. 50, no. April 2019, pp. 261–272, 2020.

[16] A. R. Jung, "The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern," *Comput. Human Behav.*, vol. 70, pp. 303–309, 2017.

[17] N. E. Frye and M. M. Dornisch, "When is trust not enough? the role of perceived privacy of communication tools in comfort with self-disclosure," *Comput. Human Behav.*, vol. 26, no. 5, pp. 1120–1127, 2010.

[18] J. Henriksen-Bulmer, S. Faily, and S. Jeary, "Privacy risk assessment in context: A meta-model based on contextual integrity," *Comput. Secur.*, vol. 82, pp. 270–283, 2019.

[19] G. de Kerviler, N. T. M. Demoulin, and P. Zidda, "Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers?," *J. Retail. Consum. Serv.*, vol. 31, pp. 334–344, 2016.

[20] H. Jia and H. Xu, "Measuring individuals' concerns over collective privacy on social networking sites," *Cyberpsychology*, vol. 10, no. 1, 2016.

[21] F. Xu, K. Michael, and X. Chen, "Factors affecting privacy disclosure on social network sites: An integrated model," *Electron. Commer. Res.*, vol. 13, no. 2, pp. 151–168, 2013.

[22] I. D. Anic, V. Škare, and I. Kursan Milaković, "The determinants and effects of online privacy concerns in the context of e-commerce," *Electron. Commer. Res. Appl.*, vol. 36, no. June, 2019.

[23] C. M. Ringle, S. Wende, and J.-M. Becker, "SmartPLS 3." SmartPLS GmbH, 2015.