Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps

Cong Duc Tran, Tin Trung Nguyen *

Faculty of Business Administration, Ton Duc Thang University, 19 Nguyen Huu Tho Street, Tan Phong Ward, District 7, Ho Chi Minh City, Viet Nam

ARTICLE INFO

Keywords:
Health risk
Privacy risk
Risk-risk tradeoff
Contact-tracing app
COVID-19
fsQCA

ABSTRACT

In the midst of the COVID-19 pandemic, contact-tracing apps have emerged as reliable tools for public health communication and the promotion of preventative health. However, to function properly, contact-tracing apps require users to provide sensitive information, which has raised concerns about data disclosure, misuse and social surveillance. Little is known about how different types of risk perception simultaneously hinder and motivate individuals' engagement in mobile health apps, particularly in the context of a pandemic. Based on the privacy calculus theory and the risk-risk tradeoff concept, this study examined the risk-risk tradeoff model to enhance the understanding of COVID-19 contact-tracing app users' decision from the perspective of risk minimization. Findings from PLS-SEM and fsQCA revealed that users engage in health risk-privacy risk tradeoff when evaluating and deciding to use the apps. The focal study therefore contributes to the research on privacy calculus theory and calls for a balanced managerial solution to mitigate this tradeoff dilemma.

1. Introduction

Mobile health applications (mHealth apps) are powerful tools for users to keep track of their health such as consumed calories, vital signs and exercise exertions with real-time recording parameters [1]. Recent years have also seen a growth in both the quality and quantity of mHealth apps, which has extended the capability of effective health communication and public healthcare management [2,3]. The survey of Rock Health and Stanford Center for Digital Health showed that the preference of US adults for communicating health issues through mobile apps has been increasing in recent years [4]. The result also revealed that approximately 44% of the respondents track their health and share health information with their medical professionals. Additionally, 25% use telemedicine and one in every 25 wearable owners uses an app to monitor their health.

mHealth apps have been proven to play a crucial role in battles against infectious diseases such as the SARS-CoV-2 (COVID-19) [2,5,6]. Specifically, contact-tracing apps with artificial intelligence technology can collect personal data of location, usage and vital signs to provide users real-time information and share medical advice accordingly [2,7]. Users of these apps can also get timely notifications about COVID-19 infection hotspots in order to avoid those areas [8,9]. Therefore, mHealth apps can assist risk mitigation strategies and share the burden of medical centers, especially when the resources for COVID-19 testing and treatment are scarce [10].

Taking advantage of this technology, many governments have deployed mHealth apps to fight against the deadly COVID-19 pandemic [8,11]. For example, the government of China has controlled the spread of COVID-19 by monitoring mobile apps in order to access citizens' travel history and quarantine status [5]. South Korea has also implemented a social tracking system with mobile apps as the core to warn their people about their proximity to infected cases as well as to detect and isolate those afflicted [12]. US agencies are cooperating with technology giants such as Apple and Google to launch COVID-19 contact-tracing apps [9,13].

However, to be useful, mobile apps may need access to personal information (e.g., identity, location, system settings, voice and text) [14]. Hence, information privacy is the main concern of users related to mobile technology adoption [15]. Belanger and Crossler [16] indicated that, with the fear that sensitive information can be disclosed and misused by malicious apps without their authorization, users often pursue actions to protect themselves. A survey on US adults by Pew Research Center reported that more than half of the participants chose not to install and 30% of them said they will uninstall a mobile app if they have concerns over their personal information being misused by the app [17]. The same privacy issue has also been raised over mHealth apps which, to

* Corresponding author.
E-mail addresses: trancongduc@tdtu.edu.vn (C.D. Tran), nguyentrungtin@tdtu.edu.vn (T.T. Nguyen).

https://doi.org/10.1016/j.techsoc.2021.101755
Received 12 May 2021; Received in revised form 25 August 2021; Accepted 12 September 2021
Available online 21 September 2021

provide benefits to users, require more sensitive data (e.g., daily habit, health status and medical history) [18]. Wiegard and Breitner [19] indicated that consumers perceive a higher level of risk when they are requested to share health information as compared to other information types.

While indicating that the unauthorized use of information by technology companies is not newly occurring, Kaplan and Ranchordás [20] warned that information privacy and security issues have become more salient in terms of the sensitive data collected and transferred through mHealth apps. Moreover, in the COVID-19 crisis, governments are forced to act for public health, which may result in loosening regulations of digital information privacy and normalizing the deployment of social surveillance [8,21,22]. In the same vein, Kaplan [23] addressed that legal, ethical and social issues, which are primarily related to information technology in healthcare, were seldom discussed when the pandemic broke out. Observers and scholars are concerned that personal data obtained during the outbreak would not be rolled back and, even worse, continue to be used after the pandemic [7,22]. Therefore, COVID-19 may not only threaten public physical wellness but also raise fear and anxiety regarding the viral infection [24] and information insecurity [25].

The impact of information privacy and security on the use of mHealth apps has also received great interest in the extant literature [26,27]. However, prior studies on behavioral intention toward mobile apps primarily focus on risk-benefit tradeoff (e.g. Refs. [6,26,28], in which perceived privacy risk is compared with perceived benefits from the functional, hedonic and monetary dimensions of the apps. Minor attention has been directed toward individuals' tradeoff between privacy risk and health risk regarding mHealth app adoption, especially in the context of viral infectious diseases. Van Houtven et al. [29] indicated that the risk-dollar tradeoff approach may be beneficial for studies designed to measure the absolute level of risk probabilities in the form of monetary benefit. However, the risk-risk tradeoff approach can lower the cognitive burdens on respondents by allowing them to compare the magnitude of relatively similar "commodities", which facilitates additional understanding of how people make decisions to maximize lifetime utility. Moreover, in the context of mHealth adoption, Atienza et al. [26] called for further investigations of different tradeoffs to information privacy that affect consumers' decisions. Therefore, based on the concerns about health risk and privacy risk regarding mHealth app use during the COVID-19 pandemic, this study aims to (1) investigate how perceived health risk and perceived privacy risk influence COVID-19 contact-tracing app users' perceived value and usage behavior and (2) whether these individuals engage in risk-risk tradeoff during their decision-making process. To achieve these purposes, the present study proposed and tested the model of risk-risk tradeoff built upon the privacy calculus theory (PCT) [30] and the concept of risk-risk tradeoff [31]. The findings from Partial Least Square-Structural Equation Modeling (PLS-SEM) and fuzzy-set Qualitative Comparative Analysis (fsQCA) highlighted that, under the uncertainty of the COVID-19, contact-tracing app users face a tradeoff between health risk and privacy risk.

In this COVID-19 pandemic, people would be ready to share their personal information for their own safety and the greater good of society [5]. Therefore, in the choice between privacy and health, they may lean toward the latter. However, trading off one risk for another is an unnecessary choice if there is an existing superior solution [31]. Hence, by exploring individuals' risk minimization in using COVID-19 contact-tracing apps, the present study calls for a more balanced approach to health risk-privacy risk tradeoffs in the post-pandemic world.

2. Literature review

2.1. Conceptual background

2.1.1. The concept of risk-risk tradeoff

The risk-risk tradeoff approach in investigating individuals' decision-making was first proposed in the work of Viscusi et al. [32]. Graham and Wiener [31] further developed the notion of risk-risk tradeoff, conceptualizing it as "the change in the portfolio of risks that occurs when a countervailing risk is generated by an effort to reduce the target risk." For example, the action of taking a certain drug to reduce a disease threat may attach a countervailing risk of side effects. The risk-risk tradeoff phenomenon is classified into four categories along two dimensions, namely, (1) the target population and (2) the difference in types of target risk and countervailing risk (Table 1). Moreover, Etkin [33] coined the term "risk transference" to describe the process of short-term risk mitigation which increases long-term vulnerability.

However, the concept of risk-risk tradeoff has mostly been adopted as a precautionary principle for decision-making at the organizational level [34–37]. Few studies have investigated the risk-risk tradeoff mechanism at the individual level. Notably, Van Houtven et al. [29] assessed a sample of 1010 households on their choices between avoiding two fatality risks, i.e., cancer risk with latency periods of 5, 15 and 25 years and automobile accident risk with immediate death. The results revealed that people have a stronger preference for avoiding the risk of cancer due to their perceived feelings of dread and suffering. However, longer periods of cancer latency and morbidity increase the acceptance of cancer risks due to the expectation that death will be less impactful later in life and the hope for a cancer cure in the future. Waters et al. [38] examined patients' difficult decisions about medical alternatives in which the treatment may decrease one risk of illness but increase the likelihood of others. However, there are other factors beyond the efficacy of the therapy and the probability of side effects influencing patients' decisions. Hypothesizing that tradeoffs in drug choice may involve multiple factors, Aikin et al. [39] conducted a study exploring consumers' tradeoff regarding prescription drugs for diabetes. The findings indicated that consumers' choices are more impacted by market claims (e.g., "best-selling") than efficacy information. In addition, Shimshack and Ward [40] explored the risk-risk tradeoff between omega-3 and mercury intakes. In response to the 2010 US national mercury advisory, consumers reduced all seafood consumption instead of just the high mercury-contained types, which backfired the advisory. Nevertheless, many aspects of the risk-risk tradeoff in consumer decision-making have remained untouched. Thus, further investigations of these tradeoff mechanisms in different consumption contexts would contribute to the advancement of the literature as well as managerial practices.

2.1.2. Privacy calculus theory

Most research frameworks aiming to provide an understanding on the acceptance of new technologies have tested the strength of non-contrary factors (e.g., usefulness, convenience, attitude and trust) as the drivers [41]. However, the extant literature also indicates inhibitors (e.g., financial cost, complexity and privacy) that hinder the

Table 1
Typology of risk-risk tradeoffs [31].

	Compared to the target risk, the countervailing risk is	
	Same type	Different type
Compared to the target risk, the countervailing risk affects		
Same population	Risk offset	Risk substitution
Different population	Risk transfer	Risk transformation

endorsement among information technology users [19]. As most individuals' decisions involve utility maximization or loss minimization, integrating these contrary factors into the same research model will provide a more holistic view of how decisions are made based on the relative weights of anticipated gain and loss.

Information privacy concern has long been regarded as the biggest intrinsic obstacle for the acceptance of new information technology. Generally, information privacy refers to individuals' control over the collection, unauthorized access and improper use of their personal information [42]. Laufer and Wolfe [30] were the first to formulate the privacy calculus theory (PCT) which posits that the simultaneous effects of positive factors regarding benefits of a technology and the negative factor of potential privacy violation derived from using that technology. Rooted in expectancy theory [43], PCT makes a similar assumption that individuals rationally estimate the probability of positive outcomes against consequences to maximize gain or minimize loss related to the use of technology. However, PCT emphasizes more on the strength of users' belief in the influence of the outcomes. An outcome that is perceived to be less likely to occur yet cause large impacts is still relevant and significant. Hence, the important concept in this theory is the cumulative strength of users' contradictory beliefs during the decision-making process, from evaluating the technology's value to actual use and reuse.

Since Laufer and Wolfe [30], PCT has been adopted to explain consumers' tradeoff between privacy risk and benefits derived from using new technology in various contexts [19,44,45]. However, little attention has been directed to examining privacy tradeoffs in mHealth apps wherein the dilemma about whether to share personal information is a serious matter. Given that contact-tracing apps during the crisis of COVID-19 may not only provide distinctive advantages toward reducing health threats but also exhibit a high level of privacy risk, users of these apps are more likely to engage in a salient privacy tradeoff. Thus, the theoretical background of the focal study is built upon the PCT to investigate the tradeoff between privacy risk and health risk among COVID-19 contact-tracing app users.

2.2. Hypothesis generation

2.2.1. Perceived value

The concept of value has its roots in psychology and economics, specifically from the theory of exchange, utility and labor value [46]. Scholars across research disciplines have proposed and adopted different terms of value which vary in context but are similar in basic concept. From the consumption perspective, value is categorized into two aspects: (1) utilitarian comprising rational, cognitive and functional and (2) hedonic including affective, emotional and experiential [47]. From the customer value theory, customer perception of value is constituted from transaction value and acquisition value of a product [46]. Thus, before performing a purchase, customers may engage in weighing the costs and benefits of their decision [48]. Similarly, customer perceived value is formulated from the concept of value maximization which is the result of calculating the cost and benefit of acquiring a product [46].

Early interpretations of value maximization center on the tradeoff between product quality and monetary cost [49,50]. However, such simplistic modeling of value maximization ignores the multi-dimensionality of the tradeoff phenomenon in decision-making. Acknowledging that perceived value is not only derived from the estimation of product quality and price, prior studies have examined the construct with different tradeoff mechanisms. For instance, Petrick [51] added emotional and social values, together with functional value (quality) and price, into the definition of perceived value. In the context of electronic commerce, Chen and Dubinsky [52] measured benefits by the product quality, costs by prices and perceived risk of the transaction. Although also built on the cost-benefit paradigm, the cost component in the perceived value of Chung and Koo [53] measures non-monetary sacrifices (i.e., effort and complexity) which are more relevant to the use of social media. The non-monetary aspect of cost in perceived value is further analyzed by taking into account the potential violation of information privacy which is forfeited against the overall benefit of health management regarding the use of mHealth smart services [19].

In the focal study, the conceptualization of perceived value is put forward by combining the PCT and the risk-risk tradeoff to understand the adoption of COVID-19 contact-tracing apps. Particularly, if perceived value is low (i.e., perceived privacy risk outweighs perceived health risk), users are likely to show resistance toward using such apps. In contrast, if perceived value is high (i.e., perceived health risk outweighs perceived privacy risk), users are more likely to continue to endorse the apps. Therefore, the following hypothesis was formulated.

H1. Perceived value is positively associated with COVID-19 contact-tracing app usage.

2.2.2. Perceived health risk and perceived privacy risk

Perceived risk is conceptualized as individuals' expectation of loss [54]. The construct is regarded to include two aspects, namely, probability and severity [55]. Higher levels of probability and severity of negative consequences are linked to greater risk perceived by the individual. Risk perception is also referred to as a powerful explanatory variable for consumer behaviors as they are motivated to avoid mistakes in making a purchase [54]. Regarding health issues, perceived health risk is defined as an individuals' assessment of chances that unfavorable outcomes may occur from hazards such as environment (chemical pollution, nuclear waste), medical therapies (vaccines, contraceptives), lifestyle behaviors (smoking, alcoholic drinking) [56] or infectious diseases [57]. Brewer et al. [58] noted that most theories of health behaviors agree on the predictive role of perceived risk on preventive behaviors. These behaviors are adopted with the belief that the probability of contracting diseases will decrease in the future [59].

The relationship between health risk perception and individuals' actions to reduce potential harm has been investigated in various contexts [57,60]. For instance, Hampson et al. [61] reported that perceived health risk reduced cigarette smoking in men. People with higher risk perceptions showed a higher propensity for vaccination [58]. Gregory et al. [62] indicated that obese adults with low levels of health risk perception were less willing to lose weight. In the context of epidemics, health risk perception has also been emphasized to motivate precautionary responses. For example, people with higher perceived risk were more likely to adopt self-protecting behaviors against SARS transmission [63]. Measuring individual- and societal-level risk perception, Yoo and Choi [64] reported that the interaction of health risk perception and self-efficacy could predict MERS-related communication in social media. More recently, conducting a study with data from ten countries, Dryhurst et al. [65] found a positive correlation between COVID-19-related risk perception and precautionary actions such as washing hands and wearing a face mask. Abdelrahman [66] highlighted health risk perception as a predictor of social distancing during the COVID-19 crisis. In the same vein, people who perceived high threats from COVID-19 also consider continuing to use mobile banking apps as a social distancing practice [67]. Notably, the meta-analysis study of Zhao et al. [68] indicated that perceived health risk, in the form of perceived severity, is one of the determinants of individuals' adoption intention toward mobile health services.

Similar to perceived health risk, perceived privacy risk is also included in the umbrella term of perceived risk. Specifically, perceived privacy risk refers to individuals' expectation of loss associated with the exposure or misuse of private information [69]. When users cannot control whether their information is used for the right purposes, they perceive the service as less desirable. Moreover, consumers may be unwilling to endorse a mobile service if privacy risks outweigh the potential benefits from information disclosure [19].

Perceived privacy risk has also been identified as one of the critical factors influencing the behavioral intention toward healthcare technologies [68]. Miltgen et al. [70] confirmed the negative impact of privacy risk perception on the intention to use biometrics systems. Other studies have also concluded that privacy concerns act as a barrier toward consumers' willingness to share health information and negatively affect their intention to use mHealth [27,71].

From the privacy calculus perspective, Jiang et al. [72] developed the privacy tradeoff model which was later adopted in Wang et al. [45] and Koohikamali et al. [28]. The privacy tradeoff suggests that users are not completely dissuaded by privacy concerns and are willing to compromise certain risks of privacy to gain potential monetary or social compensations [45]. In other words, users weigh between the negative consequences and positive outcomes of disclosing personal information in the decision to use a technological application.

Indeed, decisions in the face of risk usually involve rational utility maximization or maximum loss minimization, which are the main concepts in decision theories [73,74]. Drawing upon this logic, people may also conduct risk-risk tradeoff as a decision-making mechanism to minimize the expected loss, in which one risk may be accepted to lower the likelihood of a more severe risk. In risk-risk tradeoff, mitigating the probability and severity of net risk can be considered a benefit. However, individuals' tradeoff between health risk and privacy risk has received little attention in the extant literature, especially when both health and privacy issues are the major concerns during the COVID-19 pandemic [8,21]. Therefore, based on the concept of risk-risk tradeoff [31] and the PCT [30], we assume that users engage in health risk-privacy risk tradeoff when evaluating COVID-19 contact-tracing apps' value and deciding to use the apps. From the above discussions, the following hypotheses were proposed. The research framework is outlined in Fig. 1.

H2. Perceived health risk is positively associated with perceived value of COVID-19 contact-tracing apps.

H3. Perceived privacy risk is negatively associated with perceived value of COVID-19 contact-tracing apps.

H4. Perceived health risk is positively associated with COVID-19 contact-tracing app usage.

H5. Perceived privacy risk is negatively associated with COVID-19 contact-tracing app usage.

3. Method

3.1. Data collection

Due to social distancing during the COVID-19 outbreak, we conducted an online survey recruiting participants via Amazon Mechanical Turk (MTurk). Mturk is a crowdsourcing system that has been commonly used in similar research [75,76]. To address the issues of cheating, speeding, hypothesis guessing and other concerns about the quality of data from MTurk [77,78], we used the following screening questions and techniques to design the survey. First, we predetermined the criteria to participate in the study that the survey takers must have completed at least 1000 tasks on MTurk with an acceptance rate above 95%. Second, to avoid experience bias, respondents who reported that they tested positive for COVID-19 were screened out. Third, we checked whether the respondents were app users by describing a hypothetical app based on Exposure Notifications (e.g., Covid Watch Arizona, COVID Alert PA), then asking if they were using a similar app. Fourth, one attention check and one language check were included to identify poor participants. Fifth, we mixed the order of the questions and prevented backtracking within the questionnaire to mitigate the potential hypothesis guessing. Lastly, we collected data on different days and times, from late October to early November 2020, to have a diverse sample.

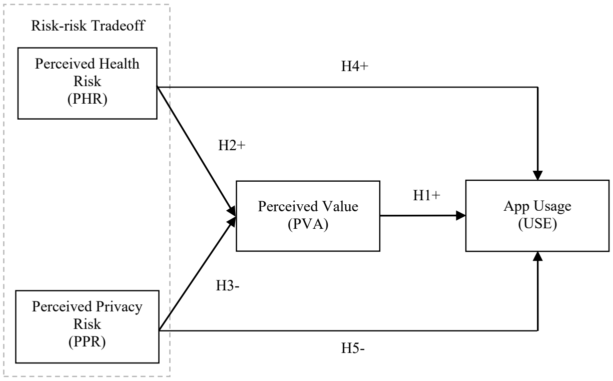

Fig. 1. Research framework.

A total of 350 US users of COVID-19 contact-tracing apps were recruited. However, only 285 responses were valid for further analyses. Table 2 describes the sample based on their demographics. In particular, the sample comprises 43.86% female and 56.14% male participants. About 61.75% of the participants are in the 18–50 year age bracket. Approximately 75.09% have a bachelor's or a higher degree.

3.2. Measures

All items of the independent variables were measured on a 5-point Likert scale ranging from 1 "strongly disagree" to 5 "strongly agree". Specifically, three perceived privacy risk (PPR) items were modified from Wiegard and Breitner [19] to fit the context of COVID-19 contact-tracing apps. To accurately capture the perceived health risk (PHR) that motivates the precautionary action of adopting contact-tracing apps, we followed Brewer et al. [79] to developed two items measuring the likelihood of contracting COVID-19 and the severity of this disease that are conditioned against not using the apps. Three items for perceived value (PVA) were modified from Xu et al. [80]. Finally, the dependent variable of app usage (USE) measures the self-reported frequency of use. The descriptive statistics of all variables are illustrated in Table 3.

4. Data analysis and results

4.1. Convergent validity analysis

Table 3 presents the results of the convergent validity test of the measurement model. All indicators met the minimum requirement of convergent validity as loading values, Cronbach's alpha (CA) and composite reliabilities (CR) were above 0.70 and AVE values were above 0.50 [81]. The Heterotrait-Monotrait Ratio (HTMT) test indicates that all ratios between independent and dependent variables were less than 0.90 (Table 4), which confirms the discriminant of all latent variables [82]. In addition, the ratios of variance inflation factor (VIF) of all

Table 2
Sample demographics (n = 285).

Characteristics		Frequency	Per cent
Gender	Female	125	43.86
	Male	160	56.14
Age	18–30	46	16.14
	31–40	33	11.58
	41–50	97	34.04
	51–60	69	24.21
	>60	40	14.04
Education	Less than senior high school	3	1.05
	Senior high school	71	24.91
	Bachelor's degree	161	56.49
	Master's degree	41	14.39
	Doctoral degree	9	3.16

Table 3
Descriptive statistics, items loadings and validities.

Construct	Item	Loadings	Mean	Std. D.	AVE	CR	CA	Mean	Std. Error	Std. D.
Perceived health risk (PHR)	It is likely that my health will be affected by COVID-19 in the next 6 months if I don't use a COVID-19 contact tracing app. (PHR1-likelihood)	0.896	2.326	1.029	0.812	0.896	0.769	1.884	0.054	0.905
	My health will be seriously damaged by COVID-19 in the next 6 months if I don't use a COVID-19 contact tracing app. (PHR2-severity)	0.906	1.442	0.980						
Perceived privacy risk (PPR)	It would be risky to disclose my personal information to COVID-19 contact-tracing apps. (PPR1)	0.922	3.519	1.146	0.854	0.946	0.915	3.426	0.064	1.082
	There would be high potential for loss associated with disclosing my personal information to COVID-19 contact-tracing apps. (PPR2)	0.913	3.312	1.194						
	There would be too much uncertainty associated with giving my personal information to COVID-19 contact-tracing apps. (PPR3)	0.936	3.446	1.172						
Perceived value (PVA)	Compared to the risks of my information disclosure, the use of COVID-19 contact-tracing apps is beneficial to me. (PVA1)	0.908	3.260	0.991	0.816	0.930	0.887	3.048	0.054	0.908
	Compared to the information I need to disclose, the use of COVID-19 contact-tracing apps offers value to me. (PVA2)	0.927	3.110	0.994						
	Overall, the use of COVID-19 contact-tracing apps delivers good value to me. (PVA3)	0.874	2.779	1.033						
App usage (USE)	How often do you use the COVID-19 contact-tracing app every week? (USE)	–	2.270	1.103	–	–	–	2.270	0.065	1.103

Note: Std.D.: Standard deviation. Std. Error: Standard error. AVE: Average variance extracted. CR: Composite reliability. CA: Cronbach's alpha. According to Hair et al. [81], the ratios of loading, AVE, CR and CA are required to be above 0.7, 0.5, 0.7 and 0.7, respectively.

Table 4
Heterotrait-Monotrait Ratio (HTMT) discriminant analysis.

	PHR	PPR	PVA	USE
PHR				
PPR	0.463			
PVA	0.604	0.509		
USE	0.780	0.513	0.641	

indicators were lower than the recommended threshold: the VIF of PPR was highest at 3.824 and that of PHR was lowest at 1.640 (VIF ≤ 5) [83], which suggests the minimum collinearity in every item of the structural model.

4.2. PLS-SEM analysis

To explore the relationship among perceived health risk, perceived privacy risk, perceived value and COVID-19 contact-tracing app usage, this study employed Structural Equation Modeling (SEM) technique to test the net-effect relations among latent variables. Gefen et al. [84] indicated that SEM integrates the measurement and structural model into a simultaneous assessment. Therefore, this method is flexible to model the relationships among criterion variables and multiple predictors [85]. This study conducted the measurement validation and tested the model with SmartPLS version 3.3.2. In addition, 5000 bootstrapping replication from the original sample was performed as recommended by Hair et al. [86] to get the validated results. The bootstrap confidence interval (CI) was reported to further present the stability of coefficient estimation [81].

Table 5 reports the structural model assessment results after controlling the demographic variables. Perceived health risk (PHR) was revealed to have a positive correlation with app usage (USE) (*$\beta = 0.466$, $\rho = 0.000$, CI is [0.363, 0.560]*), while perceived privacy risk (PPR) had a positive association with USE (*β = -0.171, ρ = 0.000, CI is [-0.268, -0.071]*). Furthermore, the statistical results showed a positive association between PHR and perceived value (PVA) (*$\beta = 0.374$, $\rho = 0.000$; CI is [0,274, 0.461]*) and a negative association between PPR and PVA (*β = -0.317, $\rho = 0.000$, CI is [-0.406, -0.226]*). Besides, a high perceived value was related to a high frequency of use which was statically illustrated by the positive relationship between PVA and USE (*$\beta = 0.286$, $\rho = 0.000$, CI is [0.181, 0.393]*). These findings confirmed the proposed hypotheses (H1, H2, H3, H4 and H5) and the research model, which indicates that the participants engage in a risk-risk tradeoff between privacy information disclosure and the probability of being affected by the COVID-19 when using contact-tracing apps.

We further extended the analysis by investigating the indirect effects between the variables following the procedures of Nitzl et al. [87]. The results revealed that PVA significantly mediated the paths between PHR and USE (*β = 0.107, ρ = 0.000*) and PPR and USE (*β = -0.091, ρ = 0.000)*. We also evaluated the model with the cross-validated

Table 5
Structural model path coefficients testing results.

Effects on endogenous variables	β	t	p	CI		f^2	Decisions
				2.5%	97.5%		
1. Perceived value (*Adj.*$R^2 = 0.329$; $Q^2 = 0.265$)							
Perceived health risk (*H2+*)	0.374	7.868	0.000*	0.274	0.461	0.188	Supported
Perceived privacy risk (*H3-*)	-0.317	6.844	0.000*	-0.406	-0.226	0.127	Supported
2. mHealth app usage (*Adj.*$R^2 = 0.583$; $Q^2 = 0.565$)							
Perceived value (*H1+*)	0.286	5.376	0.000*	0.181	0.393	0.137	Supported
Perceived health risk (*H4+*)	0.466	9.362	0.000*	0.363	0.560	0.392	Supported
Perceived privacy risk (*H5-*)	-0.171	3.405	0.001*	-0.268	-0.071	0.059	Supported

Note: Null hypothesis of constant variance were rejected if p-value is lower than 0.05 [81]. Statistically significance is at 1% (*). Standardized root mean square residual (SRMR) = 0.046. CI: Confidence intervals.

redundancy index (Q^2) for the endogenous reflective constructs. A Q^2 greater than 0 implies that the model has predictive relevance. The results summarized in Table 5 confirmed that the structural model had satisfactory predictive relevance for all the endogenous constructs. We additionally computed the standardized root mean square residual (SRMR) that is recommended to be under 0.08 by Henseler et al. [82]. The research model achieved an SRMR of 0.046, which indicates an appropriate fit. Furthermore, since f^2 measures the strength of explanation between exogenous and endogenous variables [88,89], the results of effect size (Table 5) confirmed the medium and large significant effects of PHR and PPR on the magnitude of PVA and USE.

Finally, three control variables, namely, age, gender and education, were included in the analysis to address whether the relationships tested in this study are affected by them [90]. No significant changes for the influence of the endogenous variable were observed after the inclusion. Of the three control variables, only age was found to have a significant negative impact on app usage (*$\beta = -0.082$, $\rho = 0.014$).*

4.3. Fuzzy-set qualitative comparative analysis

Built upon the complexity theory and Boolean logic, fuzzy-set qualitative analysis (fsQCA) is a case-based approach that has recently received great attention across disciplines of health information technology research [90,91]. While variable-based analysis approaches primarily focus on testing the finality – that is, the direct or indirect impact of single dependent variables on the dependent variables, case-based approaches stress the equifinality – that is, the different configurations (combinations) of conditions on a specific outcome regardless of whether these configurations are contradictory [92,93]. As both approaches have exclusive strengths and limitations [94], fsQCA was complementarily applied to delve deeper into the data set to shed light on the health risk-privacy risk tradeoff in using COVID-19 contact-tracing apps.

FsQCA uses two measures to determine the relationship between sets [95]. Consistency (Equation (1)) indicates the extent to which a condition set is sufficient for an outcome set. Coverage (Equation (2)) represents how much the outcome set is covered by the condition set.

$$\text{Consistency} = \Sigma[\min(\text{Xi}, \text{Yi})]/\Sigma(\text{Xi}) \quad (1)$$

$$\text{Coverage} = \Sigma[\min(\text{Xi}, \text{Yi})]/\Sigma(\text{Yi}) \quad (2)$$

The procedure of fsQCA comprises three fundamental steps as follows. First, the original data from the 5-point Likert scale were calibrated into fuzzy membership scores ranging from 0.0 to 0.5 (out-of-set) and 0.5 to 1.0 (in-set). The score of 0.5 is the crossover point. As fsQCA classifies the data set into cases according to in-set and out-of-set dichotomy and analyzes the subset relation using fuzzy scores, fsQCA is considered a qualitative-quantitative hybrid method. This study assigned the Likert scale values of 5, 3 and 1 to the three membership anchors of 0.95, 0.5 and 0.05, respectively. For the binary variable of gender, the value of 0 denotes female and 1 denotes the opposite. As there are two conditions which are perceived health risk (PHR) and perceived privacy risk (PPR) relevant to the outcome of high usage frequency (USE), we followed Thai and Wang [96] to categorize the data set into four cases demonstrated in Table 6.

Table 6
Case matrix.

	Perceived privacy risk	
	High	Low
Perceived health risk		
High	PHR*PPR	PHR*ppr
Low	phr*PPR	phr*ppr

Note: "*" is equivalent to Boolean logic AND. Uppercase antecedent names denote high scores (>0.5). Lowercase denotes the contrary.

Second, necessary condition analysis was conducted to address which antecedents of PHR and PPR are necessary for USE. As shown in Table 7, although the coverage values ranged from 0.3449 to 0.8669, higher than recommended cut-off point of 0.25, all consistencies were below the threshold of 0.9 [95], which suggests that no solitary antecedents are necessary enough for USE.

Third, sufficient condition analysis was performed to identify the antecedents and their configurations leading to the outcome of USE. Following Pappas et al. [97], this study set the consistency cut-off point at 0.85. The results yielded from the analysis revealed two equifinal configurations of conditions sufficient for USE: PHR*ppr and PHR*PPR (Table 8). Consistency of the first configuration achieved at 0.9132 and the second at 0.87. The overall consistency was 0.8669. The overall coverage was 0.6031 indicating that the two solutions covered approximately 60% of the cases that had high usage frequency.

Additionally, three demographic variables, namely, gender (GEN, gen), age (AGE, age) and education (EDU, edu) were considered jointly with perceived health risk and perceived privacy risk in the sufficient condition analysis to get a thorough understanding of the effect of risk-risk tradeoff on COVID-19 contact-tracing app usage. The findings indicated one solution: USE = f (PHR*ppr*GEN*age*edu) with an acceptable consistency of 0.911. This result is interpreted as that the combination of high perceived health risk, low perceived privacy risk, male, young age and low education sufficiently leads to the high frequency of app usage.

5. General discussion

The main focus of this study has been to clarify how perceived health risk and perceived privacy risk influence individuals' adoption of COVID-19 contact-tracing apps from the risk minimization perspective. In an attempt to serve this purpose, a risk-risk tradeoff model was developed based on the PCT and the concept of risk-risk tradeoff. Findings from the PLS-SEM analysis revealed the direct effects of health risk and privacy risk perceptions on perceived value and app usage, which confirms the risk-risk tradeoff model. The mediating role of perceived value between health risk and privacy risk perceptions and app usage was also statistically supported. While these variance-based analyses shed light on the net effects between the tested variables, the case-based method – fsQCA provided a deeper and more insightful investigation into the data set revealing that there were two causal configurations of conditions sufficient for the outcome of high use frequency. The first configuration included high health risk perception and low privacy risk perception. Individuals who fall in this case are more likely to engage in using COVID-19 contact tracing apps. The second configuration comprised health risk and privacy risk perceptions both at high levels, which indicates that individuals in this group face risk-risk tradeoffs when using the apps. Furthermore, results from PLS-SEM and fsQCA agreed that age was negatively associated with app usage. As age is considered the proxy of individuals' technology literacy and competence [68], the adoption of contact-tracing apps may also be affected by these factors. This result was consistent with the findings in previous research that older users may not be as skilled as the young, and are therefore less likely to adopt and share personal information to a new

Table 7
Results of the necessary condition analysis.

Outcome	USE	
Condition	Consistency	Coverage
PHR	0.6031	0.8669
phr	0.8401	0.3449
PPR	0.6986	0.3668
ppr	0.7929	0.6462

Note: Uppercase antecedent names denote high scores (>0.5). Lowercase denotes the contrary.

Table 8
Results of the sufficient condition analysis.

Outcome		USE		
Solution		Raw consistency	Solution consistency	Solution coverage
1	PHR*ppr	0.9132	0.8669	0.6031
2	PHR*PPR	0.8700		

Note: "*" is equivalent to Boolean logic AND. Uppercase antecedent names denote high scores (>0.5). Lowercase denotes the contrary.

and complex technology [68,72,98].

These findings support prior studies linking health risk and privacy risk perception with the adoption of healthcare technologies [68], which provides useful implications for both academics and practitioners. Responding to Ahadzadeh et al.'s [60] call for research to foster a more extensive understanding of the relationship between perceived health risk and information technology usage in different platforms and applications, this study explored the positive influence of the COVID-19 health-related risk on the use of contact-tracing apps. This result echoes the findings in prior work that people who perceive higher levels of health risk are more attentive to health communication and preventive behaviors [64,65]. Also, the results revealed that individuals with high levels of privacy risk perception were less likely to continue endorsing the apps. Therefore, the risk of privacy violation could be one of the critical factors in explaining why people use mHealth apps only for a short time [99]. Also, reflecting on the call for investigations on different types of information privacy tradeoffs [26], this study is among the first to propose and examine the tradeoff between health risk and privacy risk regarding mHealth app use.

Overall, the focal study contributes to the research on privacy calculus theory by exploring the tradeoff between health risk and privacy risk in COVID-19 contact-tracing app use. Moving beyond the context of the pandemic, upcoming research can further develop the risk-risk tradeoff model in many different ways. First, the antecedents of the two components of the model can be explored, which provides more fruitful insights into how the risk-risk tradeoff is formed. This direction is similar to how the risk-benefit model has been exploited in prior studies [19,72,100]. Second, as this research focuses solely on risk substitution, it is beneficial for future research to examine other types of risk-risk tradeoffs (see Table 1). Third, the risk-risk tradeoff can also be extended by incorporating benefit variables to form a triad model. For example, Wang et al. [45] combined monetary rewards, social rewards and privacy concerns in their tradeoff framework.

From a methodological perspective, the focal study demonstrates a more appropriate approach to investigating the tradeoff phenomenon. The variance-based approaches focus on testing the net effects between variables [93]. For example, how perceived health risk (PHR) and perceived privacy risk (PPR) are correlated with app use. In contrast, fsQCA allows the examination of contradictory cases leading to the same outcome. For instance, if there are two antecedents (k), namely, health risk (HR) and privacy risk (PR), fsQCA categorizes the data set into four cases (2^k): (1) low HR, low PR, (2) high HR, low PR, (3) low HR, high PR and (4) high HR, high PR. It is expected that case 2 leads to high mHealth app use, but the tradeoff is questionable if one perceives high health risk and no privacy risk at all. This is similar to case 1 where the tradeoff is not applicable. In this context, cases 3 and 4 provide a more relevant field to understand the tradeoff concept.

Despite its power in theory drafting and testing, fsQCA is not free from limitations. When the original data is calibrated into fuzzy scores, multi-item scales are converted into a single indicator [101,102]. Therefore, examining the effect size of each item is impossible. Moreover, fsQCA provides no standards to measure the validity and reliability of the questionnaire as well as model fit. Considering the exclusive advantages and limitations of variance-based approaches and fsQCA, they should be used in a complementary rather than a substitute manner [96, 101].

In the crisis of the COVID-19 outbreak, mHealth apps have emerged as a reliable channel for public health communication and preventative health promotion. Nevertheless, to be useful, mHealth apps need access to users' sensitive information which has raised concerns about data disclosure, misuse and social surveillance [18,22]. In this pandemic, people may compromise their information privacy for community health [5]. However, as we can and should enjoy the rights over personal privacy as well as healthcare, any decisions involving this tradeoff mechanism lead to a false choice. Indeed, rational decision-making processes in the situation of uncertainty should always attempt to alleviate the net risk rather than compromise one type of risk for another, or a short-term risk for a long-term non-observable risk.

Not all COVID-19 contact-tracing apps are created equally. During the pandemic, governments may be so preoccupied with saving lives that some contact-tracing approaches are implemented under a presupposition that citizens should compromise individual privacy for the greater good. Contacting-tracing apps in some countries include the functions of location tracking and facial recognition to assist public officials in identifying users and enforcing quarantine [103]. Personal data collected from these contact-tracing apps are promised to keep anonymous. However, anonymity is not equivalent to privacy. Indeed, privacy is individuals' right to decide what information to be shared and whom they are shared with [104]. A less privacy-invasive approach is taken in other countries with the launch of voluntary apps that adopt a proximity-based rather than a location-based architecture [9,105]. However, such apps are not free from privacy infringements because infected users can be re-identified based on group data [104,106]. Furthermore, according to Williams et al. [105], privacy concerns, lack of information and misconception about COVID-19 contact-tracing apps are among the main reasons explaining why people hesitate to install. Therefore, to reduce users' concerns about social control, app providers must commit to handling data with users' consent and offer satisfactory action plans when privacy intrusions occur. Additionally, to increase the adoption rate, the design choice of the apps should be handed to the public. In an ideal case, more than one app with different levels of utility-privacy tradeoffs can be developed and offered to the citizens [106]. Most importantly, transparency of privacy rights and data handling should be adequately communicated with the public to dispel misconceptions, alleviate privacy concerns as well as build trust in contact-tracing apps.

As with any study, limitations should be addressed. First, the sample size in this study is relatively small and does not cover all communities; hence, the findings do not represent the US population as a whole. Although the main contribution of this study is the confirmation of the health risk-privacy risk tradeoff phenomenon, with a larger sample and more demographic data, we could have better explored the patterns in individuals that explain their tradeoffs. Second, to control the potential experience bias, we screened out participants who self-reported to be infected by COVID-19. However, we did not collect information on whether their close ones had been adversely impacted by the virus. Third, the participants were recruited from MTurk. Since most MTurkers are tech-savvy and highly educated individuals who have substantial knowledge of technology, future studies can work on more diverse samples, which makes it possible to test the potential moderating effects of self-efficacy or technology literacy. Fourth, although several screening techniques were performed to control the quality of data collected from MTurk as recommended in Kees et al. [78], solely using data from this crowdsourcing platform may restrict the study's generalizability due to the potential self-selection bias. Therefore, testing the research model with samples from different sources is suggested with future efforts. Finally, the focal study is restricted to a single-country sample, which has not taken into account the cultural and technological differences among parts of the world. Hence, comparative studies of how health risk and privacy risk perceptions affect contact-tracing app adoption in different countries would be necessary.

Author statement

Cong Duc Tran: Data curation, PLS-SEM analysis, Writing – draft and revised manuscript. **Tin Trung Nguyen:** Conceptualization, Methodology, fsQCA, Writing – draft and revised manuscript, Reviewing and editing.

Acknowledgement

The authors thank the anonymous reviewers for their constructive remarks. We are grateful to Mr. Tristan Fields and Ms. Victoria Hanh Nguyen for their help with the readability of the manuscript.

References

[1] L. Dam, D. Roy, D.J. Atkin, D. Rogers, Applying an integrative technology adoption paradigm to health app adoption and use, J. Broadcast. Electron. Media 62 (4) (2018) 654–672, https://doi.org/10.1080/08838151.2018.1519568.

[2] R.S. Istepanian, T. AlAnzi, Mobile Health (M-health): Evidence-Based Progress or Scientific Retrogression, Biomedical Information Technology, 2020, pp. 717–733, https://doi.org/10.1016/B978-0-12-816034-3.00022-5.

[3] M. Rajak, K. Shaw, Evaluation and selection of mobile health (mHealth) applications using AHP and fuzzy TOPSIS, Technol. Soc. 59 (2019) 101186, https://doi.org/10.1016/j.techsoc.2019.101186.

[4] Rock Health, Digital Health Consumer Adoption Report, 2019. https://rockhealth.com/reports/digital-health-consumer-adoption-report-2019/. (Accessed 11 January 2021). Accessed.

[5] C. Barbieri, J.P. Darnis, Technology: an Exit Strategy for COVID-19? Commentaries Istituto Affari Internazionali, 2020, pp. 1–4.

[6] G. Fox, T. Clohessy, L. van der Werff, P. Rosati, T. Lynn, Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications, Comput. Hum. Behav. 121 (2021) 106806, https://doi.org/10.1016/j.chb.2021.106806.

[7] W. Naudé, Artificial Intelligence vs COVID-19: Limitations, Constraints and Pitfalls, AI & Society, 2020, https://doi.org/10.1007/s00146-020-00978-0.

[8] J. Abeler, M. Bäcker, U. Buermeyer, H. Zillessen, COVID-19 contact tracing and data protection can go together, JMIR mHealth and uHealth 8 (4) (2020), e19359, https://doi.org/10.2196/19359.

[9] E.M. Redmiles, User concerns 8 tradeoffs in technology-facilitated COVID-19 response, Digital Government: Research and Practice 2 (1) (2020) 1–12, https://doi.org/10.1145/3428093.

[10] D.A. Drew, L.H. Nguyen, C.J. Steves, C. Menni, M. Freydin, T. Varsavsky, A. T. Chan, Rapid implementation of mobile technology for real-time epidemiology of COVID-19, Science 368 (6497) (2020) 1362–1367, https://doi.org/10.1126/science.abc0473.

[11] M. Silva A., Mobile Apps during COVID-19, European Emergency Number Association, 2020. https://eena.org/document/covid-19-apps/. (Accessed 11 January 2021).

[12] A. Cuthbertson, Coronavirus Apps Let People Avoid High-Risk Locations in South Korea, 2020. Independent, https://www.independent.co.uk/life-style/gadgets-and-tech/news/coronavirus-news-app-south-korea-latest-cases-deaths-location-a9371651.html/. (Accessed 26 January 2021).

[13] K. Grind, R. McMillan, A.W. Mathews, To track virus, governments weigh surveillance tools that push privacy limits, Wall St. J. (2020). https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841/. (Accessed 11 January 2021).

[14] K. Degirmenci, N. Guhr, M.H. Breitner, Mobile applications and access to personal information: a discussion of users' privacy concerns, in: M. Chau, R. Baskerville (Eds.), Proceedings of the 34th International Conference on Information Systems (ICIS 2013), 2013, pp. 1–21.

[15] X. Guo, X. Zhang, Y. Sun, The privacy–personalization paradox in mHealth services acceptance of different age groups, Electron. Commer. Res. Appl. 16 (2016) 55–65, https://doi.org/10.1016/j.elerap.2015.11.001.

[16] F. Belanger, R.E. Crossler, Dealing with digital traces: understanding protective behaviors on mobile devices, J. Strat. Inf. Syst. 28 (1) (2019) 34–49, https://doi.org/10.1016/j.jsis.2018.11.002.

[17] J.L. Boyles, A. Smith, M. Madden, Apps and Privacy: More than Half of App Users Have Uninstalled or Decided to Not Install an App Due to Concerns about Their Personal Information, Internet & Technology, 2012. Pew Research Center, http://www.pewinternet.org/2012/09/05/main-findings-7/. (Accessed 11 January 2021).

[18] M. Hussain, A. Al-Haiqi, A.A. Zaidan, B.B. Zaidan, M. Kiah, S. Iqbal, M. Abdulnabi, A security framework for mHealth apps on Android platform, Comput. Secur. 75 (2018) 191–217, https://doi.org/10.1016/j.cose.2018.02.003.

[19] R.B. Wiegard, M.H. Breitner, Smart services in healthcare: a risk-benefit-analysis of pay-as-you-live services from customer perspective in Germany, Electron. Mark. 29 (1) (2019) 107–123, https://doi.org/10.1007/s12525-017-0274-1.

[20] B. Kaplan, S. Ranchordas, Alzheimer's and m-health: regulatory, privacy, and ethical considerations, Everyday Technologies in Healthcare 1 (2019) 31–52.

[21] A.J. Bokolo, Exploring the adoption of telemedicine and virtual software for care of outpatients during and after COVID-19 pandemic, Ir. J. Med. Sci. 190 (2020) 1–10, https://doi.org/10.1007/s11845-020-02299-z.

[22] A.R. Brough, K.D. Martin, Consumer privacy during (and after) the COVID-19 pandemic, J. Publ. Pol. Market. 40 (1) (2021) 108–110, https://doi.org/10.1177/0743915620929999.

[23] B. Kaplan, Revisting health information technology ethical, legal, and social issues and evaluation: telehealth/telemedicine and Covid-19, Int. J. Med. Inf. 143 (2020), https://doi.org/10.1016/j.ijmedinf.2020.104239, 104239.

[24] Y. Huang, N. Zhao, Generalized anxiety disorder, depressive symptoms and sleep quality during COVID-19 outbreak in China: a web-based cross-sectional survey, Psychiatr. Res. 288 (2020) 112954, https://doi.org/10.1016/j.psychres.2020.112954.

[25] A. Guinchard, Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? Int. Rev. Law Comput. Technol. 35 (1) (2020) 84–97, https://doi.org/10.1080/13600869.2020.1794569.

[26] A.A. Atienza, C. Zarcadoolas, W. Vaughon, P. Hughes, V. Patel, W.Y.S. Chou, J. Pritts, Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study, J. Health Commun. 20 (6) (2015) 673–679, https://doi.org/10.1080/10810730.2015.1018560.

[27] L. Zhou, J. Bao, V. Watzlaf, B. Parmanto, Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study, JMIR mHealth and uHealth 7 (4) (2019) e11223, https://doi.org/10.2196/11223.

[28] M. Koohikamali, A.M. French, D.J. Kim, An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: a longitudinal perspective, Decis. Support Syst. 119 (2019) 46–59, https://doi.org/10.1016/j.dss.2019.02.007.

[29] G. Van Houtven, M.B. Sullivan, C. Dockins, Cancer premiums and latency effects: a risk tradeoff approach for valuing reductions in fatal cancer risks, J. Risk Uncertain. 36 (2) (2008) 179–199, https://doi.org/10.1007/s11166-008-9032-2.

[30] R.S. Laufer, M. Wolfe, Privacy as a concept and a social issue: a multidimensional developmental theory, J. Soc. Issue. 33 (3) (1977) 22–42, https://doi.org/10.1111/j.1540-4560.1977.tb01880.x.

[31] J.D. Graham, J.B. Wiener, Confronting risk tradeoffs, in: J.D. Graham, J.B. Wiener (Eds.), Risk vs. Risk, Harvard University Press, Cambridge, MA, 1995, pp. 1–41.

[32] W.K. Viscusi, W.A. Magat, J. Huber, Pricing environmental health risks: survey assessments of risk-risk and risk-dollar trade-offs for chronic bronchitis, J. Environ. Econ. Manag. 21 (1) (1991) 32–51, https://doi.org/10.1016/0095-0696(91)90003-2.

[33] D. Etkin, Risk transference and related trends: driving forces towards more mega-disasters, Global Environ. Change B Environ. Hazards 1 (2) (1999) 69–75, https://doi.org/10.3763/ehaz.1999.0109.

[34] F. Carlsson, D. Daruvala, H. Jaldell, Do administrators have the same priorities for risk reductions as the general public? J. Risk Uncertain. 45 (1) (2012) 79–95, https://doi.org/10.1007/s11166-012-9147-3.

[35] S.E. Hrudey, Chlorination disinfection by-products, public health risk tradeoffs and me, Water Res. 43 (8) (2009) 2057–2092, https://doi.org/10.1016/j.watres.2009.02.011.

[36] A.S. Jovanović, V. Pilić, Dealing with risk–risk interdependencies and trade-offs in relation to development and use of new technologies, J. Risk Res. 16 (3–4) (2013) 393–406, https://doi.org/10.1080/13669877.2012.729528.

[37] R. Lofstedt, A. Schlag, Risk-risk tradeoffs: what should we do in Europe? J. Risk Res. 20 (8) (2017) 963–983, https://doi.org/10.1080/13669877.2016.1153505.

[38] E.A. Waters, N.D. Weinstein, G.A. Colditz, K. Emmons, Formats for improving risk communication in medical tradeoff decisions, J. Health Commun. 11 (2) (2006) 167–182, https://doi.org/10.1080/10810730500526695.

[39] K.J. Aikin, K.R. Betts, K.S. Ziemer, A. Keisler, Consumer tradeoff of advertising claim versus efficacy information in direct-to-consumer prescription drug ads, Res. Soc. Adm. Pharm. 15 (12) (2019) 1484–1488, https://doi.org/10.1016/j.sapharm.2019.01.012.

[40] J.P. Shimshack, M.B. Ward, Mercury advisories and household health trade-offs, J. Health Econ. 29 (5) (2010) 674–685, https://doi.org/10.1016/j.jhealeco.2010.05.001.

[41] G. Torkzadeh, G. Dhillon, Measuring factors that influence the success of Internet commerce, Inf. Syst. Res. 13 (2) (2002) 187–204, https://doi.org/10.1287/isre.13.2.187.87.

[42] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, MIS Q. 20 (2) (1996) 167–196, https://doi.org/10.2307/249477.

[43] V.H. Vroom, Work and Motivation, Wiley & Sons, New York, NY, 1964.

[44] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Inf. Syst. Res. 17 (1) (2006) 61–80, https://doi.org/10.1287/isre.1060.0080.

[45] L. Wang, J. Yan, J. Lin, W. Cui, Let the users tell the truth: self-disclosure intention and self-disclosure honesty in mobile social networking, Int. J. Inf. Manag. 37 (1) (2017) 1428–1440, https://doi.org/10.1016/j.ijinfomgt.2016.10.006.

[46] H.W. Kim, H.C. Chan, S. Gupta, Value-based adoption of mobile internet: an empirical investigation, Decis. Support Syst. 43 (1) (2007) 111–126, https://doi.org/10.1016/j.dss.2005.05.009.

[47] J.N. Sheth, B.I. Newman, B.L. Gross, Consumption Values and Market Choices: Theory and Applications, Southwestern Publishing, Cincinnati, OH, 1991.

[48] R. Thaler, Mental accounting and consumer choice, Market. Sci. 4 (3) (1985) 199–214, https://doi.org/10.1287/mksc.4.3.199.

[49] T.Z. Chang, A.R. Wildt, Price, product information, and purchase intention: an empirical study, J. Acad. Market. Sci. 22 (1) (1994) 16–27, https://doi.org/10.1177/0092070394221002.

[50] D. Grewal, K.B. Monroe, R. Krishnan, The effects of price-comparison advertising on buyers' perceptions of acquisition value, transaction value, and behavioral intentions, J. Market. 62 (2) (1998) 46–59, https://doi.org/10.1177/002224299806200204.

[51] J.F. Petrick, Development of a multi-dimensional scale for measuring the perceived value of a service, J. Leisure Res. 34 (2) (2002) 119–134, https://doi.org/10.1080/00222216.2002.11949965.

[52] Z. Chen, A.J. Dubinsky, A conceptual model of perceived customer value in e commerce: a preliminary investigation, Psychol. Market. 20 (4) (2003) 323–347, https://doi.org/10.1002/mar.10076.

[53] N. Chung, C. Koo, The use of social media in travel information search, Telematics Inf. 32 (2) (2015) 215–229, https://doi.org/10.1016/j.tele.2014.08.005.

[54] V. Mitchell, Consumer perceived risk: conceptualisations and models, Eur. J. Market. 33 (1/2) (1999) 163–195, https://doi.org/10.1108/03090569910249229.

[55] N. Kogan, M.A. Wallach, Risk-taking: A Study in Cognition and Personality, Holt, Rhinehart & Winston, New York, NY, 1964.

[56] D. Krewski, L. Lemyre, M.C. Turner, J.E. Lee, C. Dallaire, L. Bouchard, P. Mercier, Public perception of population health risks in Canada: health hazards and sources of information, Human and ecological risk assessment 12 (4) (2006) 626–644, https://doi.org/10.1080/10807030600561832.

[57] A. Leppin, A.R. Aro, Risk perceptions related to SARS and avian influenza: theoretical foundations of current empirical research, Int. J. Behav. Med. 16 (1) (2009) 7–29, https://doi.org/10.1007/s12529-008-9002-8.

[58] N.T. Brewer, N.D. Weinstein, C.L. Cuite, J.E. Herrington, Risk perceptions and their relation to risk behavior, Ann. Behav. Med. 27 (2) (2004) 125–130, https://doi.org/10.1037/0278-6133.26.2.136.

[59] S. Milne, P. Sheeran, S. Orbell, Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory, J. Appl. Soc. Psychol. 30 (1) (2000) 106–143, https://doi.org/10.1111/j.1559-1816.2000.tb02308.x.

[60] A.S. Ahadzadeh, S.P. Sharif, F.S. Ong, Online health information seeking among women: the moderating role of health consciousness, Online Inf. Rev. 42 (1) (2018) 58–72, https://doi.org/10.1108/OIR-02-2016-0066.

[61] S.E. Hampson, J.A. Andrews, M. Barckley, E. Lichtenstein, M.E. Lee, Conscientiousness, perceived risk, and risk-reduction behaviors: a preliminary study, Health Psychol. 19 (5) (2000) 496, https://doi.org/10.1037/0278-6133.19.5.496.

[62] C.O. Gregory, H.M. Blanck, C. Gillespie, L.M. Maynard, M.K. Serdula, Perceived health risk of excess body weight among overweight and obese men and women: differences by sex, Prev. Med. 47 (1) (2008) 46–52, https://doi.org/10.1016/j.ypmed.2008.01.008.

[63] G.M. Leung, T.H. Lam, L.M. Ho, S.Y. Ho, B.H.Y. Chan, I.O.L. Wong, A.J. Hedley, The impact of community psychological responses on outbreak control for severe acute respiratory syndrome in Hong Kong, J. Epidemiol. Community 57 (11) (2003) 857–863, https://doi.org/10.1136/jech.57.11.857.

[64] W. Yoo, D.H. Choi, Predictors of expressing and receiving information on social networking sites during MERS-CoV outbreak in South Korea, J. Risk Res. (2019) 1–16, https://doi.org/10.1080/13669877.2019.1569105.

[65] S. Dryhurst, C.R. Schneider, J. Kerr, A.L. Freeman, G. Recchia, A.M. Van Der Bles, S. van der Linden, Risk perceptions of COVID-19 around the world, J. Risk Res. 23 (7–8) (2020) 994–1006, https://doi.org/10.1080/13669877.2020.1758193.

[66] M. Abdelrahman, Personality traits, risk perception, and protective behaviors of Arab residents of Qatar during the COVID-19 pandemic, Int. J. Ment. Health Addiction (2020) 1–12, https://doi.org/10.1007/s11469-020-00352-7.

[67] C.C. Sreelakshmi, S.K. Prathap, Continuance adoption of mobile-based payments in Covid-19 context: an integrated framework of health belief model and expectation confirmation model, Int. J. Pervasive Comput. Commun. 16 (4) (2020) 351–369, https://doi.org/10.1108/IJPCC-06-2020-0069.

[68] Y. Zhao, Q. Ni, R. Zhou, What factors influence the mobile health service adoption? A meta-analysis and the moderating role of age, Int. J. Inf. Manag. 43 (2018) 342–350, https://doi.org/10.1016/j.ijinfomgt.2017.08.006.

[69] H. Xu, T. Dinev, H.J. Smith, P. Hart, Examining the formation of individual's privacy concerns: toward an integrative view, in: The 29th International Conference on Information Systems, Paris, France, 2008.

[70] C.L. Miltgen, A. Popovič, T. Oliveira, Determinants of end-user acceptance of biometrics: integrating the "Big 3" of technology acceptance with privacy context, Decis. Support Syst. 56 (2013) 103–114, https://doi.org/10.1016/j.dss.2013.05.010.

[71] Z. Deng, Z. Hong, C. Ren, W. Zhang, F. Xiang, What predicts patients' adoption intention toward mHealth services in China: empirical study, JMIR mHealth and uHealth 6 (8) (2018) e172, https://doi.org/10.2196/mhealth.9316.

[72] Z. Jiang, C.S. Heng, B.C. Choi, Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions, Inf. Syst. Res. 24 (3) (2013) 579–595, https://doi.org/10.1287/isre.1120.0441.

[73] W. Edwards, The theory of decision making, Psychol. Bull. 51 (4) (1954) 380, https://doi.org/10.1037/h0053870.

[74] P. Slovic, B. Fischhoff, S. Lichtenstein, Behavioral Decision Theory Perspectives on Protective Behavior, Cambridge University, 1987.

[75] S. Min, K.K.F. So, M. Jeong, Consumer adoption of the Uber mobile application: insights from diffusion of innovation theory and technology acceptance model, J. Trav. Tourism Market. 36 (7) (2019) 770–783, https://doi.org/10.1080/10548408.2018.1507866.

[76] T. Zhang, C. Lu, M. Kizildag, Banking "on-the-go": examining consumers' adoption of mobile banking services, International Journal of Quality and Service Sciences 10 (3) (2018) 279–295, https://doi.org/10.1108/IJQSS-07-2017-0067.

[77] S.J. Chang, A. Van Witteloostuijn, L. Eden, From the editors: common method variance in international business research, J. Int. Bus. Stud. 41 (2010) 178–184, https://doi.org/10.1057/jibs.2009.88.

[78] J. Kees, C. Berry, S. Burton, K. Sheehan, An analysis of data quality: professional panels, student subject pools, and Amazon's Mechanical Turk, J. Advert. 46 (1) (2017) 141–155, https://doi.org/10.1080/00913367.2016.1269304.

[79] N.T. Brewer, G.B. Chapman, F.X. Gibbons, M. Gerrard, K.D. McCaul, N. D. Weinstein, Meta-analysis of the relationship between risk perception and health behavior: the example of vaccination, Health Psychol. 26 (2) (2007) 136, https://doi.org/10.1037/0278-6133.26.2.136.

[80] H. Xu, X.R. Luo, J.M. Carroll, M.B. Rosson, The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing, Decis. Support Syst. 51 (1) (2011) 42–52, https://doi.org/10.1016/j.dss.2010.11.017.

[81] J.F. Hair, M. Sarstedt, C.M. Ringle, S.P. Gudergan, Advanced Issues in Partial Least Squares Structural Equation Modeling (PLS-SEM), Sage, Thousand Oaks, CA, 2017.

[82] J. Henseler, C.M. Ringle, M. Sarstedt, A new criterion for assessing discriminant validity in variance-based structural equation modeling, J. Acad. Market. Sci. 43 (1) (2015) 115–135, https://doi.org/10.1007/s11747-014-0403-8.

[83] N. Kock, Common method bias in PLS-SEM: a full collinearity assessment approach, Int. J. e-Collaboration 11 (4) (2015) 1–10, https://doi.org/10.4018/ijec.2015100101.

[84] D. Gefen, E.E. Rigdon, D. Straub, 's comments: an update and extension to SEM guidelines for administrative and social science research, MIS Q. 35 (2) (2011), https://doi.org/10.2307/23044042 iii-xiv.

[85] W.W. Chin, The partial least squares approach to structural equation modeling, Modern Methods for Business Research 295 (2) (1998) 295–336.

[86] J.F. Hair, M. Sarstedt, C.M. Ringle, J.A. Mena, An assessment of the use of partial least squares structural equation modeling in marketing research, J. Acad. Market. Sci. 40 (3) (2012) 414–433, https://doi.org/10.1007/s11747-011-0261-6.

[87] C. Nitzl, J.L. Roldan, G. Cepeda, Mediation analysis in partial least squares path modeling, Ind. Manag. Data Syst. 116 (9) (2016) 1849–1864, https://doi.org/10.1108/IMDS-07-2015-0302.

[88] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, Academic press, 2013.

[89] J. Henseler, C.M. Ringle, R.R. Sinkovics, The use of partial least squares path modeling in international marketing, in: New Challenges to International Marketing, Emerald Group Publishing Limited, 2009.

[90] P. Duarte, J.C. Pinho, A mixed methods UTAUT2-based approach to assess mobile health adoption, J. Bus. Res. 102 (2019) 140–150, https://doi.org/10.1016/j.jbusres.2019.05.022.

[91] T.T. Nguyen, T.C.A.H. Nguyen, C.D. Tran, Exploring individuals' adoption of COVID-19 contact-tracing apps: a mixed-methods approach, Libr. Hi Tech (2021), https://doi.org/10.1108/LHT-06-2021-0180. In press.

[92] J.L. Jiao, X.L. Zhang, Y.S. Tang, What factors determine the survival of green innovative enterprises in China?–A method based on fsQCA, Technol. Soc. 62 (2020) 101314, https://doi.org/10.1016/j.techsoc.2020.101314.

[93] A.G. Woodside, A. Schpektor, X. Xia, Triple sense-making of findings from marketing experiments using the dominant variable based-logic, case-based logic, and isomorphic modeling, Int. J. Bus. Econ. 12 (2) (2013) 131–153.

[94] M.T. Phung, P.T.M. Ly, T.T. Nguyen, The effect of authenticity perceptions and brand equity on brand choice intention, J. Bus. Res. 101 (2019) 726–736, https://doi.org/10.1016/j.jbusres.2019.01.002.

[95] C.C. Ragin, Redesigning Social Inquiry: Fuzzy Sets and beyond, University of Chicago Press, Chicago, 2008.

[96] T.D.H. Thai, T. Wang, Investigating the effect of social endorsement on customer brand relationships by using statistical analysis and fuzzy set qualitative comparative analysis (fsQCA), Comput. Hum. Behav. 113 (2020) 106499, https://doi.org/10.1016/j.chb.2020.106499.

[97] I.O. Pappas, P.E. Kourouthanassis, M.N. Giannakos, V. Chrissikopoulos, Explaining online shopping behavior with fsQCA: the role of cognitive and affective perceptions, J. Bus. Res. 69 (2) (2016) 794–803.

[98] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, Q. Zhu, Health information privacy concerns, antecedents, and information disclosure intention in online health communities, Inf. Manag. 55 (4) (2018) 482–493, https://doi.org/10.1016/j.im.2017.11.003.

[99] J. Cho, The impact of post-adoption beliefs on the continued use of health apps, Int. J. Med. Inf. 87 (2016) 75–83, https://doi.org/10.1016/j.ijmedinf.2015.12.016.

[100] H. Li, J. Wu, Y. Gao, Y. Shi, Examining individuals' adoption of healthcare wearable devices: an empirical study from privacy calculus perspective, Int. J. Med. Inf. 88 (2016) 8–17, https://doi.org/10.1016/j.ijmedinf.2015.12.010.

[101] M.T. Phung, P.T.M. Ly, T.T. Nguyen, N. Nguyen-Thanh, An FsQCA investigation of eWOM and social influence on product adoption intention, J. Promot. Manag. 26 (5) (2020) 726–747, https://doi.org/10.1080/10496491.2020.1729318.

[102] K.H. Huarng, Qualitative analysis with structural associations, J. Bus. Res. 69 (11) (2016) 5187–5191, https://doi.org/10.1016/j.jbusres.2016.04.110.

[103] C. Pagliari, The ethics and value of contact tracing apps: international insights and implications for Scotland's COVID-19 response, Journal of Global Health 10 (2) (2020), https://doi.org/10.7189/jogh.10.020103.

[104] M. Lanzing, Contact tracing apps: an ethical roadmap, Ethics Inf. Technol. (2020) 1–4, https://doi.org/10.1007/s10676-020-09548-w.

[105] S.N. Williams, C.J. Armitage, T. Tampe, K. Dienes, Public attitudes towards COVID-19 contact tracing apps: a UK-based focus group study, Health Expect. 24 (2) (2021) 377–385, https://doi.org/10.1111/hex.13179.

[106] T. Li, C. Faklaris, J. King, Y. Agarwal, L. Dabbish, J.I. Hong, Decentralized Is Not Risk-free: Understanding Public Perceptions of Privacy-Utility Trade-Offs in COVID-19 Contact-Tracing Apps, 2020 arXiv preprint arXiv:2005.11957.