The Privacy Trap of Digital Transformation: The Existence and the Implication

Cho-Hsun Lu[1*], Yen-Hung Chen[2], Pi-Tzong Jan[1]
[1] Department of Applied Informatics, Fo Guang University
[2] Department of Information Management, National Taipei University of Nursing and Health Sciences
chlu@mail.fgu.edu.tw, pplong@gmail.com, ptjan@mail.fgu.edu.tw

Abstract

This study explores why a developing country may fall into the privacy trap of digital transformation after Covid-19. The privacy trap is that, when the developing country executes its digital transformation policy, the government inevitably compromises their civilian privacy and often have no way of knowing when/why/how the service will use or leak the privacy. To date, little scholarly literature has examined the existence and implication of the privacy trap in a developing country. Therefore, we analyze data from 306 respondents in Taiwan based on descriptive and inferential statistics. The results show the privacy trap exists and may be derived by that the bandwagon effect overriding the effects of privacy concerns on the willingness to provide personal information. These findings implicate that, based on the in-depth expert interview, one possible way but also the biggest challenge to escaping the privacy trap is to transform from the current economic system of cost-oriented labor to the economic system of a risk-oriented education system supporting breakthroughs in science and technology. This study could ultimately contribute to the developing countries to protect their civilian's privacy when executing digital transformation especially from a digital minority to a digital beneficiary.

Keywords: Digital transformation, Privacy trap, Bandwagon effect, Taiwan, Post-pandemic era

1 Introduction

Digital technology was a tediously long process of changing our lifestyle and improving our society because of the inherent support, operation, and training procedure are restricted to physical building and paper works for years. Unfortunately, since 2020, the Covid-19 crisis inhibits people from doing things in a conventional way. On the business level, people imperatively need to work from home (WFH) and hold a meeting remotely to curb cluster infection, and, on the societal level, people also need to shop online and make payment via mobile phone, instead of cash or credit card, to avoid contact infection. The COVID-19 crisis speeds up the adoption of digital technologies by just one year to bring about decades of the progress our business and social sector plan to do [1]. Suddenly, the digital transformation is not an academic theory but is becoming exigent demand of policy execution in the post-pandemic era.

The digital transformation (DT), unlike digitization of converting information into a digital format, is a fundamental change process of an entity (organization, industry, or society), enabled by digital technologies, accompanied by the strategic leverage of key resources and capabilities, aiming to radically to improve or refine the value proposition of an existing digitalized information for its stakeholders [2]. Notably, the improved and refined value of the digitalized information is shaped by technology itself with scarcely or even without human intervention. For example, Alipay, a Chinese third-party payment platform, applies cryptocurrency, blockchain, artificial intelligence to shape a digital ecosystem that provides civilian a gate way to access resources online including check their social insurance, pay for electricity, search for public transport, and so on, which completely reinventing China's retail sector [2].

The digital transformation process, however, had been inevitably a challenge and required years to force people dramatically and rapidly to be adopted. But Covid-19 enables the government to push its civilian a giant step forward of digital transformation in the name of pandemic-prevention policies. For example, when entering the physical building, e.g., shopping mall, office, school, we must comply with the name registration guides to provide our privacy to the government and retailers via mobile Apps for contact tracing and entry permission; or when shopping online or offline, we have to make digital payment without cash to avoid contact infection. The civilian is therefore forced to download the apps and registration their privacy (or called personal identity information, PII), e.g., name, phone number, email address, identity number. The civilian may have doubts about the speculative behavior of the APP which causes privacy risks since the App developer or the service provider does not have sufficient proficiency in information security and privacy protection [3-4].

Almost every service and application developed during the digital transformation processes civilian's privacy [5]. Privacy Protection becomes a societal need and requires immediate regulation to ensure all organizations complying with the requirements and generate documentary evidence of how it handles the processing of privacy. On the other hand, the government also need to educate civilian to have privacy protection awareness and skill. But these security measures require time and resources. This forced the government to fall into the privacy trap (or called privacy paradox) [6]: both the privacy owner and privacy processor claim to be very concerned about privacy but know very little to protect the privacy within a limited time with scarce resource under the premise of exigent pandemic-prevention policies. This

*Corresponding Author: Cho-Hsun Lu; E-mail: chlu@mail.fgu.edu.tw
DOI: 10.53106/160792642022012301006

phenomenon is involved the information assurance issues that the government has to consider the pros and cons of information security technology and to avoid various information governance problems caused by traditional priority considerations of information technology security [35].

Despite the robust theoretical literature, to the best of our knowledge, to date, there is surprisingly no empirical discussion on how the privacy trap functions in the post-pandemic era, especially for the developing country. To be more specific, the previous studies of privacy trap are merely focused on the behavior towards privacy-protection attitude and privacy-protection action which eventually results in a dichotomy between compromising or uncompromising with their privacy [6-7]. These studies do not explore the reaction of the people and consequent compensation action for the people, when they have no choice but to be forced to compromise with their privacy to face the Covid-19 and follow the instruction of pandemic-prevention policies.

This study, therefore, contributes to the literature on digital transformation and information development by providing a model for analyzing the presence of privacy trap in the post-pandemic era, and in what form privacy trap exists using the common data of the Mobile App market in Taiwan as a case study. The research result could ultimately help the developing countries to protect their civilian's privacy when executing digital transformation especially from a digital minority to a digital beneficiary.

2 Theoretical Background and Hypotheses

2.1 Theoretical background

The proposed model to explore the privacy trap issues is based on Elaboration Likelihood Model (ELM) [8]. This research uses the ELM concept of the central route and the peripheral route to infer that the privacy trap is attributable to the individual's willingness to disclose privacy. The privacy calculus [9] is set as the central route, and the bandwagon effect [10-11] as the peripheral route of this research.

The ELM attempts to describe the user's attitude to accept external information and to interpret the information is based on personal subjective knowledge and experience. ELM explains that the user applies "Central Route" and "Peripheral Route" to process information. In this study, once the individual decides to make a decision based on his own ability and personal willingness to disclose his/her privacy, he/she applies the central route. Otherwise, if an individual does not have sufficient ability or unwillingness to make judgments about privacy disclosure decisions, he/she prefers to adopt a peripheral route.

The privacy calculus assumes that the individual is completely rational and has sufficient ability to determine the value of personal privacy information and assess the risk of privacy being exposed [6]. Dinev and Hart [9] believe that users are willing to disclose personal information on the Internet because they have evaluated and had confidence regarding the seller's or retailer's protection policies. The factors of "Perceived privacy risks of App", "Perceived benefits from App", and "information privacy concerns" are applied to represent the privacy calculus.

The bandwagon effect means people to adopt certain behaviors or attitudes simply because others are doing so [10-11]. The factors of "fear of isolation" and "perceived APPs reputation" are adopt to represent the bandwagon effect. "Fear of isolation" means public opinion or groups disagree with an individual's opinion on the topic matter, leading that the individual's silence and then to motivate individual to ascertain what the public thinks [10]. For example, the consumers usually cannot acquire sufficient information from online/mobile service providers [12-14], and they are hard to confirm whether providers have sufficient capabilities, goodwill, and predictability [12-14]. Once the consumers are unable or unwilling to make decision on personal information disclosure, they will act as if they belong to a majority and conformity with the perceived dominant opinion [8-10]. "Reputation" means the beliefs or opinions that others are held about the mobile service or Apps [7].

2.2 Research Model Constructs and Hypotheses

The research model and hypotheses based on the above discussion are summarized in Figure 1 and Table 1. The definition of each aspect of the research structure, the number of items, and the main references of each research aspect are shown in Table 2. The details are as follows.

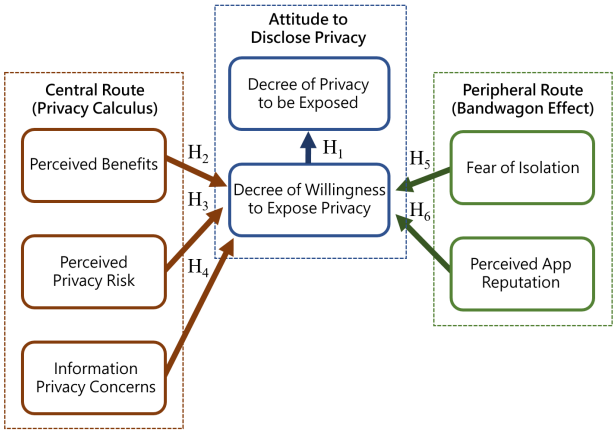


Figure 1. Research framework

Table 1. Hypotheses

Description
H1. Civilian's Decree of Willingness to Expose Privacy positively affects the Decree of Willingness to Expose Privacy
H2. Civilian's Perceived Benefits from Apps positively affects the Decree of Willingness to Expose Privacy
H3. Civilian's Perceived Privacy Risk of Apps negatively affects the Decree of Willingness to Expose Privacy
H4. Civilian's Information Privacy Concerns negatively affects the Decree of Willingness to Expose Privacy
H5. Civilian's Fear of Isolation positively affects the Privacy Attitude
H6. Civilian's Perceived App Reputation positively affects the Privacy Attitude

Table 2. Constructs in the research framework model

Construct Category	Acronym	Questionnaire Items	References
Decree of Privacy to be Exposed	DPE	3	Dinev & Hart[9]
Decree of Willingness to Expose Privacy	DWE	6	Dienlin & Trepte[15]
Perceived Benefits	PB	4	Kim[16]
Perceived Privacy Risk	PPR	5	Dinev & Hart[9]
Information Privacy Concerns	IPC	4	Smith et al.[17]; Malhotra et al.[18]
Fear of Isolation	FOI	3	Shim & Oh (2018)
Perceived App Reputation	PAR	3	Gu et al.[7]

Regarding the privacy trap, the civilians may be worried about the leakage of information privacy, but they do not always choose to not disclose personal information. This phenomenon is measured in this study by "the attitude to disclose privacy." This study furthermore divides "the attitude to disclose privacy" into "decree of willingness to expose privacy" and "the decree of privacy to be exposed". The reasons are based on the practice of Dienlin and Trepte [15] that the attitude, whether positive or negative, is a two-fold variable: one is the intention to expose the attitude and the latter is only the degree to which the civilian is willing to disclose private information in the context of downloading the mobile app [9]. Therefore, the first hypothesis is:

H1. Civilian's Decree of Willingness to Expose Privacy positively affects the Decree of Willingness to Expose Privacy

This study defines the "Perceived Benefits from Apps" as "the user's subjective perception of the positive value expected to be brought by the mobile app downloaded by the digital distribution platform" [19]. The factor to accept information systems based on Davis's [20] technology acceptance model is using technology can improve working efficiency. In Moore and Benbasat's [21] innovation diffusion theory, they also use Relative Advantage to describe whether civilians consider whether to use innovative technology, mainly because the use of this technology can bring benefits that are better than previous technologies. Kim et al. [22] conducted a study on civilian's acceptance of e-commerce services and believed that civilians tried to maximize benefits and minimize risks, and after the benefits and risks were subtracted, they expected to maximize the positive benefits to determine whether accepts the use of e-commerce services. Therefore, based on privacy calculations, whether civilians have a positive or negative attitude towards the need to disclose private information when downloading mobile apps from digital distribution platforms, the benefit of using apps is an important consideration on the Decree of Willingness to Expose Privacy:

H2. Civilian's Perceived Benefits from Apps positively affects the Decree of Willingness to Expose Privacy

This study defines perceived risk as "the civilian's subjective perception of the uncertainty and possible negative effects felt by the mobile app downloaded by the digital publishing platform". In addition to the possible benefits of using new APP [23], the possible negative effect also affects civilian acceptance [3-4, 24-26]. Civilians may not be able to directly face-to-face evaluate the seller and experience services on the spot in mobile or online service, and they then confront privacy leaking issues due to possibility of insufficient profession or speculative behaviors of service provider [14]. Therefore, the acceptance of mobile applications and mobile commerce is affected by consumer perceived risk [16, 22, 27].

H3. Civilian's Perceived Privacy Risk of Apps negatively affects the Decree of Willingness to Expose Privacy

The conventional scholars constructed various concepts of information privacy concerns including collection, data error, unauthorized secondary use, and inappropriate access [17]. However, unlike the conventional privacy risk of "inappropriate access", Pavlou et al. [14] used Principal-Agent Relationships to explore the uncertainty of e-commerce transactions. They believe there exists "unknown unknowns" risks that come from situations that are so unexpected that they would not be considered. The unknown unknowns are derived by the nature of the unknown relative to past experience, and they may be a detriment to the facility and endanger public health and safety. Therefore, information privacy concerns mean that civilians may not be able to predict whether service providers are capable and willing to protect their personal and transaction information when facing uncertain situation, e.g., pandemic issues and following political policies, and believe that downloading mobile apps from digital distribution platforms may bring negative benefits [28].

H4. Civilian's Information Privacy Concerns negatively affects the Decree of Willingness to Expose Privacy

When civilians use online or mobile services, they may take a suspicious attitude [27, 29] but fear isolation. They face information asymmetry to confirm whether the service provider or government has sufficient ability, goodwill, and predictability of behavior [12-14]. Zhou et al. [8] believed that if civilians did not have the ability and willingness to judge that mobile services are trustworthy, they will observe the majority of other civilians and follows their behavior pattern in light of the fear of isolation. Therefore, the fear of isolation has a positive influence on the attitude of privacy and belongs to the variable of the peripheral route [10].

H5. Civilian's Fear of Isolation positively affects the Decree of Willingness to Expose Privacy

Since most civilians use the mobile app privacy protection information regulated by the platform and government, they will give mobile app publishers a considerable degree of trust, if they do not have the ability and willingness to judge that mobile services are trustworthy. They, therefore, have a positive attitude towards providing private information to download mobile apps from digital distribution platforms [25, 30], and belongs to variables of the peripheral route:

H6. Civilian's Perceived App Reputation positively affects the Decree of Willingness to Expose Privacy

Table 3. Confirmatory factor analysis statistics

Constructs	Questionnaire Items Acronym	Mean	Std Deviation	Std. Loading	CR	Cronbach's α	AVE
PPR	PPR1	4.63	1.317	0.765	0.900	0.898	0.643
	PPR2	4.11	1.302	0.755			
	PPR3	4.45	1.262	0.886			
	PPR4	4.55	1.201	0.806			
	PPR5	4.34	1.274	0.792			
PB	PB1	4.55	1.203	0.698	0.855	0.855	0.597
	PB2	4.61	1.216	0.801			
	PB3	4.54	1.139	0.788			
	PB4	4.80	1.173	0.798			
IPC	IPC1	4.67	1.254	0.714	0.901	0.897	0.697
	IPC2	5.09	1.318	0.815			
	IPC3	4.92	1.254	0.942			
	IPC4	4.88	1.264	0.853			
FOI	FOI1	4.16	1.134	0.846	0.889	0.886	0.729
	FOI2	3.98	1.11	0.905			
	FOI3	4.03	1.083	0.807			
FAR	FAR1	4.30	1.321	0.822	0.891	0.883	0.732
	FAR2	4.47	1.263	0.944			
	FAR3	4.59	1.283	0.793			
DWE	DWE1	4.09	1.142	0.643	0.864	0.849	0.563
	DWE2	3.75	1.226	0.824			
	DWE3	3.73	1.137	0.823			
	DWE4	4.00	1.176	0.593			
	DWE5	4.04	1.105	0.834			
DPE	DPE1	3.99	1.154	0.884	0.872	0.891	0.632
	DPE2	3.94	1.212	0.838			
	DPE3	3.51	1.343	0.729			
	DPE4	3.45	1.367	0.717			

Table 4. Latent variable statistics

	PPR	PB	IPC	FOI	FAR	DWE	DPE
PPR	**0.802**						
PB	0.351	**0.773**					
IPC	0.724	0.514	**0.835**				
FOI	-0.127	0.487	-0.057	**0.854**			
FAR	0.013	0.452	0.093	0.405	**0.856**		
DWE	-0.215	0.209	-0.283	0.610	0.356	**0.750**	
DPE	-0.141	0.302	-0.166	0.642	0.322	0.800	**0.795**

3 Data Collection and Analysis

This study is conducted via a cross-sectional survey research design, and data are randomly collected from the Mobile App market in Taiwan as a case study. A random sample determination formula described in the literature of De Vaus [31] and Cochran [32].

sampling strategy was employed, and field experts were invited for interviews using the list obtained from the Office of Science and Technology (OST), a task force of the R.O.C. Executive House in Taiwan. The questionnaires were made through questionnaire, interview, and telephone, using the

The data collected in this research uses statistical software IBM SPSS AMOS version 23.0 as the analysis tool, which

evaluates the reliability, internal consistency, content validity, convergent validity and discriminant validity of the questionnaire. The results are shown in Table 3, 4, and 5 and the detailed explanation is as follows:

In terms of reliability, composite reliability (CR) is used for evaluation and the CR value of all latent variables ranges from 0.855 to 0.901, which is greater than the 0.7 threshold recommended by Bagozzi and Yi [33]. This shows the potential variables meet the reliability requirements. This study also used Cronbach's α value to measure the internal consistency of the scale items in the survey questionnaire. The Cronbach's α value in this study ranges from 0.849 to 0.898 and is greater than 0.7, which has high reliability.

This study also evaluates the content validity, convergent validity, and discriminant validity. Content validity mainly evaluates whether the question items used to measure a concept are sufficient to measure the concept [34]. This research first explores the complete literature to find out 30 measurement questions that are related to the concept of this research. It then invites field experts to verify and revised the question items including sentence suitability, sentence fluency, item length, etc., to ensure that the question items have sufficient content validity.

The convergence validity refers to the degree of conformity of the same construct as measured by multiple variables [34]. The criteria for judging whether the measurement item has sufficient convergence validity are (1) the standardization of the measurement item Factor Loadings value is greater than zero, (2) the Composite Reliability (CR) value is greater than 0.7, and (3) the Average Variance Extracted (AVE) is greater than 0.5. The collected data as shown in Table 3 that the standard load of all items is greater than 0.5; the CR values of all latent variables and constructs are greater than 0.7, and the average extraction variation is all greater than 0.5. Therefore, the question items have sufficient convergence validity.

Difference validity is mainly used to confirm that each aspect of the questionnaire is different. This study applies the average variant extraction (AVE) method. Fornell and Larcker [35] believe that the research aspect has sufficient discriminative validity when the AVE value is greater than the square value of the correlation coefficient (Correlation Estimate) between other aspects. As shown in Table 4, the data collected in this study satisfies these criteria and indicates that the aspect of this research should have sufficient discriminative validity.

4 Result and Discussion

Of the 3,000 questionnaires, 306 responses were valid questionnaires, which represent a useable response rate 10.2%. As shown in Table 5, the respondents are mainly aged from 20 to 29 years old (61.4% in total), and the gender is mostly female (66%). As the average income of this study is mainly fresh graduate or the most are hourly worker (56.2%). Among them, in terms of the survey participants' use of mobile apps, most civilians use mobile apps for an average of about 3 to 6 hours per day (37.3%), and the frequency of downloading mobile apps is mostly at least once a month (31.7%). Smartphones mainly use mobile commerce (301 times), and the top three types of mobile commerce mainly used include "social and communication (239 times)", "games and entertainment (205 times)", "shopping and consumption (200 times)".

Based on the responses from questionnaires, six hypotheses are tested to observe the path coefficients between external modes in terms of the directionality, strength, and significance, as shown in Figure 2 and Table 6.

First, the hypothesis H1, the civilian's decree of willingness to expose privacy positively affects the decree of willingness to expose privacy, is significant. This means that once the civilian is inclined to expose privacy, they intend to expose the degree of privacy they are asked to expose. Therefore, the key of privacy trap should focus on what factor evokes the willingness to expose privacy.

Second, regarding the central route of privacy calculus (H2, H3 and H4), only H4 has a significant testing result. This means the civilians mainly concern about the "unknown unknowns" privacy leak risks that come from situations that are so unexpected. They also admit that they are able to predict whether service providers are capable and willing to protect their personal and transaction information, so the perceived benefits and risks do not significantly affect the willingness of the civilians to expose privacy, based on the testing results of H3 and H4. These further imply that the privacy trap exists that the civilians claim to be very concerned about privacy, based on the testing result of H2, but know very little to protect the privacy, based on the testing result of H3 and H4.

Third, and finally, the peripheral route of bandwagon effect (H5 and H6) has the significant testing result, and the Fear of Isolation (H5) has sufficient positive effect (0.5699) on the Decree of Willingness to Expose Privacy than the negative effect of Information Privacy Concerns (-0.362). The results show the privacy trap may be derived by that the bandwagon effect overriding the effects of privacy concerns on the willingness to provide personal information.

This study also evaluates the effects of different ages and gender on the willingness to expose privacy. Table 7 shows that the civilian over thirty years old perceives privacy risk of apps and therefore has significantly negative effects on the willingness to expose privacy than the civilian below thirty years old. This might indicate that the more sufficient social experience the civilians have, the more concerns about the risks to expose their privacy. On the other hand, the female civilians are more sensitive in the perceived benefits and risk of apps on the willingness to expose privacy than males, based on the Gender testing results of H2, H3, and H4.

This study furthermore explores the effects of different incomes and mobile apps download frequency on the willingness to expose privacy. The left-hand side columns of Table 8 shows that the civilians with low income are more willing to expose their privacy if they perceive the benefit of APP, compared to the civilians with higher incomes. Furthermore, the bandwagon effects play a significant role to stir up low-income civilians to expose their privacy, compared to the higher-income civilian. The right-hand side columns of Table 6 demonstrates that the civilian the download mobile APPs several times per day are more sensitive in the perceived benefits, risk, reputation of apps on the willingness to expose privacy than male, based on the download frequency testing results of H2, H3, and H6.

As the results discussed above, we conclude that:

(1) The privacy trap likely exists based on the observation that the civilian claim to be very

concerned about privacy (H4, H5, H6 are significant) but know very little to protect the privacy within a limited time with scarce resource under the premise of exigent pandemic-prevention policies (H2 and H3 are not significant).

(2) The privacy trap may be derived by that the bandwagon effect based on the observation that H5 and H6 are significant.

(3) The female civilians are more sensitive in the perceived benefits and risk of apps on the willingness to expose privacy.

(4) The civilians with lower-income or insufficient social experience expose their privacy mainly due to the bandwagon based on the testing results of Table 7 and 8.

Table 5. Demographic profile for respondents (n=306)

Variables	Attribution	Frequency	Percentage (%)
Gender	Female	202	66
	Male	104	34
Age	≤ 19 years	26	8.5
	20 - 29 Years	188	61.4
	30 - 39 Years	56	18.4
	40 - 49 Years	21	6.9
	50 - 59 Years	14	4.5
	≥ 60 Years	1	0.3
Average Income Per Month (in NT Dollars)	No Income	172	56.2
	≤ 20,000	61	19.9
	20,001 - 40,000	42	13.7
	40,001 - 70,000	17	5.6
	70,001 - 100,000	12	3.9
	≥ 100,000	2	0.7
Average Income Per Month (in NT Dollars)	No Income	172	56.2
	≤ 20,000	61	19.9
	20,001 - 40,000	42	13.7
	40,001 - 70,000	17	5.6
	70,001 - 100,000	12	3.9
	≥ 100,000	2	0.7
Usage Time in Mobile Devices Per Day	≤ 1 Hour	32	10.5
	1 – 3 Hours	87	28.4
	3 – 6 Hours	114	37.3
	≥ 6 Hours	73	23.8
Download Mobile Apps Frequency	Once Per Day	24	7.8
	Several Times Per Day	48	15.7
	Several Times Time Per Week	55	18
	One Time Per Month	82	26.8
	Several Times Per Month	97	31.7
User M-Commerce Access Mobile Devices (Multiple Choices)	Tablet Computer (e.g. Apple iPad)	40	13.1
	Smartphone (e.g. iPhone or Android)	301	98.4
* respondents may have one or more devices	Smartwatch (e.g. Apple Watch)	16	5.2
M-Commerce Services (Multiple Choices)	Social Media and Networking	239	78.1
	Shopping	200	65.4
	Personal Financial Services	70	22.9
	Game and Entertainment	205	67.0
	Travel and Traffic	111	36.3
	Health and Sport	53	17.3
* respondents may use multiple services	Education	105	34.3
	Productivity and Business	34	11.1
	News	93	30.4
	Lifestyle	73	23.9

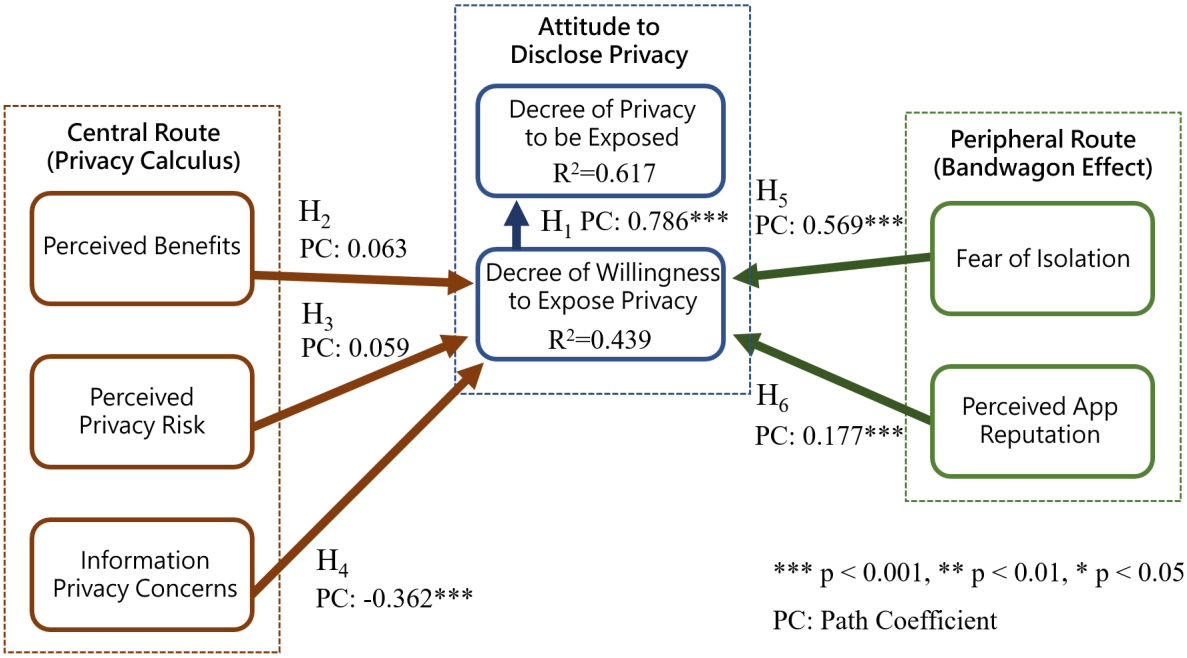


Figure 2. SEM completely standardized path coefficients

Table 6. Result of hypothesis testing

Description	**Result**
H1. Civilian's Decree of Willingness to Expose Privacy positively affects the Decree of Privacy to be Exposed	Significant
H2. Civilian's Perceived Benefits from Apps positively affects the Decree of Willingness to Expose Privacy	Not Significant
H3. Civilian's Perceived Privacy Risk of Apps negatively affects the Decree of Willingness to Expose Privacy	Not Significant
H4. Civilian's Information Privacy Concerns negatively affects the Decree of Willingness to Expose Privacy	Significant
H5. Civilian's Fear of Isolation positively affects the Decree of Willingness to Expose Privacy	Significant
H6. Civilian's Perceived App Reputation positively affects the Decree of Willingness to Expose Privacy	Significant

Table 7. Result of hypothesis testing of different ages and genders

	Age		Gender	
Hypothesis	<30	30<	Female	Male
H1	1.003***	0.884***	1.329***	0.629***
H2	0.093	0.085	0.098*	0.013
H3	0.002	0.236**	0.088*	0.015
H4	-0.229***	-0.757***	-0.302***	-0.253**
H5	0.372***	0.402**	0.416***	0.417***
H6	0.118**	0.173*	0.059**	0.221**
*** p < 0.001, ** p < 0.01, * p < 0.05				

Table 8. Result of hypothesis testing of different incomes and download frequency

	Income			Download Frequency		
Hypothesis	<1000 USD	1,000USD~ 2,000USD	2,000USD<	Several Times Per Day	Several Times Time Per Week	Several Times Per Month
H1	1.017***	0.627**	0.925***	1.121***	0.991***	0.756***
H2	0.140**	0.061	-0.226	-0.112*	0.129	0.037
H3	0.014	-0.032	0.289	0.195***	-0.109	0.046
H4	-0.271***	-0.648**	-0.573**	-0.241***	-0.322***	-0.256**
H5	0.370***	0.213	0.583	0.641***	0.262***	0.413***
H6	0.123**	0.117	0.189	0.190***	0.107	0.066
*** p < 0.001, ** p < 0.01, * p < 0.05						

5. Conclusion

This study analyzes the presence of privacy trap in the post-pandemic era, and in what form privacy trap exists using the common data of the Mobile App market in Taiwan as a case study.

The findings show the privacy trap in the post-pandemic era may be derived by that the bandwagon effect. The result also indicates that the female civilians are more sensitive in the perceived benefits and risk of apps on the willingness to expose privacy; the civilians with lower-income or insufficient social experience expose their privacy mainly due to the bandwagon. The civilian furthermore admits that they are unable to evaluate whether service providers are capable and willing to protect their personal and transaction information, leading that they mainly concern about the "unknown unknowns" privacy leak risks.

The finging implication implicates that, based on the in-depth expert interview, one possible way but also the biggest challenge to escaping the privacy trap is to transform from the current economic system of cost-oriented labor to the economic system of a risk-oriented education system supporting breakthroughs in science and technology, especially for the population of insufficient working experience, male, low-income, and high download frequency of Mobile Apps.

The contribution of the research result could ultimately help the developing countries to protect their civilian's privacy when executing digital transformation especially from a digital minority to a digital beneficiary.

The limitation of this study is that the finding and implication may imply only in developing country, since the proposed hypothesis model is tested according to the data collected in Taiwan.

Acknowledgments

The authors would like to thank the Ministry of Science and Technology of the R.O.C., for financially supporting this research under Contract No. MOST 110-2221-E-227-001 - and Tzu-Chi University of Science and Technology under Contract No. TCCT-1071A03.

References

[1] M. Deja, D. Rak, B. Bell, Digital Transformation Readiness: Perspectives on Academia and Library Outcomes in Information Literacy, *The Journal of Academic Librarianship*, Vol. 47, No. 5, pp. 102403, September, 2021.

[2] C. Gong, V. Ribiere, Developing a Unified Definition of Digital Transformation, *Technovation*, Vol. 102, pp. 102217, April, 2021.

[3] S. Glover, I. Benbasat, A Comprehensive Model of Perceived Risk of E-Commerce Transactions, *International Journal of Electronic Commerce*, Vol. 15, No. 2, pp. 47-78, Winter, 2010-2011.

[4] P. A. Pavlou, Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, *International Journal of Electronic Commerce*, Vol. 7, No. 3, pp. 101-134, Spring, 2003.

[5] ISO/IEC, *Security Techniques — Extension to Iso/Iec 27001 and Iso/Iec 27002 for Privacy Information Management — Requirements and Guidelines (Iso/Iec 27701:2019)*, August, 2019.

[6] S. Barth, M. D. T. de Jong, The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – a Systematic Literature Review, *Telematics and Informatics*, Vol. 34, No. 7, pp. 1038-1058, November, 2017.

[7] J. Gu, Y. Xu, H. Xu, C. Zhang, H. Ling, Privacy Concerns for Mobile App Download: An Elaboration Likelihood Model Perspective, *Decision Support Systems*, Vol. 94, pp. 19-28, February, 2017.

[8] T. Zhou, Understanding Users' Initial Trust in Mobile Banking: An Elaboration Likelihood Perspective, *Computers in Human Behavior*, Vol. 28, No. 4, pp. 1518-1525, July, 2012.

[9] T. Dinev, P. Hart, An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research*, Vol. 17, No. 1, pp. 61-80, March, 2006.

[10] K. Shim , S.-K. Oh, Who Creates the Bandwagon? The Dynamics of Fear of Isolation, Opinion Congruency and Anonymity-Preference on Social Media in The 2017 South Korean Presidential Election, *Computers in Human Behavior*, Vol. 86, pp. 181-189, September, 2018.

[11] T. F. Waddell , S. S. Sundar, Bandwagon Effects in Social Television: How Audience Metrics Related to Size and Opinion Affect the Enjoyment of Digital Media, *Computers in Human Behavior*, Vol. 107, pp. 106270, June, 2020.

[12] D. H. McKnight, V. Choudhury, C. Kacmar, The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model, *Journal of Strategic Information Systems*, Vol. 11, No. 3-4, pp. 297-323, December, 2002.

[13] D. H. McKnight, V. Choudhury, C. Kacmar, Developing and Validating Trust Measures for E-Commerce: An Integrative Typology, *Information Systems Research*, Vol. 13, No. 3, pp. 334-359, September, 2002.

[14] P. A. Pavlou, H. Liang, Y. Xue, Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective, *MIS Quarterly*, Vol. 31, No. 1, pp. 105-136, March, 2007.

[15] T. Dienlin, S. Trepte, Is the Privacy Paradox a Relic of the Past? An in-Depth Analysis of Privacy Attitudes and Privacy Behaviors, *European Journal of Social Psychology*, Vol. 45, No. 3, pp. 285-297, April, 2015.

[16] D. J. Kim, D. L. Ferrin, H. R. Rao, A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents, *Decision Support Systems*, Vol. 44, No. 2, pp. 544-564, January, 2008.

[17] H. J. Smith, S. J. Milberg, S. J. Burke, Information Privacy: Measuring Individuals' Concerns About Organizational Practices, *MIS Quarterly*, Vol. 20, No. 2, pp. 167-196, June, 1996.

[18] N. K. Malhotra, S. S. Kim, J. Agarwal, Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model, *Information Systems*

Research, Vol. 15, No. 4, pp. 336-355, December, 2004.

[19] T. Zhou, The Impact of Privacy Concern on User Adoption of Location-Based Services, *Industrial Management & Data Systems*, Vol. 111, No. 2, pp. 212-226, March, 2011.

[20] F. D. Davis, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly*, Vol. 13, No. 3, pp. 319-340, September, 1989.

[21] G. C. Moore, I. Benbasat, Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation, *Information Systems Research*, Vol. 2, No. 3, pp. 222, September, 1991.

[22] G. Kim, B. Shin, H. G. Lee, Understanding Dynamics between Initial Trust and Usage Intentions of Mobile Banking, *Information Systems Journal*, Vol. 19, No. 3, pp. 283-311, May, 2009.

[23] T. Laukkanen, Internet Vs Mobile Banking: Comparing Customer Value Perceptions, *Business Process Management Journal*, Vol. 13, No. 6, pp. 788-797, November, 2007. ABI/INFORM Global.

[24] J. C. Sweeney, G. N. Soutar, L. W. Johnson, The Role of Perceived Risk in the Quality-Value Relationship: A Study in a Retail Environment, *Journal of Retailing*, Vol. 75, No. 1, pp. 77-105, Spring, 1999.

[25] X. Luo, H. Li, J. Zhang, J. P. Shim, Examining Multi-Dimensional Trust and Multi-Faceted Risk in Initial Acceptance of Emerging Technologies: An Empirical Study of Mobile Banking Services, *Decision Support Systems*, Vol. 49, No. 2, pp. 222-234, May, 2010.

[26] I. Im, Y. Kim, H.-J. Han, The Effects of Perceived Risk and Technology Type on Users' Acceptance of Technologies, *Information & Management*, Vol. 45, No. 1, pp. 1-9, January, 2008.

[27] K. Siau , Z. Shen, Building Customer Trust in Mobile Commerce, *Communications of the ACM*, Vol. 46, No. 4, pp. 91-94, April, 2003.

[28] G. Bansal, F. M. Zahedi, D. Gefen, Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online, I*nformation & Management*, Vol. 53, No. 1, pp. 1-21, January, 2016.

[29] Y. S. Yeh, Y.-M. Li, Building Trust in M-Commerce: Contributions from Quality and Satisfaction, *Online Information Review*, Vol. 33, No. 6, pp. 1066-1086, November, 2009.

[30] H. Amin, T. Ramayah, Sms Banking: Explaining the Effects of Attitude, Social Norms and Perceived Security and Privacy, *The Electronic Journal of Information Systems in Developing Countries*, Vol. 41, No. 1, pp. 1-15, May, 2010.

[31] D. De Vaus, *Surveys in Social Research*, Allen & Unwin Academic Publisher, 2013.

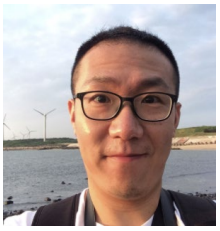
[32] W. G. Cochran, *Sampling Techniques*, John Wiley & Sons, 1977.

[33] R. P. Bagozzi, Y. Yi, On the Evaluation of Structural Equation Models, *Journal of the Academy of Marketing Science*, Vol. 16, No. 1, pp. 74-94, March, 1988.

[34] J. F. J. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling*, Thousand Oaks: Sage, 2014.

[35] C. Fornell, D. Larcker, Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research*, Vol. 18, No. 3, pp. 382-388, August, 1981.

Biographies



Cho-Hsun Lu, Assistant Professor, Department of Applied Informatics, Fo Guang University, Taiwan. Research focus: e-Commerce, Mobile Commerce, Healthcare Information Management, AR/VR Application Development.

Yen-Hung Chen, Associate Professor, Department of Information Management, National Taipei University of Nursing and Health Sciences, Taiwan. Research focus: National policy making, Business stragies planning and evaluation, Networking protocal design and efficiency estimation.

Pi-Tzong Jan, Professor, Department of Applied Informatics, Fo Guang University, Taiwan. Research focus: e-Commernce theory and practice, Digital divide, Digital convergence.