Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective

Farkhondeh Hassandoust
Saeed Akhlaghpour
Allen C. Johnston

Citation of published version:
Hassandoust, F., Akhlaghpour, S., & Johnston, A. C. (2020). Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. In Journal of the American Medical Informatics Association (Vol. 28, Issue 3, pp. 463–471). Oxford University Press (OUP). https://doi.org/10.1093/jamia/ocaa240

Journal of the American Medical Informatics Association, 28(3), 2021, 463–471
doi: 10.1093/jamia/ocaa240
Advance Access Publication Date: 4 November 2020
Research and Applications

Research and Applications

Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective

Farkhondeh Hassandoust,[1] Saeed Akhlaghpour,[2] and Allen C. Johnston[3]

[1]Business Information Systems department, Auckland University of Technology, Auckland, New Zealand, [2]UQ Business School, The University of Queensland, Brisbane, Australia and [3]Department of Information Systems, Statistics and Management Science, Culverhouse College of Business, University of Alabama, Tuscaloosa, USA

Corresponding Author: Farkhondeh Hassandoust, Business Information Systems department, Auckland University of Technology, Auckland, New Zealand; fhassand@aut.ac.nz

Received 17 June 2020; Revised 25 July 2020; Editorial Decision 10 September 2020; Accepted 12 September 2020

ABSTRACT

Objective: The study sought to develop and empirically validate an integrative situational privacy calculus model for explaining potential users' privacy concerns and intention to install a contact tracing mobile application (CTMA).

Materials and Methods: A survey instrument was developed based on the extant literature in 2 research streams of technology adoption and privacy calculus. Survey participants (N = 853) were recruited from all 50 U.S. states. Partial least squares structural equation modeling was used to validate and test the model.

Results: Individuals' intention to install a CTMA is influenced by their risk beliefs, perceived individual and societal benefits to public health, privacy concerns, privacy protection initiatives (legal and technical protection), and technology features (anonymity and use of less sensitive data). We found only indirect relationships between trust in public health authorities and intention to install CTMA. Sex, education, media exposure, and past invasion of privacy did not have a significant relationship either, but interestingly, older people were slightly more inclined than younger people to install a CTMA.

Discussion: Our survey results confirm the initial concerns about the potentially low adoption rates of CTMA. Our model provides public health agencies with a validated list of factors influencing individuals' privacy concerns and beliefs, enabling them to systematically take actions to address these identified issues, and increase CTMA adoption.

Conclusions: Developing CTMAs and increasing their adoption is an ongoing challenge for public health systems and policymakers. This research provides an evidence-based and situation-specific model for a better understanding of this theoretically and pragmatically important phenomenon.

Key words: privacy concerns; situational privacy calculus; contact tracing application

INTRODUCTION

The nature and scale of the coronavirus disease 2019 (COVID-19) pandemic make digital tracing necessary for the mitigation of one of the most widespread and deadly pandemics the world has ever seen. Between April and June 2020, several countries, including Australia, India, and the United Kingdom, rolled out official contact tracing mobile applications (CTMAs). There are also other countries, most notably Brazil and the USA, as well as several technology vendors, in-

cluding Google and Apple in a joint effort, that have expressed their intentions to release COVID-19 contact tracing technologies.[1] As an example of the critical applications of public health informatics in the system response to COVID-19,[2] the purpose of a CTMA is to automate the laborious process of contact tracing, in which public health authorities (PHAs) seek to control the spread of COVID-19 by identifying people who have been in contact with an infected person and then providing users with information regarding testing and self-quarantine. CTMAs can provide healthcare workers and government officials with data necessary not only to flatten the curve of infections and hospitalizations, but to also understand the spread of the virus—an important insight for mitigating future viral outbreaks. Nevertheless, it is not clear how well adopted the CTMAs will be.

Given the recent privacy-loss events involving mobile apps and geolocation services,[3] privacy advocates have elevated their message, including warning citizens about the dangers associated with apps designed to aid in the fight against COVID-19.[4,5] These warnings, combined with the general desire for privacy shared by most mobile users, jeopardize the efficacy of CTMAs—but how, and to what extent? Convincing individuals to participate and install these applications is a hurdle for PHAs and tech providers (eg, Apple, Google). Individuals must install one of these applications to become part of the system. Computer modeling by the University of Oxford showed that a CTMA could be effective in combating the spread of COVID-19, if nearly 60% of the population installed and used it (Wright, 2020[6]). However, many individuals may not adopt the applications because of privacy concerns - Singapore's contact tracing app was reportedly adopted by only 10%-20% of the population,[7] and despite the initial enthusiasm and 40% download target, as of June 2020, the COVIDSafe app had been adopted only by around 25% of Australians.[8] Low adoption rates will inevitably erode the value of the system.[9]

Extensive research has been conducted on the adoption of information technologies (ITs), and various influencing factors have been investigated in this decision process.[10,11] Researchers have examined individuals' attitudes, beliefs, perceptions, effort and performance expectancies, and social influence related to adoption in various healthcare contexts.[12–14] However, despite their importance, especially in the context of public health systems, the role of privacy concerns and perceived benefits (shared societal and individual benefits) have not received enough empirical attention in this research stream. This study aims to extend the existing literature and theoretical frameworks of information privacy in IT adoption by exploring the role of technological, legal, and social factors that affect privacy concerns, and perceptions of risks and benefits in the context of CTMA adoption. More specifically, we ask the following questions:

- Research Question 1: Do the perceived benefits (individual or societal benefits) that come from using CTMA alleviate individuals' concerns regarding the risk of using these apps?
- Research Question 2: Do individuals' information privacy concerns and their trust (or lack thereof) in PHAs influence their intention to install contact tracing apps?
- Research Question 3: Do technology features (sensitivity of collected information, and anonymity options) and privacy protection initiatives (technical and legal privacy protection measures) affect individuals' adoption decisions?

This study aims to answer these research questions by leveraging elements of situational privacy calculus theory and incorporating appropriate constructs and measures relevant to an individual's perspective when assessing potential CTMA installation.

Table 1. Demographic information of participants

Demographic information		Frequency	Percentage
Gender	Female	547	63.9
	Male	306	35.7
	Rather not say	3	0.4
Age	18-34 y	86	10
	25–34 y	116	13.6
	35–44 y	187	21.8
	45–54 y	141	16.5
	55–64 y	182	21.3
	≥65 y	144	16.8
Education	Some school, no degree	32	3.7
	High school graduate	179	20.9
	Some college, no degree	283	33.1
	Bachelor's degree	261	30.5
	Master's degree	60	7
	Professional degree	31	3.6
	Doctorate degree	10	1.2
State (we report on only the top 10 U.S. states in terms of frequency)	Florida	87	10.2
	California	66	7.7
	New York	61	7.1
	Texas	59	6.9
	Ohio	44	5.1
	Pennsylvania	43	5
	North Carolina	41	4.8
	New Jersey	30	3.5
	Georgia	27	3.2
	Virginia	27	3.2

SITUATIONAL PRIVACY CALCULUS

This privacy-related decision-making process is referred to as a privacy calculus[15] and has been studied extensively across a number of contexts, including mobile applications,[16] health care,[15,17] and e-commerce.[18] The privacy calculus perspective argues that individuals deliberately anticipate and weigh the privacy-related risks and benefits of information disclosure when they are faced with a situation that needs the provision of private information.[19–21] Within this literature, the conventional thought is that the privacy calculus is relatively stable, with similar risk–reward circumstances leading to similar privacy-related decision-making outcomes. However, more recently, the consensus among scholars is that privacy is situational and varies significantly from situation to situation.[22] Given the unprecedented circumstances presented by the COVID-19 pandemic, we believe that the contemporary, situational privacy calculus perspective is most appropriate for our study.

Based on this background, we apply and contextualize privacy calculus theory to understand the situational trade-off between privacy-related risks and benefits in the important and unique context of CTMA installation (related to COVID-19) and its potential shared benefits toward public health, thereby strengthening and contributing to our theoretical understanding of the privacy calculus' nomological network. A list of previous studies on privacy calculus centering on privacy concerns is presented in Supplementary Table 1.

RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

Our research model (Figure 1) is based on the privacy calculus theory, which suggests that both perceived benefits and potential risks affect

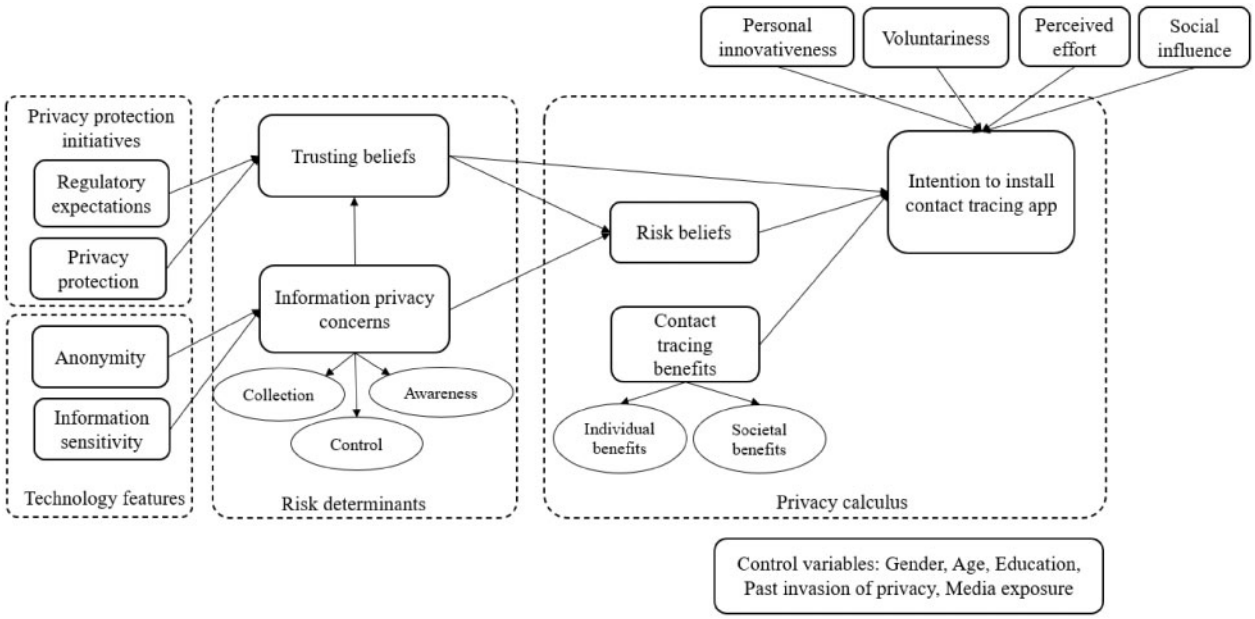

Figure 1. Proposed research model.

individual decisions. We complement this model by incorporating a large body of research on the adoption and use of technology—see Burton-Jones, Stein[10] for a review. Moreover, in line with calls for a paradigm shift in this stream,[11,23] we explicitly focus on contextualized theories and digital technology features to explain IT adoption.

In the CTMA context, measuring behavioral intention, as a proxy for actual behavior, is justified[24] because of the very limited rollout of CTMA in most of the countries. Populations in these countries have not yet faced the decision of whether to install a CTMA; therefore, one cannot yet identify their actual behavior about using a CTMA. In the following subsections, the research hypotheses are constructed around different theoretically and practically important constructs that directly or indirectly affect behavioral intention to install a CTMA.

Privacy calculus

In the privacy calculus theory, perceived privacy risk is the degree to which individuals believe there is a potential for loss associated with the release of personal information.[19,21] The other construct, perceived benefit, encompasses a wide range of financial and nonfinancial rewards in return for personal information.[25] Based on this distinction, we modeled perceived benefits as a second-order construct comprising individual benefits (eg, improving one's living and working efficiency and effectiveness) and societal benefits (eg, protecting the public health and lifting the restrictions on economic activities). In the context of CTMA, we expect these 2 types of benefits to be in alignment. The main source of conflict, however, is the trade-off between these benefits and CTMA privacy risks, such as government surveillance and misuse of personal data. This trade-off is the main determinant of the willingness or intent to provide personal information through a CTMA. Thus, following the well-established privacy calculus model, we hypothesize the following:

Hypothesis 1: Risk beliefs negatively influence individuals' intention to install CTMA.

Hypothesis 2: Perceived benefits positively influence individuals' intention to install CTMA.

Risk determinants

We define CTMA privacy concerns as individuals' perceptions of the consequences of sharing information through a CTMA.[19] Based on Malhotra et al's[21] model, privacy concerns impact trust and risk, which, in turn, shape the tendency to share personal information.[24] In the CTMA context, trusting beliefs refer to the degree to which individuals believe that the PHA releasing and controlling a CTMA is reliable in guarding their personal information collected through a CTMA.[26,27] Similarly, we define risk beliefs as perceptions that the release of personal information on a CTMA will expose it to potential data loss or misuse.[28] Drawing on this framework, we model CTMA information privacy concerns as having a positive effect on risk beliefs and a negative effect on trusting beliefs. Additionally, as individuals perceive a PHA controlling a CTMA as being trustworthy with their data, their beliefs about the risk associated with sharing contact tracing data with that PHA will dissipate. Finally, previous studies have shown that trusting beliefs directly affect behavioral intention to adopt technology.[29] Hence, we expect that the more individuals trust the PHA with their contact tracing data collected through a CTMA, the more likely they will be to adopt the app. Thus, we hypothesize the following:

Hypothesis 3: Information privacy concerns negatively influence individuals' trusting beliefs.

Hypothesis 4: Information privacy concerns positively influence individuals' risk beliefs.

Hypothesis 5: Trusting beliefs negatively influence individuals' risk beliefs.

Hypothesis 6: Trusting beliefs positively influence individuals' intention to install CTMA.

Privacy protection initiatives

We have integrated the most pertinent factors shown to influence the perception of trust, and proposed that trusting beliefs of individuals are a function of expected outcomes of privacy protection initiatives, namely legal influences (regulatory expectations), and privacy protections. Trust is an important aspect in any relationship,

in which the trustors cannot directly control the actions of the trustees (eg, PHAs), and as a result, there will be potential negative consequences if a party fails to deliver its promises.[30] Therefore, it is critical to investigate the determinants of trustors' beliefs.[31]

The regulatory affairs enforce the type of personal information that firms are allowed to collect from individuals, as well as the methods that stored personal information would be protected against misuse.[32] In a similar vein, privacy protection consists of technical practices and solutions that aim to protect online privacy.[33] Such privacy protection tools include privacy policy statements and the provision of privacy-enhancing mechanisms.[34] Trust can only exist if an individual believes that the trustees have the ability and initiatives to fulfill the promised services at the expected quality.[31] In the context of CTMA, if individuals believe that the trustees (PHAs) have appropriate protection privacy practices, as well as compliance with privacy regulations, they are more likely to trust in PHAs, in order to share their personal information. Thus, we hypothesize the following:

Hypothesis 7: Regulatory expectations positively affect CTMA individuals' trusting beliefs.

Hypothesis 8: Privacy protection positively affects CTMA individuals' trusting beliefs.

Technology features

We focus on 2 technology design choices, anonymity and information sensitivity, with impacts CTMA users' privacy concerns. Anonymity is defined as the ability to conceal an individual's real identity.[35] Anonymity, typically determined by technology features,[36] can lead to less fear of social disapproval, surveillance, and evaluation.[25,37] Similarly, in the context of a CTMA, we expect that if individuals believe they can interact with the system anonymously, they will have less concern for privacy.

The second technology feature in our model is the use of sensitive information in a CTMA. We adopt Dinev et al's[35] definition of information sensitivity as a personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent (ie, a CTMA). In general, sharing more sensitive information with mobile apps causes individuals to be more concerned, because if the shared information is disclosed to third parties, they must deal with potentially harmful consequences (eg, identity theft).[35] For example. when a mobile app requests access to the device's GPS location, individuals pay more attention before granting such permission.[38,39] Given the importance of anonymity and information sensitivity features, in Google and Apple's proposed contact tracing technology, users maintain full anonymity and do not need to register their personal information. Also, most of the proposed CTMAs use less sensitive (Bluetooth) proximity data as opposed to more sensitive (GPS location) data, despite the arguably higher precision and effectiveness of location data for contact tracing. Hence, we hypothesize:

Hypothesis 9: Anonymity negatively influences information privacy concerns.

Hypothesis 10: Information sensitivity positively influences information privacy concerns.

Technology adoption

In addition to privacy-related factors, we included in our model a set of constructs found to be powerful predictors of behavioral intention to adopt a technology. *Performance expectancy* is measured in our proposed situated privacy calculus model using the contextualized *perceived benefits* construct. Next, in line with Wang and Benbasat,[40] *effort expectancy* is labeled as *perceived effort* and the latter's measures are adapted. Given the importance of voluntariness of the adoption (vs. an adoption mandated by the government or workplace), we followed Moore & Benbasat's[41] seminal study and included *voluntariness* as a predictor of behavioral intention to install a CTMA. We also include *social influence* because, in situations that involve potentially adopting an emerging technology, consumers often rely on mimetic behavior and word of mouth to inform their decisions about whether to do so.[42,43] Finally, based on the context (experimenting with mobile apps), we included *personal innovativeness* with IT.[44] Hence, based on the extant body of literature, we hypothesize:

Hypothesis 11: Social influence positively influences individuals' intention to install CTMA.

Hypothesis 12: Personal innovativeness positively influences individuals' intention to install CTMA.

Hypothesis 13: Perceived effort negatively influences individuals' intention to install CTMA.

Hypothesis 14: Voluntariness negatively influences individuals' intention to install CTMA.

RESEARCH DESIGN

To the research model (Figure 1) and its hypothesized relationships, we conducted a field survey of the U.S. citizens who may or may not choose to install a CTMA on their smartphones. The respondents were provided with general information on how CTMAs work along with a schematic representation. The survey was distributed via Qualtrics, resulting in 1528 responses, of which 856 responses remained after a few filtering questions ensuring participants had not already installed a CTMA on their smartphones, an attention check, and the removal of incomplete responses.

We developed the survey using previously validated measurement items that were operationalized with multiitem scales. A 7-point Likert scale with anchors ranging from 1 (*strongly disagree*) to 7 (*strongly agree*) was used to measure all of these key constructs. All the constructs of the measurement model were first-order reflective constructs with the exception of privacy concerns and benefits, which were treated as reflective second-order constructs. Measurement items included a few reverse-coded items to address the negative/positive connotation and associated bias. A pretest and pilot study were conducted to examine the appropriateness of the survey scales on a sample of 45 individuals. Participant recruitment was achieved by utilizing the services of a market research company—a professional panel service—that directed respondent panel members to our web-based survey. The data were collected in the U.S. between May 4 and 7, 2020. The resulting measurement items are presented in Supplementary Table 2.

DATA ANALYSIS AND RESULTS

We used partial least squares structural equation modeling (PLS-SEM) through SmartPLS 3.0 software (SmartPLS, Palo Alto, CA) to assess the research model from a predictive perspective and used the latent variable scores in a follow-up analysis.[45]PLS-SEM is an appropriate approach for large complex models with many latent vari-

Table 2. Convergent validity testing

Construct	Item	Standard loading of each item	Cronbach's alpha (α)	Composite reliability	Average variance extracted
Anonymity	ANON1	0.875	0.927	0.953	0.871
	ANON2	0.963			
	ANON3	0.958			
Awareness	AWAR1	0.916	0.917	0.947	0.857
	AWAR2	0.934			
	AWAR3	0.927			
Collection	COLL1	0.909	0.945	0.961	0.860
	COLL2	0.904			
	COLL3	0.954			
	COLL4	0.940			
Control	CONT1	0.787	0.761	0.857	0.666
	CONT2	0.820			
	CONT3	0.840			
Information sensitivity	SENS1	0.887	0.877	0.924	0.802
	SENS2	0.917			
	SENS3	0.883			
Intention to install a CTMA	INT1	0.975	0.981	0.986	0.946
	INT2	0.982			
	INT3	0.982			
	INT4_R	0.951			
Perceived effort	PEFF1	0.940	0.939	0.961	0.891
	PEFF2	0.959			
	PEFF3	0.932			
Personal innovativeness	INNO1	0.862	0.841	0.901	0.752
	INNO2	0.840			
	INNO3	0.899			
Privacy protection	PRIP1	0.856	0.910	0.931	0.711
	PRIP2	0.944			
	PRIP3	0.813			
	PRIP4	0.894			
Regulatory expectations	REGU1	0.902	0.878	0.924	0.803
	REGU2	0.877			
	REGU3	0.908			
Risk beliefs	RISK1	0.937	0.962	0.971	0.868
	RISK2	0.926			
	RISK3	0.947			
	RISK4	0.930			
	RISK5_R	0.919			
Social influence	SOINF1	0.569	0.891[a]	0.933	0.822
	SOINF2	0.928			
	SOINF3	0.842			
	SOINF4	0.929			
Societal benefits	SOCB1	0.948	0.967	0.977	0.914
	SOCB2	0.957			
	SOCB3	0.964			
	SOCB4	0.954			
Trusting beliefs	TRUS1	0.910	0.956	0.966	0.850
	TRUS2	0.937			
	TRUS3	0.932			
	TRUS4	0.904			
	TRUS5	0.925			
Utilitarian benefits	UTIB1	0.903	0.937	0.953	0.801
	UTIB2	0.925			
	UTIB3	0.923			
	UTIB4	0.819			
	UTIB5	0.900			
Voluntariness	VOLU1	0.643	0.838	0.863	0.681
	VOLU2	0.731			
	VOLU3	0.976			
	VOLU4_R	0.706			

For internal consistency, the values of Cronbach's alpha and composite reliability should be between 0.7 and 0.95. The evaluation of these estimates indicated that all of the constructs were within acceptable thresholds. Convergent validity can be assessed through the evaluation of average variance extracted values that should be above 0.5 for each composite.[45]

[a]Cronbach's α, composite reliability, and average variance extracted were calculated after removing SOINF1 and VOLU1.

CTMA: contact tracing mobile application.

ables.[46] This study followed the state-of-the-art guidelines proposed by Hair et al[45] to assess measurement and structural models. The demographic descriptions of our sample of 853 individuals across 50 U.S. states are provided in Table 1.

Given the pragmatic importance of the dependent variable in this study, we report a histogram of the respondent's intention to install a CTMA. As evident in Figure 2, a large proportion (35%) of our sample expressed extremely low or very low levels of behavioral intention to install a CTMA.

Measurement model assessment

The reliability and validity of the measurement model were tested through the evaluation of loadings, internal consistency, convergent validity, and discriminant validity.[45] According to Hair et al,[45] all the items reported a loading greater than 0.708 except VOLU2 and SOINF1, which were subsequently removed from the measurement model. The assessment of internal consistency and convergent validity is presented in Table 2.

Discriminant validity was tested based on the newly introduced criterion for establishing discriminant validity in PLS-SEM known as the heterotrait-monotrait criterion.[45]Cross-loadings of the items and heterotrait-monotrait$_{0.85}$ tables are provided in Supplementary Tables 3, 4 and 5.

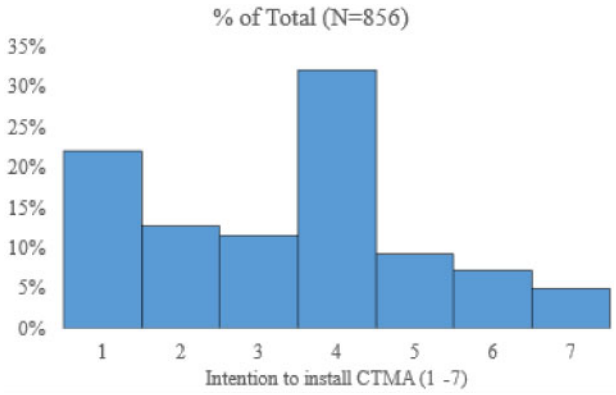

Figure 2. Histogram of the respondent's intention to install a contact tracing mobile application (CTMA).

Structural model assessment and hypothesis

Structural model evaluation includes evaluating collinearity among the exogenous constructs, examining the significance and relevance of path coefficients, and checking the model's predictive accuracy and relevance model.[45] The results of the structural model's evaluation are presented in Figure 3.

All hypotheses were supported, except for hypothesis 6, on the positive association between individuals' trusting beliefs and their intention to install a CTMA (path coefficient [β] = 0.052, $P = .113$). In terms of the explained variance provided by the research model, the privacy-related constructs (trust beliefs, risk beliefs, and benefits) and non–privacy-related constructs (personal innovativeness, voluntariness, perceived effort, and social influence) were able to explain 75% of the variance in individuals' intention to install a CTMA. The predictive relevance (Q^2) of intention to install a CTMA was obtained using a 2-stage approach with a value of 0.755, confirming the model had predictive relevance.[47] Overall, our extended model demonstrates strong explanatory power by explaining 75% of the variance in behavioral intention. It compares well with similar studies in other contexts. For example, Lazard et al's[13] and Or et al's[48] models explained 41% and 53.9% of the variance in behavioral intention to use patient portals and web-based self-management technologies, respectively.

Five control variables, namely age, sex, education, media exposure, and past invasion of privacy, were tested. Individuals' age had a positive significant relationship with their intention (β = 0.036, $P < .05$), indicating that older people are more inclined than younger people to install a CTMA. The remaining control variables had no significant relationships with the intention to install a CTMA. To reduce the potential for common method bias, we followed procedural guidelines established in the literature that are presented in Supplementary Table 5.

Post hoc analysis

We conducted multigroup analysis on age and sex to detect any significant differences in path coefficients of hypothesized relationships. The parametric test results indicate that there are significant differences in relationships between privacy concerns, trusting beliefs, and risk beliefs, as well as the relationship between voluntariness and intention among female and male groups. Findings indicate that female respondents are more worried about their privacy. In addition, the findings reveal the significant differences in relationships between anonymity and privacy concerns, as well as risk

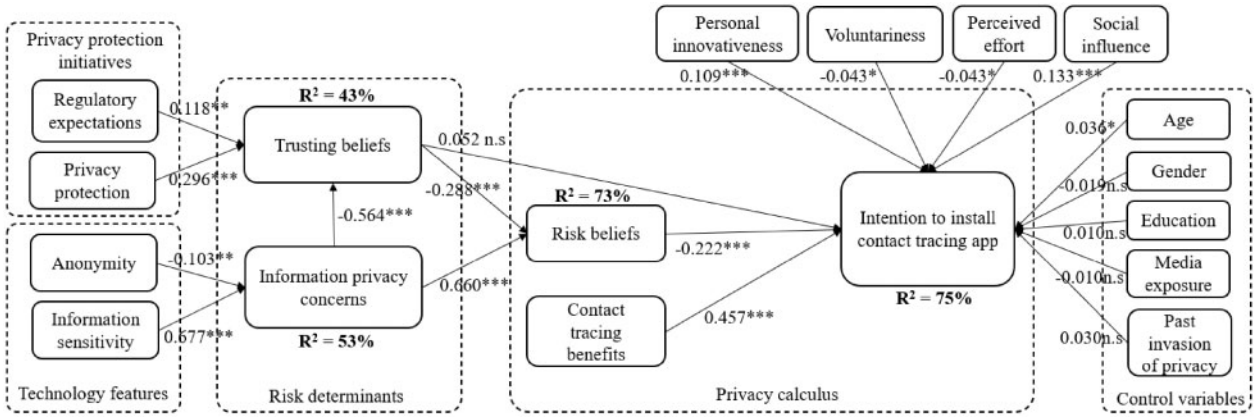

Figure 3. Structural model results. *$P < .05$, **$P < .01$, and ***$P < .001$. n.s: not significant.

beliefs, voluntariness, and intention to install a CTMA among younger and older respondents. The younger respondents are more concerned about their anonymity and voluntariness rights regarding CTMA installation. The results of post hoc analysis are presented in Supplementary Table 6.

DISCUSSION

Toward understanding the situational privacy calculus that individuals associate with the adoption of CTMAs in the fight to control the COVID-19 pandemic, we extended the existing privacy calculus models and found a range of individual, legal, and societal factors that carried weight. To the best of our knowledge, the previous studies[21,22,49,50] have not investigated the individual, legal, and social factors affecting individuals' intentions in an integrated framework. In terms of how the perceived benefits associated with CTMAs could help in limiting any risk potential adopters may also associate with the apps, we found that they had a significant mitigating impact. Previous researchers[22,49] have also discussed the situational trade-off of privacy-related risks and benefits and reported the significant role of perceived benefits in individuals' disclosure intention. This is likely the least surprising finding of this study in that it is consistent with the tenants of privacy calculus[49–51] yet it still tells us a lot about the situational thought process of CTMA adopters amid the COVID-19 pandemic. In this situation, there are clearly privacy risks being associated with the CTMAs, but their benefits are also clear and serve as a distinct motivation for intentions to install the CTMAs.

Interestingly, trust in PHAs was a significant factor in shaping the intentions of potential CTMA adopters to install the apps, but its influence was limited to the extent to which it was able to reduce the risks associated with the CTMAs. This tells us that PHAs have limits to what they can effectively promote. Constituents of PHAs are perhaps conditioned to expect information concerning their well-being and use it to help gauge their unique risk–benefit perspectives. This finding is in line with the findings of previous studies from various contexts that show that individuals' trusting beliefs play a critical role in shaping their risk beliefs.[21,24,52] However, our findings suggest that PHAs should develop trust among their constituents, not to motivate CTMA adoption, but rather to aid in the reduction of risk that they may associate with the apps. Any intentions for CTMA installation that individuals gain for the apps will be formed as an indirect consequence of such risk reduction.

This study's findings also suggest that the information privacy concerns and trusting beliefs potential CTMA adopters have in their PHAs are direct products of the technology features of the CTMAs and the privacy protection initiatives of the authorities, respectively. In terms of trusting beliefs, the strongest influence was from perceptions of privacy protection. Similar to the findings of previous research,[21,24,52] we found that as an individual's feeling that their privacy will be protected increases, so too does their trust in the PHA's ability to handle their sensitive personal data. This likely helps explain why information sensitivity was by far the most important determinant of information privacy concerns. As the sensitivity of the information provided to a CTMA increases, so too does a potential CTMA adopter's concern for its privacy. It has also been widely recognized in the literature that the type of information collected and used by third parties affects the level of individuals' perceived discomfort and privacy concerns.[21,34,35,50] Perhaps most interesting is the direct positive influence that regulatory expectations had on trusting beliefs. Prior research has also suggested that the implementation of privacy regulations helps to directly or indirectly increase individuals' trust and reduce their privacy concerns.[34,35]

IMPLICATIONS FOR RESEARCH AND PRACTICE

This research contributes to our understanding of determinants of privacy in crisis-driven situations, such as the current COVID-19 pandemic. Opportunities to explore and test models specific to privacy calculi in times of dire circumstances are rare, and this study provides a unique, timely perspective for understanding privacy as a situation-specific phenomenon; a perspective that has not yet been fully embraced within the academic community. Indeed, rather than approaching privacy as a stable, global concern, our findings point to a more specific, situational calculus that encompasses the influence of an individual, legal, and societal nature.

In times of crisis, we find an IT adoption privacy calculus that is focused on the agencies that seek to provide guidance and support for the public well-being through their recommendations for the adoption of a particular technology; yet, within this calculus, a premium is placed on how well the agencies are able to alleviate the risks associated with their adoption recommendations. The implications of this to researchers are that the technological features of a tool designed for public consumption are as important as ever, but how the public agencies that promote its use are able to gain the trust of their constituents is paramount to its adoption. Scholars should, therefore, extend their focus to include environmental factors, such as social influence, regulatory pressures, and previous experiences with privacy loss that underlie the technology adoption and appropriately weigh their influence.

The findings of this study also contribute to explaining the range of individuals' decisions in adopting CTMA. These decisions result mainly in shared public health benefits rather than individual benefits. The findings of this study also provide public health agencies with a validated list of factors influencing individuals' privacy concerns and beliefs, enabling them to systematically take action to address these identified issues. For example, our results confirmed the importance of regulatory protection expectations by individuals in shaping their CTMA adoption decision. This finding reaffirms the importance of the recently proposed U.S. bill to regulate CTMA to protect privacy.[53] A similar law was also passed in Australia, where strict penalties of up to 5 years of jail are established for those who collect, use, disclose, or decrypt CTMA data for any purpose other than contact tracing.

CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH

In this study, we contextualized and validated privacy calculus theory in the context of an adoption decision of an emerging technology (CTMA) that presents unique privacy concerns to individuals in a pandemic. Our model provided an empirical analysis of the role of technology features, privacy protection initiatives, privacy concerns, risk beliefs, and individual and shared benefits in bringing about individuals' intention to install a CTMA. The results of this study provide strong support for the influence of risk beliefs and benefits on individuals' intention to install a CTMA but not a strong support for a direct impact of trust beliefs on individuals' intention.

A limitation of this research is its orientation at a single point in time. Owing to the progressive nature of the COVID-19 pandemic

and our interest in conducting this research at the time of the introduction of COVID-19 CTMAs, we were not able to test how the progression of a treatment or vaccine would influence the adoption intentions or if the adoption decisions are market-driven. As the global and local economies start to recover, would people be more or less inclined to adopt CTMAs, and what economic factors would they look to in helping form that decision? These are all time-related insights that this study was unable to pursue but that future researchers should consider. The World Health Organization has referred to contact tracing as "the backbone of the response."[54] The adoption of CTMAs is no silver bullet to defeat COVID-19 but can have consequential importance in a country's public health response along with measures such as testing and isolating.[55]

AUTHOR CONTRIBUTIONS

FH conceived of and designed the project and was responsible for data acquisition, analysis, interpretation, and writing. SA contributed to model development, research design, data acquisition, writing, and editing. ACJ made contributions to theoretical development, data interpretation, contribution writing, and editing. All authors made substantial contributions to the revision and gave approval for the final version of the manuscript to be published and agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

SUPPLEMENTARY MATERIAL

Supplementary material is available at *Journal of the American Medical Informatics Association* online.

CONFLICT OF INTEREST STATEMENT

The authors have no competing interests to declare.

REFERENCES

1. O'Neill PH, Ryan-Mosley T, Johnson B. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. 2020. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/ Accessed May, 20, 2020.
2. Bakken S. Informatics is a critical strategy in combating the COVID-19 pandemic. *J Am Med Inform Assoc* 2020; 27 (6): 843–4.
3. Valentino-DeVries J, Singer N, Keller MH, Krolik A. Your apps know where you were last night, and they're not keeping it secret. *The New York Times*. 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html Accessed May, 25, 2020.
4. Timberg C, Harwell D. Government efforts to track virus through phone location data complicated by privacy concerns. *Washington Post*. 2020. https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/ Accessed May, 26, 2020.
5. Harari YN. The world after coronavirus. *Financial Times*. 2020. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 Accessed May, 26, 2020.
6. Wright O, Smyth C. Coronavirus. Virtual city built in anOxford University lab shows how the tracing app could work. The Times. 2020. https://www.thetimes.co.uk/article/coronavirus-virtual-city-built-in-an-oxford-university-lab-shows-how-the-tracing-app-could-work-mh8wnc3cc Accessed May, 17, 2020.
7. Coronavirus: EU and Australian tracing apps 'ready in weeks'. *BBC News*. 2020. https://www.bbc.com/news/technology-52325352 Accessed May, 25, 2020.
8. Meixner S. How many people have downloaded the COVIDSafe app and how central has it been to Australia's coronavirus response? *ABC News*. 2020. https://www.abc.net.au/news/2020-06-02/coronavirus-covid19-covidsafe-app-how-many-downloads-greg-hunt/12295130 Accessed May, 25, 2020.
9. Fussell S, Knight W. The Apple-Google contact tracing plan won't stop Covid alone. *Wired*. 2020. https://www.wired.com/story/apple-google-contact-tracing-wont-stop-covid-alone/ Accessed May, 10, 2020.
10. Burton-Jones A, Stein M-K, Mishra A. IS use.*MIS Q* Research Curations. https://static1.squarespace.com/static/5887a660b3db2b05bd09cf36/t/5deff92d8594a9745b923257/1576007981510/IS-Use-Curation-Final-Nov27.pdf Accessed June, 5, 2020.
11. Venkatesh V, Thong JY, Xu X. Unified theory of acceptance and use of technology: A synthesis and the road ahead. *J Assoc Inform Syst* 2016; 17 (5): 328–76.
12. Casillas A, Perez-Aguilar G, Abhat A, *et al*. Su salud a la mano (your health at hand): patient perceptions about a bilingual patient portal in the Los Angeles safety net. *J Am Med Inform Assoc* 2019; 26 (12): 1525–35.
13. Lazard AJ, Watkins I, Mackert MS, *et al*. Design simplicity influences patient portal use: the role of aesthetic evaluations for technology acceptance. *J Am Med Inform Assoc* 2016; 23 (e1): e157–61.
14. Holahan PJ, Lesselroth BJ, Adams K, *et al*. Beyond technology acceptance to effective technology use: a parsimonious and actionable model. *J Am Med Inform Assoc* 2015; 22 (3): 718–29.
15. Anderson CL, Agarwal R. The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Inform Syst Res* 2011; 22 (3): 469–90.
16. Keith MJ, Thompson SC, Hale J, *et al*. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *Int J Hum Comput Stud* 2013; 71 (12): 1163–73.
17. Singh T, Johnston A, Di Gangi P, Bott, G. An examination of risk perceptions and protected health information disclosure intentions: a construal level theory perspective. In: proceedings of the 2018 Americas Conference on Information Systems (AMCIS); August 16–18, 2018: New Orleans, LA.
18. Dinev T, Bellotto M, Hart P, *et al*. Privacy calculus model in e-commerce–a study of Italy and the United States. *Eur J Inform Syst* 2006; 15 (4): 389–402.
19. Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. *Inform Syst Res* 2006; 17 (1): 61–80.
20. Culnan MJ, Armstrong PK. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Sci* 1999; 10 (1): 104–15.
21. Malhotra NK, Kim SS, Agarwal J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inform Syst Res* 2004; 15 (4): 336–55.
22. Kehr F, Wentzel D, Kowatsch T, Fleisch E. Rethinking privacy decisions: pre-existing attitudes, pre-existing emotional states, and a situational privacy calculus. In: proceedings of the European Conference on Information Systems 2015; 2015: paper 95.
23. Akhlaghpour S, Wu J, Lapointe L, *et al*. The ongoing quest for the IT artifact: Looking back, moving forward. *J Inform Technol* 2013; 28 (2): 150–66.
24. Warkentin M, Goel S, Menard P. Shared benefits and information privacy: what determines smart meter technology adoption? *J Assoc Inform Sci* 2017; 18 (11): 758–86.
25. Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. *MIS Q* 2011; 35 (4): 989–1016.
26. Gefen D, Karahanna E, Straub DW. Trust and TAM in online shopping: an integrated model. *MIS Q* 2003; 27 (1): 51–90.
27. Grazioli S, Jarvenpaa SL. Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Trans Syst Man Cybern A* 2000; 30 (4): 395–410.
28. Dowling GR, Staelin R. A model of perceived risk and intended risk-handling activity. *J Consum Res* 1994; 21 (1): 119–34.
29. Jarvenpaa SL, Tractinsky N, Vitale M. Consumer trust in an Internet store. *Inform Technol Manag* 2000; 1 (1/2): 45–71.

30. Mayer RC, Davis JH, Schoorman FD. An integrative model of organizational trust. *Acad Manag Rev* 1995; 20 (3): 709–34.
31. Jarvenpaa SL, Tractinsky N, Saarinen L. Consumer trust in an Internet store: a cross-cultural validation. *J Comput Mediat Commun* 1999; 5 (2): JCMC526.
32. Swire P. Markets, self-regulation, and government enforcement in the protection of personal information. In: Privacy and Self-Regulation in the Information Age by the US Department of Commerce. In: *Privacy and Self-Regulation in the Information Age*. Washington, DC: U.S. Department of Commerce; 1997.
33. Culnan MJ, Bies RJ. Consumer privacy: Balancing economic and justice considerations. *J Social Issues* 2003; 59 (2): 323–42.
34. Hong W, Chan FK, Thong JY. Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. *J Bus Ethics* 2019 Jun 17 [E-pub ahead of print].
35. Dinev T, Xu H, Smith JH, *et al*. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *Eur J Inform Syst* 2013; 22 (3): 295–316.
36. Qian H, Scott CR. Anonymity and self-disclosure on weblogs. *J Comput Mediat Commun* 2007; 12 (4): 1428–1451.
37. Pinsonneault A, Heppel N. Anonymity in group support systems research: A new conceptualization, measure, and contingency framework. *J Manag Inform Syst* 1997; 14 (3): 89–108.
38. Xu H, Teo H-H, Tan BCY, *et al*. The role of push-pull technology in privacy calculus: the case of location-based services. *J Manag Inform Syst* 2009; 26 (3): 135–174.
39. Keith M, Babb J, Furner C, *et al*. Limited information and quick decisions: consumer privacy calculus for mobile applications. *THCI* 2016; 8 (3): 88–130.
40. Wang W, Benbasat I. Interactive decision aids for consumer decision making in e-commerce: The influence of perceived strategy restrictiveness. *MIS Q* 2009; 33 (2): 293–320.
41. Moore GC, Benbasat I. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Inform Syst Res* 1991; 2 (3): 192–222.
42. Akhlaghpour S, Lapointe L. From placebo to panacea: studying the diffusion of IT management techniques with ambiguous efficiencies: the case of capability maturity model. *J Assoc Inform Syst* 2018; 19 (6): 441–502.
43. Fichman RG. The diffusion and assimilation of information technology innovations. *Framing Domains IT Manag Project Fut Past* 2000; 105127: 105–28.
44. Hong W, Thong JYL, Chasalow LC, *et al*. User acceptance of agile information systems: A model and empirical test. *J Manag Inform Syst* 2011; 28 (1): 235–72.
45. Hair JF, Risher JJ, Sarstedt M, *et al*. When to use and how to report the results of PLS-SEM. *Eur Bus Rev* 2019; 31 (1): 2–24.
46. Henseler J, Ringle CM, Sinkovics RR. The use of partial least squares path modeling in international marketing. In: Sinkovics RR, Ghauri PN, eds. *New Challenges to International Marketing*. Melbourne, Australia: Emerald Group; 2009: 277–319.
47. Chin WW, Dibbern J. An introduction to a permutation based procedure for multi-group PLS analysis: Results of tests of differences on simulated data and a cross cultural analysis of the sourcing of information system services between Germany and the USA. In: Vinzi VE, Chin WY, Henseler J, Wang H, eds. *Handbook of Partial Least Squares*. New York, NY: Springer; 2010: 171–93.
48. Or CKL, Karsh B-T, Severtson DJ, *et al*. Factors affecting home care patients' acceptance of a web-based interactive self-management technology. *J Am Med Inform Assoc* 2011; 18 (1): 51–9.
49. Sun Y, Wang N, Shen X-L, *et al*. Location information disclosure in location-based social network services: privacy calculus, benefit structure, and gender differences. *Comput Hum Behav* 2015; 52: 278–92.
50. Li H, Wu J, Gao Y, *et al*. Examining individuals' adoption of healthcare wearable devices: an empirical study from privacy calculus perspective. *Int J Med Inform* 2016; 88: 8–17.
51. Li H, Sarathy R, Xu H. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decis Support Syst* 2011; 51 (3): 434–45.
52. Slyke C, Shim JT, Johnson R, *et al*. Concern for information privacy and online consumer purchasing. *J Assoc Inform Sci* 2006; 7 (6): 415–44.
53. Johnson B. The US's draft law on contact tracing apps is a step behind Apple and Google. *MIT Technology Review*. 2020. https://www.technologyreview.com/2020/06/02/1002491/us-covid-19-contact-tracing-privacy-law-apple-google/ Accessed June, 5, 2020.
54. World Health Organization. WHO Director-General's opening remarks at the media briefing on COVID-19 - 16 March 2020. 2020. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—16-march-2020 Accessed May, 21, 2020.
55. Bakken S. Doing what matters most. *J Am Med Inform Assoc* 2019; 26 (1): 1–2.