Jimcts

プライバシー計算理論を用いたキャッシュレス社会における「プライバシー・パラドックス」現象に関する実証研究

北海道大学大学院国際広報メディア・観光学院　修士課程
楊　　婕

The 'Privacy Paradox' in Japan's Cashless Society: An Empirical Study of Japanese Mobile Payment Users

YANG Jie

abstract

Japan has been recently focused on creating a 'cashless society'. Many of its banks and companies have been trying to promote Quick Response (QR) code payments. For example, large companies such as PayPay, LINE and Rakuten have been distributing tens of billions of yen in subsidies to users in order to stimulate the use of these payments.

However, while users are concerned that their personal information might be compromised, they are still benefitting from a variety of promotions, which is known as the 'Privacy Paradox'. Therefore, this study examines whether this paradox exists among Japanese mobile payment users by using the Privacy Calculus Theory (PCT), combined with the Theory of Planned Behavior (TPB). The results show that this paradox exists and perceived benefits are the moderating variable affecting it. In addition, perceived behavioral control positively influences privacy disclosure intentions and behaviors.

1 Introduction

Starting with the‘Japan Revitalization Strategy’(Revised, 2014), the Japanese government has been steadily promoting a cashless society by annually implementing a variety of measures. From October 2019 to June 2020, Japan's cashless payment market is experiencing an upward trend, triggered by the Ministry of Economy, Trade and Industry (METI)'s Point Reward Project. This was a time-limited program where consumers received a maximum 5% of purchases back as points when they used a cashless payment method (such as PayPay, Suica, or credit cards) at certain stores and e-commerce (EC) sites.

After the project ended, over 27,000 consumers were surveyed about their cashless payments (METI, 2020). The increase in QR code payments was particularly significant since this project's implementation. However, the use of these payments is still low, with only 17.4% of consumers using them at least once a week. On the other hand, credit cards have been found to dominate the market: the number of consumers who used them at least once a week amounted to 34.1% of the total. This means it has been difficult for these payments to gain popularity throughout Japan.

At the same time, many payment service providers have competed fiercely for mobile payment customers. The common format for electronic payments on mobile phones is‘XX pay’. Furthermore, Japan currently has more than 15 QR code payment platforms. The fields involved in these platforms include the Internet, communications, logistics, banking, and foreign companies. Cash-back campaigns are one of Japan's most common strategies for acquiring more users. In one prominent example, SoftBank drove users' uptake of PayPay by giving away 10 billion yen in 10 days. In addition, PayPay has attracted more than 45 million registered users since its launch in 2018, currently making it Japan's most frequently used QR code payment service.

As a result of its strong governmental and business promotion, although Japan's cashless payment ratio rose to 29.7% in 2020 (METI, 2020), it is still well below the global average. Therefore, Japan is often viewed as an underdeveloped country in terms of cashless payments. Survey results showed that one of the reasons for this was users' concerns about how companies managed their personal information (METI, 2020). Frequent cases of information breaches and hacking prove that these concerns are not unfounded. It is therefore necessary to find out which factors influence users' voluntary adoption and use of QR code payments when facing the risk of privacy breaches.

Various theories have been applied to explain this phenomenon, the most frequent of which are the Privacy Calculus Theory (PCT) and the Theory of

楊　婕　YANG Jie

Planned Behavior (TPB). According to PCT, perceived risks and perceived benefits influence privacy concerns, and users tend to disclose their privacy when they see more benefits than risks (Han *et al*., 2019). This study attempts to explore whether a 'Privacy Paradox' exists among Japanese mobile payment users by examining whether a contradiction exists between users' attitudes and behaviors.

2 Literature Review

2.1 Privacy Calculus Theory

Culnan and Armstrong (1999) originally proposed PCT, which argues that when disclosing their privacy, individuals try to obtain the maximum benefit at the minimum cost. Thus, they act after completing a risk-benefit calculation. As it is difficult to measure the concept of privacy itself, researchers developed the concept of privacy concerns, which is individuals' attitude towards privacy. In addition, since attitudes include both positive and negative aspects, the main focus of this study is on negative attitudes toward individuals' fear of privacy disclosure.

Perceived benefits and perceived risks are two key variables in research on personal information disclosure. Generally speaking, a higher perceived benefit involves a greater likelihood that an individual will disclose his or her privacy. Conversely, a higher perceived risk implies a higher likelihood of an individual disclosing their private information. Therefore, service providers have to motivate users by increasing their perceived benefits and reducing their perceived risks in order to improve their experience and convince them to actively use a service.

In addition, many factors influence privacy disclosure behavior. For example, Dinev and Hart (2006) presented a model of the relationship between trust in platforms and personal information disclosure in e-commerce. Additionally, Martin and Shilton (2016) indicated that the experience of using mobile apps mitigates the influence of personal preferences and contextual factors on privacy decisions.

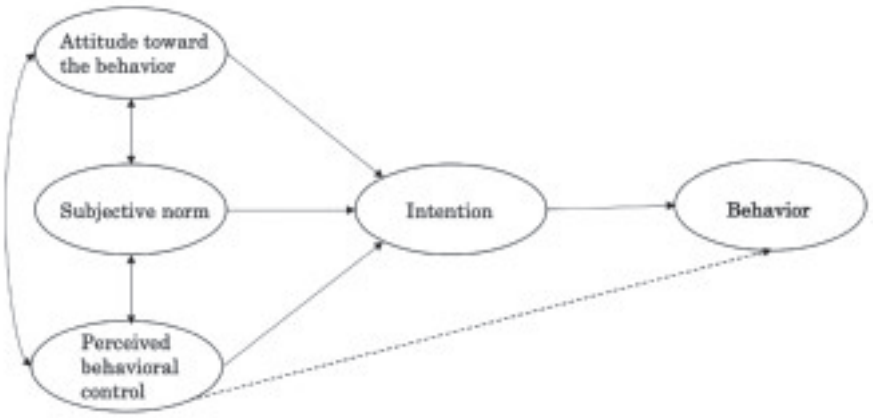
However, these previous studies separately examined the effects of perceived benefits or perceived risks on privacy concerns and privacy disclosure intentions. That is, these studies analyzed these aspects separately as independent and dependent variables when constructing their models. This does not dynamically depict the changing relationship between privacy concerns and privacy disclosure behaviors. Therefore, we propose to examine whether perceived benefits, perceived risks, trust in platforms, and usage experience impact the privacy paradox when they are moderating variables between privacy concerns and privacy disclosure intentions.

2.2 Theory of Planned Behavior

Ajzen (1991) presented the Theory of Planned Behavior (TPB) as an extension of the Theory of Reasoned Action (TRA). While TRA views attitudes towards behavior and subjective norms as factors influencing behavioral intentions, TPB adds perceived behavioral control, a personal and situational factor acting as a controlling factor for actual human behavior, as a new factor. In other words, TPB is most effective in situations where it is difficult to control behavior or when it is difficult for a person to perform solely based on his or her own volition.

Ajzen and Fishbein (1991) argued that attitudes toward behavior are beliefs and evaluations of the results obtained from an action. Moreover, subjective norms are perceptions related to how a person or group of people around them perceive a specific action that the actor considers important (Ajzen & Fishbein, 1991). This specific concept can be regarded as social pressure related to specific behaviors. Perceived behavioral control is the availability of the skills, resources, and opportunities necessary for initiating behavior, and this consists of an individual's perceived beliefs about control and their perceived ease of evaluating the importance of those beliefs. According to TPB, a more positive attitude towards an action increases the likelihood of others having higher expectations of that action, while if an action is more feasible for this individual, it is more likely that they will implement this action. If an individual believes that an action is more feasible for them, they are more likely to implement it. TPB predicts prudent behavior because behavior can be planned, and this theory helps to explain the gap between awareness and behavior (Sentosa & Mat, 2012).

Figure 1. Theory of Planned Behavior (Ajzen, 1991)



TPB has been applied in multiple disciplines to predict human behavior (Conner & Armitage, 1998). However, not all variables in the model can be measured in different contexts. Therefore, we decided to integrate privacy concerns from PCT and attitudes from TPB into one variable. Our study is about how users perceive

楊 婕 YANG Jie

privacy when using QR code payments, which is a sense that comes primarily from themselves rather than from the outside world, so we removed the subjective norms from the original model and focused on perceived behavioral control that focuses on their own capabilities.

2.3 Privacy Paradox

The‘Privacy Paradox’is a concept first mentioned in Brown (2001). The discrepancy between attitudes of privacy concerns and actual self-disclosure behavior is referred to as the‘privacy paradox’. Some studies have combined TPB and PCT to explore whether the privacy paradox exists.

Most previous studies on the‘Privacy Paradox’focus on personal information on social networking sites (e.g., Taddicken, 2014; Zhu *et al*., 2017) or e-commerce (e.g., Xu *et al*., 2011; Wilson & Valacich, 2012). While e-commerce and QR code payments are both money-related areas that require users to provide more accurate and detailed personal information than on general social networks, QR code payment services are a new and growing means of payment in Japan and very limited research exists on the privacy paradoxes associated with them. Therefore, it is important to consider the possibility of the‘Privacy Paradox’from this perspective.

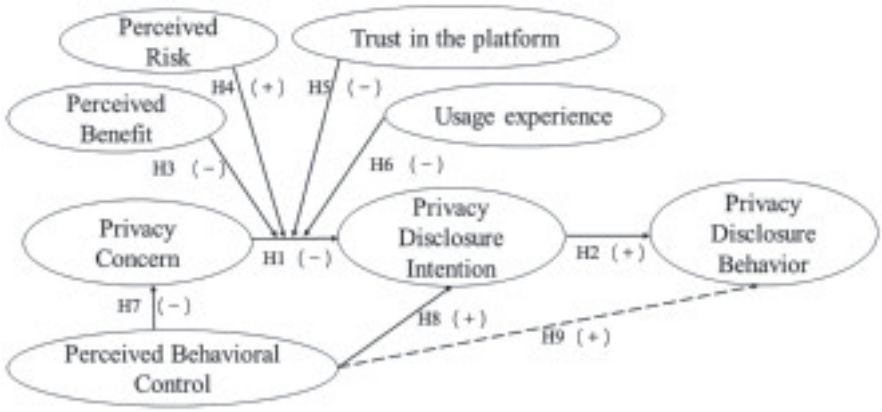
Through questionnaires, both Tabata (2014) and Mikami (2016) testified to the existence of the privacy paradox when Japanese people use the SNS. However, none of them has developed a comprehensive research model to explain the relationship among variables in a more systematic way. Consequently, we think it is necessary to discuss the privacy paradox in Japanese society in the context of a theoretical model whose effectiveness has been proven on numerous occasions.

However, previous research has indicated that there are two main ways to demonstrate the existence of the privacy paradox (Kokolakis, 2017). In the first, when privacy concerns negatively affect privacy disclosure intentions and when privacy disclosure intentions positively affect privacy disclosure behaviors, privacy concerns and privacy disclosure behaviors conflict with each other, causing the privacy paradox to exist (Acquisti *et al*., 2015). In the second case, when the variables of privacy concerns and privacy disclosure intentions are unrelated (i.e., p-values greater than 0.05), it indicates that privacy concerns and privacy disclosure intentions are unrelated and a privacy paradox exists (Martin, 2016). Therefore, while verifying the former case, this study also tries to find if there is another way to prove the privacy paradox.

3. Conceptual Model and Hypotheses

The research model for this study is presented below. By referring to PCT and TPB, this study discusses whether the 'Privacy Paradox' exists for Japanese users of QR code payments.

■Figure 2. Conceptual Model



3.1 Privacy concern

A commonly agreed definition of information privacy concern is "the extent to which individuals are concerned about how their personal information is collected and used by an organization" (Smith *et al*., 1996). Many studies are based on TPB, which suggests that privacy behavior can be effectively explained when privacy attitudes, privacy concerns, and privacy intentions are introduced. Since using QR code payments requires more detailed and accurate information than SNS, we believe that users will pay closer attention to the information provided to these payment platforms (e.g., Li, 2021; Lutz & Tamó-Larrieux, 2020). In addition, according to the Oricon Customer Satisfaction Survey (2020), Japanese consumers mentioned that uneasiness about the possibility of their personal privacy being compromised as one of the reasons why they do not often use these payments. Based on the above observations, this study considers privacy issues as a type of privacy attitude, i.e., negative attitudes toward the collection, use, and control of privacy. Therefore, this study proposes the following hypothesis:

H1: Privacy concerns of QR code payments' users negatively influence their privacy disclosure intentions.

3.2 Intention and Behavior

According to Ajzen (1991), intention is an individual's tendency to act in a particular way. Thus, intention is necessary for any behavior and the decision preceding behavior. As a result, as a third variable, 'intention' is used to resolve the contradiction between attitude and behavior (Hermes *et al*., 2021). In this study, we consider that users disclose privacy when they pay with QR codes. Before becoming a QR code payment user, individuals need to enter their information for real-name authentication. After becoming a user, the QR code payment platform will obtain all of their purchase records. Therefore, in the model, payment with QR codes is represented as privacy disclosure. Based on the above statements, this hypothesis is proposed:

H2: The privacy disclosure intentions of QR code payments' users positively influence their privacy disclosure behaviors.

3.3 Perceived benefit

Perceived benefit is a very important variable in PCT. It is believed that factors related to gaining benefits can play a motivational role in self-disclosure. In social networks, users gain social identity and interpersonal relationships by disclosing personal privacy (Han *et al*., 2019), while in e-commerce, users receive personalized services by disclosing their privacy (Sun *et al*., 2019).

However, in these studies, perceived benefit is used as an independent variable to explore the relationship with privacy concerns or privacy disclosure intentions, respectively. This study argues that this may not explore the dynamics of these two variables as they interact in the privacy paradox. Therefore, regarding it as a moderating variable between privacy concerns and privacy disclosure intentions, the following hypothesis is proposed:

H3: Perceived benefits moderate the impact of privacy concerns on privacy disclosure intentions.

3.4 Perceived risk

Like perceived benefit, perceived risk is also an important variable in PCT. Perceived risk is defined as the user's subjective beliefs about the potential losses they could experience. In social networks, it could be the risk of getting scammed or harassed (Dinev *et al*., 2006). In e-commerce, it could be the risk of property loss due to bank card information leakage (Shaw & Sergueeva, 2018). Therefore, this study proposes this hypothesis:

H4: Perceived risks moderate the impact of privacy concerns on privacy disclosure intentions.

3.5 Trust in the platform

In addition to perceived benefit and perceived risk, this study hypothesizes that other factors also moderate the relationship between privacy concerns and privacy disclosure intentions. For example, trust is "the belief that the service providers will perform certain activities in accordance with the user's expectations" (Khalilzadeh *et al*., 2017). According to Shin (2009), trust in virtual malls positively affects the customer's intention to use a mobile wallet. Therefore, this study intends to examine whether trust in platforms remains valid when it is used as a moderating variable. Based on the studies above, we propose this hypothesis:

H5: Trust in platforms moderates the impact of privacy concerns on privacy disclosure intentions.

3.6 Usage experience

De Kerviler *et al*. (2016) considered that perceived risk and convenience are not the only drivers regarding the adoption of in-store mobile payment. As De Kerviler *et al*. (2016) also investigated differences in the drivers of mobile shopping compared to more familiar ones, and highlighted the role of usage experience, the following hypothesis is proposed:

H6: Usage experience moderates the impact of privacy concerns on privacy disclosure intentions.

3.7 Perceived behavioral control

As previously mentioned, perceived behavioral control is the availability of the skills, resources, and opportunities necessary for initiating behavior, and it consists of an individual's perceived beliefs about control and the perceived ease of evaluating these beliefs' importance (Ajzen & Fishbein, 1991). Moreover, a strong user initiative is required when paying with QR code payments. If the user refuses to use these payments, they prevent any possibility of privacy disclosure to the platform. However, even if users start using these payments, the frequency of use will affect the degree of privacy disclosure (Zhang *et al*., 2019). As a result, this study represents the controls for the degree of privacy disclosure in the model as perceived behavioral controls. Therefore, the following three hypotheses are proposed:

H7: Perceived behavioral control negatively influences privacy concerns.

H8: Perceived behavioral control positively influences privacy disclosure intentions.

H9: Perceived behavioral control positively influences privacy disclosure behaviors.

If the negative effect of privacy concerns on privacy disclosure intentions is moderated by the moderating effect of four moderating variables, then privacy concerns and privacy disclosure behavior conflict with each other and a privacy paradox exists. Moreover, four moderating variables are influential in the changes that occur in the privacy paradox.

4 Research Methodology

4.1 Data Collection

A preliminary survey of Japanese university students who have used LINE Pay was conducted. Although official data from LINE Pay indicated that the main users of LINE Pay were young people aged 20 to 29. Analysis of the 110 questionnaires returned showed that these students did not use LINE Pay very often, which may be related to their generally low income. This factor may lead to inaccuracies in the impact of privacy concerns on privacy disclosure intentions. According to the results, the questionnaire was revised.

Therefore, in order to obtain more significant findings, the scope of the study was expanded for the formal survey to include all age groups who have used QR code payments. In April 2022, we commissioned Freeasy Research Company to conduct an online survey of Japanese users who previously used these payments. The survey used a five-point Likert Scale (1 = strongly disagree to 5 = strongly agree). Its items were based on the TPB, thoroughly validated in other related studies, and modified accordingly to fit the characteristics of the these payments.

Table 1 Questionnaire Items

Construct	Measurement Items		References
Privacy Concerns (PC)	PC1	I am sensitive about giving out information regarding my preferences.	Chellappa & Sin (2005)
	PC2	I am concerned about anonymous information (e.g., network information, application, etc.) that is collected about me.	
	PC3	I am concerned about how my personally un-identifiable information (e.g., Zip Code, age-range, sex, etc.) will be used by the firm.	
	PC4	I am concerned about how my personally identifiable information (e.g., name, shipping address, credit card or bank account information, etc.) will be used by the firm.	

Privacy Disclosure Intention (PDI)		PDI1	I will continue to use QR code payment in the future.	Lee *et al.* (2019).
		PDI2	I will use the QR code payment more often than now.	
		PDI3	I will use the QR code payment more actively than the usual payment methods.	
Privacy Disclosure Behavior (PDB)		PDB1	I frequently use the QR code payment.	Zhang *et al.* (2019). Nguyen & Khoa (2019)
		PDB2	I provide my personal information when asked by QR code payment company. (e.g., Zip Code, age-range, sex, etc.)	
		PDB3	I often disclose even sensitive personal information to QR code payment company. (e.g., different bank accounts, etc.)	
Privacy Behavioral Control (PBC)		PBC1	I think I have the skill to keep my privacy in QR code payment securely.	Zhang *et al.* (2019)
		PBC2	I think that I am in control over the data securely in QR code payment.	
		PBC3	I think that I am capable of preventing security risk in QR code payment.	
Perceived Benefit (PB)	Convenience	PB1	Using the QR code payment would allow me to save time during my shopping.	Kerviler *et al.* (2016). Sun *et al.* (2019)
		PB2	Using the QR code payment would be a convenient way to do shopping.	
		PB3	Using the QR code payment can provide me with personalized services.	
	Economic	PB4	Using the QR code payment would allow me to do my shopping at a lower financial cost. (e.g., cashback.)	
		PB5	Using the QR code payment would allow me to save money. (e.g., coupon.)	
		PB6	Using the QR code payment would allow me to take advantage of promotional offers. (e.g., campaign.)	
Perceived Risk (PR)	Transaction Risk	PR1	When using the QR code payment, I feel that my payment data would be compromised.	Shaw & Sergueeva (2018)

		PR2	When using the QR code payment, I feel that there would be a transaction error.	Dinev *et al.* (2006), Shaw & Sergueeva (2018)
		PR3	When using the QR code payment, I feel that hackers would access my payment data.	
	Privacy Risk	PR4	I believe if I use the QR code payment, personal information submitted could be misused.	
		PR5	I believe if I use the QR code payment, personal information could be made available to others without my knowledge.	
		PR6	I believe if I use the QR code payment, my personal privacy could be threatened.	
Trust in the Platform (TP)		TP1	I believe the service providers of QR code payments keep their promise.	Khalilzadeh *et al.* (2017)
		TP2	I believe the service providers of QR code payments keep customers' interests in mind.	
		TP3	I believe the service providers of QR code payments are trustworthy.	
		TP4	I believe the service providers of QR code payments will do everything to secure the transactions for users.	
Usage Experience (UE)		UE1	I have a great deal of experience with using the QR code payment for shopping.	De Kerviler *et al.* (2016)
		UE2	I am familiar with the different functionalities of the QR code payment for shopping.	
		UE3	I frequently update my knowledge about the functionalities of the QR code payment for shopping.	

■Table 2 Demographic Characteristics of the Respondents

Category	Item	Frequency (N=382)	Percentage (%)
Gender	Male	188	49.21
	Female	194	50.79
Age	Under 20	27	7.07
	20-29	79	20.68
	30-39	82	21.47
	40-49	92	24.08

	50-59	81	21.20
	Over 60	21	5.50
Annual income	Less than 1 million yen	32	8.38
	1～2 million yen	22	5.76
	2～3 million yen	30	7.85
	3～4 million yen	53	13.87
	4～5 million yen	51	13.35
	5～6 million yen	36	9.42
	6～7 million yen	30	7.85
	7～8 million yen	25	6.54
	8～9 million yen	18	4.71
	9～10 million yen	39	10.21
	10～12 million yen	18	4.71
	12～15 million yen	14	3.66
	15～18 million yen	3	0.79
	18～20 million yen	4	1.05
	More than 20 million yen	7	1.83
Frequency of usage	Almost every day	55	14.40
	4～5 days a week	52	13.61
	2～3 days a week	109	28.53
	About 1 day a week	60	15.71
	About 1 day every 2～3 weeks	41	10.73
	About 1 day per month	43	11.26
	Lower than the above	22	5.76

4.2 Data Analysis

Subsequently, 382 valid responses were collected from Japanese users who had used QR code payments. The demographic characteristics are displayed in Table 2. The gender composition was 188 (49.21%) male and 194 (50.79%) female, and the age composition was relatively evenly distributed, with 79-92 (about 20% each) in their 20s, 30s, 40s, and 50s, respectively. The largest number of respondents were in their 40s, which may be related to the fact that their income level is at a relatively high value. Respondents' annual income was mainly between 1 ～ 10 million yen, accounting for about 79.56% of the total. And about the frequency of usage, most people use it at least about 1 day per month, while 2-3 days a week or more is the most common use.

The collected data was explored using SPSS and AMOS software to understand the relationships between the variables. Since new moderating variables were added to the original TPB model, they were first examined by using Exploratory Factor Analysis (EFA), followed by Confirmatory Factors Analysis (CFA).

5 Results and Discussion

5.1 Measurement Model

Factor extraction was analyzed using the maximum likelihood method, and factor rotation was analyzed using the Promax method.

Table 3 Results of Exploratory Factor Analysis

Item	Factor Loading							
	1	2	3	4	5	6	7	8
Factor1: Perceived Risk (PR) α = 0.929								
PR 5	**0.931**	0.157	0.064	-0.042	0.002	-0.101	-0.095	-0.068
PR 6	**0.860**	0.015	0.033	-0.066	0.004	0.004	-0.018	-0.013
PR 4	**0.856**	-0.014	-0.065	-0.067	-0.044	0.094	-0.002	0.060
PR 3	**0.852**	0.026	0.032	0.043	-0.036	-0.013	0.030	0.009
PR 1	**0.736**	-0.101	-0.100	0.099	0.021	0.037	0.156	0.001
PR 2	**0.689**	-0.152	-0.028	0.074	0.110	0.047	0.004	0.074
Factor2: Trust in the Platform (TP) α = 0.904								
TP 4	0.010	**0.932**	0.005	0.001	0.009	-0.084	0.017	-0.007
TP 3	0.008	**0.892**	0.024	0.003	0.031	0.010	-0.031	-0.035
TP 1	-0.041	**0.649**	0.046	0.037	-0.046	0.112	-0.005	0.071
TP 2	-0.056	**0.527**	-0.156	0.133	0.060	0.275	0.051	0.034
Factor3: Privacy Disclosure Intention (PDI) α = 0.867								
PDI 3	-0.048	-0.037	**0.920**	0.077	0.014	-0.006	-0.027	-0.017
PDI 2	0.000	-0.003	**0.733**	0.009	0.022	0.118	0.025	0.062
PDI 1	0.007	0.026	**0.710**	-0.056	-0.006	0.034	0.047	-0.008
Factor4: Privacy Behavioral Control (PBC) α = 0.857								
PBC 1	0.021	-0.022	0.007	**0.858**	0.023	-0.027	-0.050	0.005
PBC 2	0.060	0.084	-0.020	**0.804**	-0.087	0.077	-0.022	-0.051
PBC 3	-0.061	0.003	0.053	**0.782**	0.053	-0.111	0.044	0.041
Factor5: Usage Experience (UE) α = 0.880								
UE 2	-0.058	-0.083	-0.017	-0.018	**0.884**	0.084	0.028	0.046
UE 1	0.086	0.091	0.131	-0.050	**0.827**	-0.139	-0.072	-0.049
UE 3	0.014	0.032	-0.093	0.068	**0.810**	0.051	0.027	-0.023
Factor6: Perceived Benefit (PB) α = 0.847								
PB 4	0.043	-0.076	0.106	-0.022	0.009	**0.921**	-0.056	-0.083
PB 5	0.020	0.062	-0.026	-0.014	-0.037	**0.813**	-0.052	-0.031
PB 6	0.047	0.088	0.177	0.027	-0.030	**0.528**	0.040	0.029
PB 3	-0.086	0.149	0.038	-0.073	0.074	**0.455**	0.086	0.104
Factor7: Privacy Concerns (PC) α = 0.868								
PC 3	0.084	0.020	0.015	0.001	0.006	-0.020	**0.800**	-0.006
PC 2	0.060	-0.058	-0.046	-0.004	0.004	0.046	**0.786**	0.012

PC 4	0.143	0.072	0.098	-0.035	-0.036	-0.107	**0.718**	-0.053
Factor8: Privacy Disclosure Behavior (PDB) α = 0.759								
PDB 2	0.017	0.028	-0.007	-0.051	-0.016	-0.071	-0.033	**1.057**
PDB 3	0.047	-0.009	0.053	0.115	-0.006	0.051	0.007	**0.527**

After EFA, four items (PC1, PDB1, PB 1, PB 2) with factor loadings less than 0.3 were removed. The KMO value was 0.905 and the significance probability of Bartlett's sphericity test was 0.000, which were suitable for factor analysis.

■Table 4　Results of Convergent Validity

Construct	Item	Factor Loading	Composite Reliability	AVE
Privacy Disclosure Intention	PDI 1	0.722	0.891	0.733
	PDI 2	0.885		
	PDI 3	0.880		
Privacy Concerns	PC 1	–	0.868	0.686
	PC 2	0.793		
	PC 3	0.855		
	PC 4	0.837		
Privacy Behavioral Control	PBC 1	0.844	0.878	0.705
	PBC 2	0.806		
	PBC 3	0.801		
Privacy Disclosure Behavior	PDB 1	–	0.766	0.622
	PDB 2	0.837		
	PDB 3	0.731		
Trust in the Platform	TP 1	0.808	0.921	0.744
	TP 2	0.808		
	TP 3	0.894		
	TP 4	0.858		
Perceived Risk	PR 1	0.821	0.932	0.698
	PR 2	0.705		
	PR 3	0.865		
	PR 4	0.854		
	PR 5	0.861		
	PR 6	0.858		
Usage Experience	UE 1	0.803	0.877	0.705
	UE 2	0.879		
	UE 3	0.847		
Perceived Benefit	PB 1	–	0.861	0.608
	PB 2	–		
	PB 3	0.692		
	PB 4	0.838		
	PB 5	0.769		
	PB 6	0.765		

Then, convergent validity was confirmed. As performed in Table 4, the factor loading of PB3 (0.692) was less than 0.70, but considering the validity of its content, it was not removed and used as before. Except for this, all other factor loadings exceeded 0.70. And all the values of C.R. and AVE were higher than the recommended levels 0.70 and 0.50 respectively. The Cronbach's α coefficients of each variable and the factor loadings of most items also exceeded 0.70. Therefore, the measurement model's convergent validity was supported.

■Table 5 Results of Discriminant Validity

		Correlation of constructs							
Variable	AVE	PC	PDI	PDB	PBC	PR	TP	UE	PB
PC	0.686	**0.829**							
PDI	0.733	0.287	**0.856**						
PDB	0.622	0.036	0.459	**0.789**					
PBC	0.705	-0.020	0.366	0.529	**0.840**				
PR	0.698	0.668	0.065	0.035	-0.119	**0.835**			
TP	0.744	0.092	0.588	0.582	0.663	-0.078	**0.863**		
UE	0.705	0.064	0.476	0.422	0.500	0.105	0.521	**0.839**	
PB	0.608	0.180	0.742	0.580	0.480	0.033	0.764	0.550	**0.780**

Note. PC = Privacy concerns; PDI = Privacy disclosure Intention; PDB = Privacy disclosure behavior; PBC = Privacy behavioral control; PR = Perceived risk; TP = Trust in the platform; UE = Usage experience; PB = Perceived benefit. The square roots of AVE are highlighted in bold.

The measurement model was estimated by using CFA. and a good model fit (Toyota, 2007, pp.236-245) was demonstrated (χ^2/ df =1.812, GFI =0.969, AGFI =0.947, CFI =0.985, NFI =0.967, TLI =0.978, SRMR =0.0316, RMSEA =0.046).

5.2 Structural Model

The model fit was χ^2/ df =1.778, GFI =0.969, AGFI =0.948, CFI =0.985, NFI =0.967, TLI =0.979, =0.045, all of which met the same recommended criteria as above.

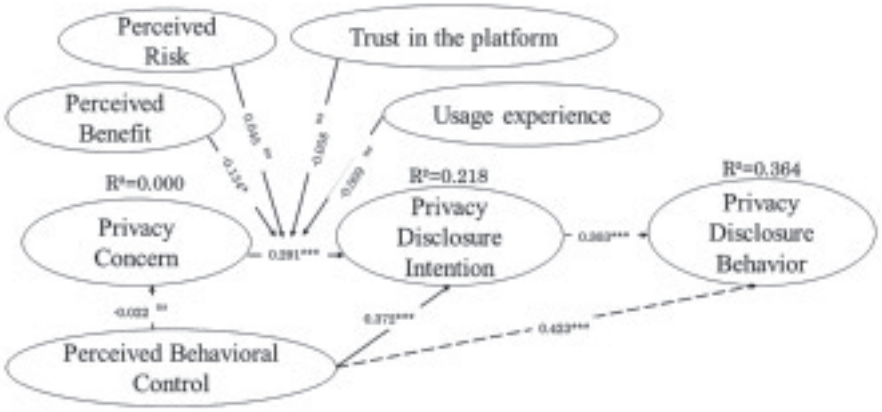
■Table 6 Analysis Results of the Model by Path Analysis

Hypothesis	Path	Estimate	t value	P value	Test Result
H1	PC → PDI	0.291	5.175	0.000	supported
H2	PDI → PDB	0.303	4.898	0.000	supported
H3	PB → (PC→PDI)	-0.134	-2.261	0.024	supported
H4	PR → (PC→PDI)	0.045	1.122	0.262	unsupported
H5	TP → (PC→PDI)	-0.058	-1.005	0.315	unsupported
H6	UE → (PC→PDI)	-0.009	-.187	0.852	unsupported
H7	PBC → PC	-0.022	-0.367	0.714	unsupported
H8	PBC → PDI	0.372	6.409	0.000	supported

H9	PBC → PDB	0.423	6.628	0.000	supported
R^2					
Privacy concerns			0.000 (0.0%)		
Privacy disclosure intention			0.218 (21.8%)		
Privacy disclosure behavior			0.364 (36.4%)		

Note. PC = Privacy concerns; PDI = Privacy disclosure intention; PDB = Privacy disclosure behavior; PBC = Privacy behavioral control; PB = Perceived benefit; PR = Perceived risk; TP = Trust in the Platform; UE = Usage Experience.

■Figure 3. Result of structural model test



*p < 0.05; ***p < 0.001; ns: non-significant at the 0.05 level

As shown in Table 5, privacy concerns positively influenced privacy disclosure intentions, and privacy disclosure intentions positively influenced their privacy disclosure behaviors. In addition, perceived benefits negatively moderated the impact of privacy concerns on privacy disclosure intentions. Furthermore, perceived behavioral control positively influenced privacy disclosure intentions and privacy disclosure behaviors.

However, a clear causal relationship between perceived behavioral control and privacy concerns was not verified. In addition, the moderating effect of perceived risks, trust in platforms, and usage experience were not proven. In other words, H4, H5, H6, and H7 were rejected, while the others were supported.

It is worth noting that the results of the study and of H1 were contradictory. By examining demographic characteristics, we found that respondents generally used QR code payments more frequently, which involved a larger proportion of middle and upper class income groups. Additionally, the average point for the variable of privacy concerns was higher than 3 (the mean). Therefore, we argue that when privacy disclosure intention is sufficiently strong, even with the effect of privacy concerns, it does not weaken the variable of privacy disclosure intention. Meanwhile, privacy disclosure intention has a positive effect on privacy disclosure behavior, demonstrating the existence of a privacy paradox.

6 Conclusion

6.1 Discussions and Implications

This study examined whether there is a 'Privacy Paradox' among Japanese QR code payment users based on PCT combined with TPB. It would be possible to understand the factors influencing this paradox by examining whether a contradiction exists between users' attitudes and behaviors.

Firstly, although contrary to the hypothesis, when privacy concerns are higher, privacy disclosure intentions are also higher. This path exemplifies the existence of a privacy paradox. Then, as with previous research, higher privacy disclosure intentions implies more privacy disclosure behaviors. Secondly, although perceived behavioral control cannot influence privacy concerns, it positively affects privacy disclosure intentions and behaviors. Therefore, when users more adept manage their privacy, they are more likely to disclose it. Finally, regarding the moderating variable, although only the perceived benefit is valid, the conclusions drawn based on it are worth exploring. The positive impact of privacy concerns on privacy disclosure intentions diminishes as users perceive more benefits. In other words, providers of QR code payment services cannot just increase their promotions, as this will instead reduce users' loyalty.

We believe there are two reasons why H1 contradicts the results. One of these reasons is that some users are already accustomed to using QR code payments: about five years have passed since the beginning of Japan's widespread promotion of these payments. Thus, it is possible that the effect of privacy concerns on privacy disclosure intentions shifts from negative to positive, i.e., privacy concerns affect users' privacy disclosure from the beginning of these intentions. The second reason may be the order of the questionnaire items. When editing the questionnaire, we chose the privacy disclosure intention as the first item, and privacy concerns as the second item. It is not fully clear whether there is an effect on these respondents' logic, but we want to mention it as a concern and will improve it in future studies.

Regarding why only perceived benefit is significant for the moderating variables, our analysis suggests that because previous studies applied perceived risk, trust in platforms, and usage experience as independent variables affecting privacy disclosure intentions, the questionnaire items may not fit closely with our study. For example, Zhu *et al*. (2016) demonstrated that perceived risk and perceived benefit influenced privacy concerns and privacy disclosure intention, respectively. And the effect of perceived risk on privacy disclosure intention was not significant. Trust in the platforms is a mediating variable that influences privacy disclosure intention (Dinev & Hart 2006). This is the reason why H4, H5, and H6 were rejected. So the moderating effects of these three variables need to be further investigated to

confirm.

Although H8 and H9 were both valid, H7 was rejected and we argue that ‘privacy concerns’ and ‘attitudes’ in the TPB model are defined differently. ‘Attitude’ is a neutral term, whereas ‘privacy concerns’ have a negative impact. We will improve the questioning items in future studies.

On the practical side, Japan's QR code payment platforms are facing intense competition. Additionally, the entry of more than 15 platforms has blocked the market's user growth. Therefore, determining how to differentiate one's platform from other platforms while sustaining development requires paying close attention to user feedback and promptly improving service quality. This study shows that the implementation of cashback campaigns is not a long-term solution and that more innovative strategies are needed to integrate these payments more effectively into users' daily lives.

Meanwhile, it is important to remember the user's ability to control the disclosure of personal privacy. As most of the questionnaire respondents were concentrated between the ages of 20 and 59, they were essentially capable of independently using QR code payments. At the same time, living in the information age, they are more sensitive to personal privacy. Therefore, it does not take much time for them to learn how to update their skills with using these payments. For this reason, Japan's QR code payment service providers need to focus on their users' ability to control privacy disclosures. For example, creating a more user-friendly interface gives users greater freedom to choose which information they want to disclose. Another option is to provide users with a more secure service and teach them how to autonomously protect their privacy. While promoting these payments, many platforms have accidentally leaked users' personal information or hackers have stolen these platforms' users' personal information. We believe that these improvements require not only the effort of individual users, but also the attention of these platforms, thus strengthening protection measures intended to guard users' privacy.

In addition to the privacy concerns that are the main validation of this study, there are many reasons why cashless payments in Japan are below the global average. According to a survey conducted by the METI (2022), insistence on cash is one of the important reasons. In an aging society, many seniors do not have smartphones, let alone download QR code payment applications. What's more, there is very little counterfeit currency in Japan and ATMs are everywhere, so it is very easy to withdraw cash. Cash is therefore the most basic method of payment. However, as the impacts of COVID-19 continue to grow, avoiding contact while making payments has become a special attention in daily life. As a result, we believe that this may indirectly contribute to the development of QR code payments and change the “cash-based” mindset of the Japanese society.

This study is considered academically original as it is the first to link PCT and TPB to study Japan's mobile payment services. The literature on the privacy

paradox can become increasingly diverse by publishing empirical studies focusing on Japanese mobile payments. In addition, this study provides another perspective on the privacy paradox by using moderating variables as well as examining their relationship with privacy concerns and privacy disclosure intentions. In practical terms, it can also provide insights for how to develop Japan into a cashless society. That is, the existence of the privacy paradox is a double-edged sword. Reasonable analysis of its influencing factors can effectively contribute to Japan's development of QR code payments. On the contrary, if it significantly infringes on users' interests, it could decrease the popularity of these payments.

6.2 Limitations and Future Research

This study currently has two unresolved questions.

The first is the relationship between privacy concerns and privacy disclosure intentions. This study's conclusion is contrary to the research hypothesis, but we still believe it can prove the existence of the privacy paradox. However, this requires additional research to demonstrate whether survey group characteristics can influence the positive effect of privacy concerns on privacy disclosure intentions.

The second is related to the moderating variable. This study only focused on perceived benefit as a valid moderating variable, and it is worth exploring in future as to which other factors may be moderating variables. At the same time, we cannot rule out the possibility that the three proposed variables (perceived risk, trust in platforms, usage experience) may also become moderating variables. In future studies, we will further improve our questionnaire design in conjunction with other researchers' previous studies.

Acknowledgement

I would like to express my deepest gratitude to my supervisor, Associate Professor Juhyeok Jang, who gave me constant guidance and advice during the writing of this paper. I would also like to thank the reviewers for their valuable comments, which have made this manuscript more methodologically rigorous and sound. Any errors are mine.

References

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

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Process* 50(2): 179-211.

Ajzen, I. (2002). Constructing a TPB questionnaire: Conceptual and methodological considerations.

Brown, B. (2001). Studying the internet experience. Publishing Systems and Solutions Laboratory. *HP Laboratories Bristol*. HPL-2001-49.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination

of the online consumer's dilemma. I*nformation Technology and Management* 6(2-3): 181-202.

Conner, M., & Armitage, C. J. (1998). Extending the theory of planned behavior: A review and avenues for further research. *Journal of applied social psychology*, 28(15), 1429-1464.

Culnan, M. J, & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. I*NFORMS*.

Dada, A. (2021). Exploring The Influence of Electronic Word-Of-Mouth (eWOM) On Intention to Share-Wallet: A Study of UK Retail Banking Customer Using the Theory of Planned Behaviour (TPB) (*Doctoral dissertation, Cardiff Metropolitan University*).

De, Kerviler, G., Demoulin, N. T., & Zidda, P. (2016). Adoption of in-store mobile payment: Are perceived risk and convenience the only drivers?. *Journal of Retailing and Consumer Services*, 3*1*, 334-344.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce—a study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389-402.

Fan, A., Wu, Q., Yan, X., Lu, X., Ma, Y., & Xiao, X. (2021). Research on influencing factors of personal information disclosure intention of social media in China. *Data and Information Management*, 5(1), 195-207.

Han, M., Shen, S., Zhou, Y., Xu, Z., Miao, T., & Qi, J. (2019). An analysis of the cause of privacy paradox among SNS users: Take Chinese college students as an example. *In Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Hermes, S., Sutanrikulu, A., Schreieck, M., & Krcmar, H. (2021). Who Quits Privacy-Invasive Online Platform Operators? A Segmentation Study with Implications for the Privacy Paradox. In H*ICSS* (pp. 1-10).

Khalilzadeh, J., Ozturk, A. B., & Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior*, 7*0*, 460-474.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64, 122-134.

Lee, J. M., Lee, B., & Rha, J. Y. (2019). Determinants of mobile payment usage and the moderating effect of gender: Extending the UTAUT model with privacy risk. *International Journal of Electronic Commerce Studies*, *10*(1), 43-64.

Li, J. (2021). Factors influencing users' continuance intention towards travel-related Consumer Generated Media mobile application in China. *The Journal of International Media, Communication, and Tourism Studies*, No.33, 43-60.

Lutz, C., & Tamó-Larrieux, A. (2020). The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots. *Human-Machine Communication*, 1, 87-111.

Martin, K., & Shilton, K. (2016). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*, 67(8), 1871-1882.

Mikami, S. (2015). Self-disclosure in SNS and the Privacy Paradox. *Toyo UniversityRepository for Academic Resources*, 53(1), 65-77. (in Japanese).

Mikami, S. (2016). Revisiting the Privacy Paradox— Analysis of Factors Regulating the Degree of Self Disclosure in Social Networks. *The Bulletin of Faculty of Sociology, Toyo University*, 54(1), 69-81. (in Japanese).

Ministry of Economy, Trade and Industry. (2020). Current status and significance of cashless.1. (in Japanese).

NGUYEN, H. M., & KHOA, B. T. (2019). The relationship between the perceived mental benefits, online trust, and personal information disclosure in online shopping. *The Journal of Asian Finance, Economics, and Business*, 6(4), 261-270.

Oricon Customer Satisfaction(R) Survey. (2020, October). Survey on "Smartphone Payment

Service”Usage, Retrieved December 18, 2001, from https://cs.oricon.co.jp/michitari/article/217/. (in Japanese).

Sentosa, I., & Mat, N. K. N. (2012). Examining a theory of planned behavior (TPB) and technology acceptance model (TAM) in internet purchasing using structural equation modeling. R*esearchers World*, 3(2 Part 2), 62.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management*, 45, 44-55.

Shin, D. H. (2009). Towards an understanding of the consumer acceptance of mobile wallet. *Computers in Human Behavior*, 25(6), 1343-1354.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. M*IS quarterly*, 167-196.

Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating privacy and information disclosure behavior in social electronic commerce. *Sustainability*, 11(12), 3311.

Tabata, A. (2014). Privacy Awareness of Kwansei-Gakuin University Students: in regard of “Privacy Paradox”. *The Bulletin of Faculty of Sociology, Kwansei-Gakuin University*, (118), 89-101. (in Japanese).

Taddicken, M. (2014). The ‘privacy paradox’ in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of computer-mediated communication*, 19(2), 248-273.

Tatsuya, N., Takuya N., & Hiroki I. (2011). Measurement of Internet Anxiety an Investigation of Its Relationships with Self-Efficacy. *Information Processing Society of Japan SIG Technical Report*, (11): 1-6.

Toyota, H. (2007). Covariance Structure Analysis [Amos]—Structural Equation Modeling. Tokyo: TokyoTosho Co.,Ltd. (in Japanese).

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. J*ournal of the Association for Information Systems*, 7(6), 16.

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems*, 51(1), 42-52.

Zhang, J., Luximon, Y., & Song, Y. (2019). The role of consumers' perceived security, perceived control, interface design features, and conscientiousness in continuous use of mobile payment services. *Sustainability*, 11(23), 6843.

Zhu, H., Wang, K., Yan, ZJ., & Wu, J. (2017). An Analysis of Privacy Paradox Phenomenon in SNS Users Based on Privacy Calculus. *Journal of Intelligence*, 36(2): 134-139+121. (in Chinese).

（令和4年5月2日受理、令和4年9月20日採択）