Digital Health Innovation: Exploring Adoption of COVID-19 Digital Contact Tracing Apps

ABSTRACT

With the outbreak of COVID-19, contact tracing is becoming a used intervention to control the spread of this highly infectious disease. This study explores an individual's intention to adopt COVID-19 Digital Contact Tracing (DCT) apps. A conceptual framework developed for this study combines Procedural Fairness Theory, Dual Calculus Theory, Protection Motivation Theory, Theory of Planned Behaviour, and Hofstede's Cultural Dimension Theory. The study adopts a quantitative approach collecting data from 714 respondents using a random sampling technique. The proposed model is tested using structural equation modeling. Empirical results found that the perceived effectiveness of privacy policy negatively influenced privacy concerns, whereas perceived vulnerability had a positive influence. Expected personal and community-related outcomes of sharing information positively influenced attitudes towards DCT apps, while privacy concerns had a negative effect. The intention to adopt DCT apps were positively influenced by attitude, subjective norms, and privacy self-efficacy. This study is the first to empirically test the adoption of DCT apps of the COVID-19 pandemic and contributes both theoretically and practically towards understanding factors influencing its widespread adoption.

Index Terms: Digital contact tracing; COVID-19; Privacy; Information disclosure; Adoption intention.

Paper type: Research paper

I. INTRODUCTION

On January 30, 2020, the World Health Organisation (WHO) declared a public health emergency of international concern with the outbreak of coronavirus disease 2019 (COVID-19). COVID-19 is an infectious disease that is caused by the novel coronavirus SARS-COV-2. Contact tracing and case isolation are the commonly used interventions to control the spread of this highly infectious disease [1, 2]. -

Contact tracing involves identifying and informing individuals who have come in contact with a COVID-19 positive patient. Manual procedures for contact tracing are not efficient enough to control the spread of the virus. Globally governments have resorted to technology to provide an innovative solution to this problem [3]. Therefore, with smartphone usage becoming ubiquitous, there is an opportunity to leverage this technology for Digital Contact Tracing (DCT). DCT would allow for an almost instantaneous alert to be sent to close contacts of the diagnosed patients to self-isolate. This system would utilize location data obtained through Bluetooth from smartphones to trace individuals and their interactions [4]. Despite this method having the potential to reduce the inefficiency of manual contact tracing, it has given rise to significant privacy concerns. For the successful implementation of DCT apps, a higher "transmission rate" than COVID-19 is required for DCT apps to assist in fighting this pandemic.

The topic of privacy had gained significant popularity with practitioners and researchers [5-8]. Privacy decision making was found to be a rational process of weighing the costs and benefits [9, 10]. However, studies are producing contradictory findings relating to privacy and information disclosure. Barth and De Jong [11] found the decision-making process to be irrational with individuals giving minimal to no consideration to privacy risk factors. This highlights the contextual nature of privacy decision making [12] and suggests the requirement for further studies in different contexts [13, 14].

Studies have shown significant differences in individuals' perceptions in different countries when evaluating the costs and benefits relating to privacy [9]. Gutierrez et al. [9] argued that personality traits and culture influence the individuals in the USA to be more attracted to rewards. However, in Europe, intrusiveness is a critical factor when considering privacy and information disclosure. Similarly, Pentina et al. [15] found that technological infrastructure and the epercentnvironment influence the technology adoption rate in both China and the USA. The USA is currently lagging on the rollout of contact tracing applications. Albama, North Carolina, North Dakota, South Dakota and Utah have all released contact tracing applications as each state had been left to develop their own. The USA's patchwork approach makes the effective deployment of an application particularly challenging [16].

A review of the privacy literature highlights that minimal studies have been undertaken to date in developing countries. This study is the first to consider the privacy and information sharing dilemma in Fiji. Fiji is an island country located in the South Pacific. The two major islands of

the country are Viti Levu and Vanua Levu. The capital city of Suva is located on the island of Viti Levu [17]. The country has a population of approximately 750,000 **[18]**. Despite Fiji being the most developed country in the South Pacific, it differs from other developed countries in terms of their economy, cultural and technological infrastructure, and legal environment [19].

This study offers important managerial insights. First, it it beneficial to app developers and those in-charge of its successful implementation in realizing issues influencing the adoption of DCT apps. Second, the study assists app developers in their efforts to develop DCT apps that individuals are more likely to adopt. Third, the study offers insights for government departments charged with the implementation of DCT apps to formulate strategies that would be most effective in reducing an individual's concerns towards these apps. This can be in terms of helping individuals realize the personal and community benefits of adopting DCT apps. Fourth, as individuals are more likely to adopt technology that conform to their values, this study highlights the importance of cultural factors in DCT app adoption. As countries and individuals differ in terms of cultural dimensions such as individualism/collectivism and uncertainty avoidance, empirical evidence from this study provides novel insights into the influence of culture on their perceptions of DCT apps during the COVID-19 crisis. Such enhanced understanding would enable app developers and those charged with its implementation to tailor DCT apps more effectively to potential users.

II. LITERATURE REVIEW AND THEORETICAL BACKGROUND

A. Digital Contact Tracing

Information disclosure is defined as individuals revealing personal information voluntarily and intentionally to others [20]. Amidst the COVID-19 pandemic, information disclosure by individuals can help automate the contact tracing efforts. Several different countries have various methods and apps for contact tracing. For example, in March 2020, Singapore developed and implemented an app called *TraceTogether*. The app uses Bluetooth technology to collect information regarding users who have been in close proximity to one another. This information is used by the health ministry to track and contact all individuals who have come in contact with a COVID-19 patient. However, the country has seen a low uptake of this application by citizens [21]. Australia launched its DCT software named *COVIDSafe,* in late April 2020. The app allows smartphones to perform a "digital handshake" when it comes within

five feet of another device and notifies users if they have come into contact with a diagnosed person for more than 15 minutes. A similar app was expected to be launched by New Zealand in early May 2020. The country is relying on the citizens' voluntary adoption of this app. Privacy Foundation Chair, Gehan Gunasekara, has stated that trust in the government's commitment towards data protection is vital to ensure the successful adoption of this app [22]. France has also launched a location tracing app called StopCovid in June. This app uses Bluetooth technology to track users who have been in close contact for more than 15 minutes. The French app uploads the collected data on centralized government servers [23]. A similar app called *Corona-Warn-App* has abeen launched in Germany. The app does not log the location of individuals and also recognizes other users of the app in close proximity [24]. This was done to reduce the privacy concerns of individuals. In June, Fiji launched a DCT app called *CareFiji* [25]. The technology giants Apple and Google have formed an alliance to develop a similar app that would be part of the mobile-phones operating systems by mid-May 2020. This will be a significant step in DCT efforts as together, both companies own about 99 percent of the smartphone market share. Thus it can be seen that the governments of several countries have identified the potential for DCT apps in the fight with COVID-19. As such, this study provides initial empirical evidence regarding individual's factors influencing their privacy concerns and intention to adopt DCT apps.

B. Dual calculus perspectives

The privacy calculus theory has been used extensively to investigate concerns relating to privacy [10]. According to this theory, individuals are more likely to disclose personal information if the risk-benefit analysis is favorable [26]. However, there are certain limitations of this theory. First, the risk-benefit assessment of information disclosure is contextual [27]. Second, this theory ignores the antecedents of privacy concerns. To address these gaps, Li [28] proposed a dual calculus model. The dual calculus model assumes that the risk calculus influences the privacy calculus, which impacts on information disclosure. The risk calculus is based on balancing the expected risk and coping effectiveness of individuals [10]. The coping mechanisms reduce privacy concerns while the expected risk increases [28].

Therefore, based on the risk calculus theory, this study considers perceived severity and perceived vulnerability as threats to information disclosure in DCT apps, while privacy self-efficacy would be used to measure coping effectiveness. Based on the privacy calculus theory, the benefits of DCT apps would be expected personal outcomes of sharing information and

potential community-related outcomes of sharing information while the risk would be the privacy concerns of adopting DCT apps.

C. Theory of Planned Behavior (TPB)

According to the TPB, an individual's intention to adopt DCT apps is driven by their attitude, perceived behavioral control (PBC) and subjective norms. Attitude is defined as an individual's overall assessment of the intended behavior that is formed based on their evaluations and perceived outcomes [29]. In this study, attitudes towards contact tracing apps are influenced by expected personal outcomes of sharing information, expected community-related outcomes of sharing information, and privacy concerns. Subjective norms are an individual's perception of significant others' beliefs or socially imposed normative pressure that leads them to act [29]. Here, the subjective norms is an individual's significant other belief regarding adopting DCT apps. PBC is defined as an individual's controllability of behavior based on experiences from the past. Privacy self-efficacy is the most relevant factor for PBC in this study.

D. Hofstede's Cultural Theory

Culture concerns shared societal perceptions, beliefs, and values. The information systems literature highlights culture at various levels, such as national, organizational, group, and individual [19]. The societal norms and practices have a profound impact on societal acceptance and adoption of technology [19, 30]. This study explores the cultural dimensions at an individual level to moderate the impact between information privacy concerns and attitude towards DCT apps using the dimensions of culture proposed by Hofstede [31]. According to Hofstede [32], national culture scores should not be used to understand an individual's behavior [32]. National cultural dimensions are exhibited through an individuals' espoused cultural values [33]. This study adopts two dimensions of culture proposed by Hofstede, namely collectivism and uncertainty avoidance. These are the two most applied and relevant dimensions of culture to understand technology adoption [19].

TABLE 1
ESPOUSED NATIONAL CULTURAL DIMENSION DEFINITIONS

Dimensions	Description
Collectivism (COL)	The extent to which an individual acquires their identity by being a member of a community [14].
Uncertainty Avoidance (UA)	The degree to which vagueness and unfamiliar circumstances are perceived as threats [14].

III. CONCEPTUAL FRAMEWORK AND HYPOTHESES DEVELOPMENT

From the review of literature and theories, it was evident that due to the differences in emphasis of these theories, a study incorporating multiple theories could lead to a more holistic understanding of this phenomenon. Therefore, by combining Procedural Fairness Theory, Dual Calculus Theory, Protection Motivation Theory, Theory of Planned Behavior and Hofstede's Cultural Dimension Theory a comprehensive model is proposed that enables a deeper understanding of privacy concerns at a time when the world is faced with a global pandemic.

A. Perceived effectiveness of privacy policy

Extant literature on privacy states that personal information shared by individuals can be collected by institutions or organizations if individuals have given consent [34, 35]. For an organization to extract and use an individual's data, the organization must have a privacy policy that highlights the use of data and how the information will be safeguarded [36]. Individuals who are willing to use the services must agree to the terms and conditions of the privacy policy and provide consent to use their personal information.

The perceived effectiveness of privacy policy is an individual's understanding of a set of written statements obtainable during user registration, which highlights an organization's or developer's intention to use the personal information extracted and how this data will be safeguarded [37]. In a mobile phone application context, Zhao et al. [38] elucidated that privacy policy explains to the users how their data will be used by the business. The privacy policy only becomes effective when the users of the product or service believe in the commitment of the organization to protect their information [36]. According to a study on the motivation to self-disclose personal information in mobile applications, the privacy policy is an effective strategy to address privacy concerns due to the existence of a negative relationship between the

two constructs [39]. This indicates that individuals are more likely to share their personal information if they feel the information is protected and will not be misused [40]. Therefore, it is hypothesized that:

H1: Perceived effectiveness of privacy policy negatively influences privacy concerns relating to DCT apps.

B. Perceived effectiveness of industry self-regulation

Another type of institutional privacy assurance is the perceived effectiveness of self-regulation. This refers to the seal issued by independent certifying agencies like TRUSTe and VeriSign to developers and organizations [37]. The display of such seals encourages individuals to register for products and services with the assurance that the information they provide will not be misused. For mobile applications, it becomes the responsibility of the developers to safeguard the personal information provided by the users [41]. The independent certifying agencies will then monitor whether the developers are abiding by the industry regulations [37]. This reduces the information privacy concerns of users. Gong et al. [39] confirmed that the perceived effectiveness of industry self-regulation lowers privacy concerns in disclosing personal information on mobile applications. Consequently, users of these applications are more likely to disclose personal information as they trust and believe in the industry's self-regulation [40]. In the context of the contact tracing application, users will have lower information privacy concerns if the industry self-regulation of the application is perceived to be effective. Therefore, it is hypothesized that:

H2: Perceived effectiveness of industry self-regulation negatively influences privacy concerns relating to DCT apps.

C. Perceived severity

Perceived severity is defined as the negative consequences perceived by individuals as a result of security threats [42]. Such threats elicit behaviors that protect privacy concerns. Individuals concerned about information security take the necessary precautions to safeguard their data. Such actions are driven by the perceived negative consequences and impact of losing personal or private data [43]. These concerns are magnified for mobile phone users due to the interconnectedness of individuals, things, and objects. Wang et al. [13] found in the context of disclosure of personal information through mobile phone applications, that individuals with high perceived severity are less likely to disclose personal information as they perceive there

is a high risk of their data to be misused. Moreover, according to Mohamed and Ahmad [43], a person who perceives that losing information will result in severe consequences is more concerned regarding sharing information on social networking sites. A further study on the privacy concerns of sharing health information in online health communities stated the deep concern of privacy relating to the sharing of health information being influenced by a high degree of perceived severity of the information being misused [10]. Privacy concerns have become greater for some individuals due to the increase in negative activities such as identity theft and internet fraud [44]. Thus, in the context of the contact tracing application, individuals who perceive that the information gathered from this mobile phone application will be misused, are more concerned about the privacy of their personal health information. Therefore, it can be hypothesized that:

H3: Perceived severity positively influences privacy concerns relating to DCT apps.

D. Perceived vulnerability

Perceived vulnerability is an individual's evaluation of possibly encountering a threat [45]. An individual's perception of the negative consequences of sharing personal information is described as vulnerability. The vulnerability of individuals increases when they perceive that disclosure of personal information will lead to potential threats such as abuse or misuse of information [46]. Dinev and Hart [46] study on antecedents and privacy concerns of sharing information on the internet highlighted a positive relationship between perceived vulnerability and privacy concern. Additionally, Mohamed and Ahmad [43] carried out a study in Malaysia that confirmed perceived vulnerability as an antecedent of privacy concerns in sharing information on social networking sites. Whilst, Zhang et al. [10] stated that users of online health communities are concerned regarding disclosing personal health information if they perceive that there is a risk of losing personal information. Thus, this study postulates that individuals who perceive information privacy threats by sharing personal information through the contact tracing application are more concerned regarding information privacy. Hence, the following hypothesis is proposed.

H4: Perceived vulnerability positively influences privacy concerns relating to DCT apps.

E. Perceived privacy self-efficacy

Self-efficacy is a key contract of the social cognitive theory as it evaluates an individual's ability to organize and perform actions that will enable them to achieve the desired performance

[47, 48]. This solely depends on the individual's self-judgment of their ability to perform an activity. In the context of privacy concerns, privacy self-efficacy is an individual's judgment and confidence of oneself to manage privacy issues [28] and safeguard personal information or data [49]. More knowledge or information regarding a specific activity (high self-efficacy) leads to fewer privacy concerns as individuals become confident in dealing with privacy issues. Youn [50] study on online privacy concerns and protection behavior demonstrated a negative relationship between privacy self-efficacy and online privacy concerns in young adolescents. Yao et al. [51] on online privacy user concerns confirmed that the more knowledge individuals acquire regarding internet usage and fluency, the less concerned they will be regarding privacy when sharing information on virtual platforms. A further study conducted on health information disclosure in online health communities highlighted that individuals with internet skills and medical knowledge are less concerned about privacy when sharing personal health information [10]. In the context of the adoption of a contact tracing application, it is suggested that the more application knowledge people have, the less likely they will be concerned regarding privacy when sharing personal health information. Therefore, the following hypothesis is suggested:

H5: Perceived privacy self-efficacy negatively influences privacy concerns relating to DCT apps.

F. Expected personal outcomes

The expected personal outcome is an individual's judgment of the personal benefits gained from sharing personal information with the general public [52]. Chung [53] explained the expected personal outcome as a way of sharing personal information to assist others. In return, feelings of self-satisfaction and the importance of assisting the greater community are common self-benefits attained from sharing personal information. Additionally, Atkinson et al. [54] found that individuals with poor health conditions tend to disclose personal information on virtual health communities to seek social support from others in the communities. Therefore, the intention of these individuals to disclose personal information is for self-benefit purposes. However, it depends on an individual's attitude towards disclosure of personal information to benefit oneself. As this study focuses on the contact tracing application, individuals with the intention to self-benefit are likely to have a positive attitude towards the application. The individuals will want to know if they have had an encounter with someone who has been tested positive for COVID-19. Thus, the hypothesis is as follows:

H6: Expected personal outcomes of sharing information positively influences attitude towards DCT apps.

G. Expected community-related outcomes

Another construct explored in the privacy calculus model is the expected community-related outcome of sharing personal information. This construct explains that the community will benefit from the shared personal information [55]. In the virtual environment, seeking and providing social support will only be possible when individuals share their personal information and experiences to make a meaningful impact in the broader community [56]. In the context of this study, it is expected that individuals use the contact tracing application to assist the greater community and prevent the spread of COVID-19. Individuals with a high level of emotional attachment to communities are likely to provide emotional support and assist communities to combat issues [55]. Nevertheless, the intention to use this application to benefit the community depends on an individual's attitude towards the contact tracing application itself and how comfortable one is to share personal information regarding their health and location. Individuals who are focused on helping the community to trace contacts of a patient tested positive are likely to have a positive attitude towards this application. Therefore, this study posits the following hypothesis:

H7: Expected community-related outcomes of sharing information positively influences attitude towards DCT apps.

H. Privacy concerns

Privacy concerns are prevalent when it comes to the sharing of personal information. It is the concern felt by an individual to share their personal information in a public forum [37]. The virtual world has raised several privacy concerns on data collection and control over data [35]. Extant literature notes that individuals are less likely to share personal information on online platforms as they are concerned about information privacy [57]. Privacy concerns are one of the various behavioral beliefs of attitude towards disclosure of personal information. Therefore, the more one is worried regarding sharing personal information due to privacy concerns, the more negative their attitude becomes towards adopting a technology that will extract personal information. A study on online privacy protection, found that the negative attitudes towards data collection was due to information privacy concerns of individuals [50]. Ketelaar and van Balen [58] stated on phone-embedded tracking that a negative attitude was a result of high

information privacy concerns of users. In the context of this study, users will develop a negative attitude towards the extraction of personal information by the contact tracing application as they are concerned about their personal information being misused. Hence, this study postulates the following hypothesis:

H8: Privacy concerns negatively influence attitude towards DCT apps.

I. Cultural moderators

Hofstede [31] espoused culture theory defines collectivism is the degree to which an individual values the interest of a community rather than oneself. In a collectivist culture, the integration of people in groups leads to interdependence and sacrifice as they are not self-oriented. The strong sense of community in a collectivist society results in decisions and actions that would succeed in the community [31, 59, 60]. A privacy study on Hofstede's culture theory found that collectivists have a higher rate of acceptance of sharing personal information as these individuals value societal welfare [61]. This is because collectivists are less concerned about information privacy and want the community to benefit from the sharing of information. As such, this study suggests that collectivists will boost the effectiveness of contract tracing application as collectivists are less concerned about information privacy, thus, a positive attitude towards sharing personal information. Hence, it can be hypothesized:

H9a: The relationship between privacy concerns and attitude is weaker in cultures that are high in collectivism.

Uncertainty avoidance refers to an individual in the society who is reluctant to engage in risk-taking behaviors [31]. When exposed to an ambiguous situation, the members of a risk-averse society feel anxious. Societies with high uncertainty avoidance consider ambiguity as a threat and follow regulations to safeguard themselves from the unknown [62]. High uncertainty avoidance is common in highly structured societies [63]. According to Cao and Everard [64], information privacy becomes more of a concern in high uncertainty avoidance societies. Another privacy-related research confirmed that greater information privacy concerns are a result of uncertainty avoidance [20]. These studies indicate the people living in such societies will be reluctant to disclose personal information. These individuals are less likely to develop a positive attitude and adopt the contact tracing application. As this application will be new and require personal information, risk-averse individuals will not consider installing this application. Therefore, it is hypothesized that:

H9b: The relationship between privacy concerns and attitude is stronger in cultures with low uncertainty avoidance.

J. Attitude

According to TPB, attitude and subjective norms are two antecedent factors that influence behavioral intention [65]. Attitude is an overall evaluation of an individual's behavior [66]. Attitude towards disclosing personal information is formed from the behavioral beliefs, which includes the perceived benefit and privacy concerns [28]. The virtual environment is receiving significant attention in terms of privacy concerns relating to the sharing of personal information. A study on information sharing decisions on social networking sites confirmed a positive relationship between attitudes towards sharing information and the intention to share information on social networking sites [67]. Furthermore, a study on privacy concerns with electronic health records stated that an individual's attitude towards electronic health systems would influence the likelihood of adopting this technology [68]. Another study on online privacy and behavior towards information disclosure stated that the behavioral intention to disclose information on an online platform is influenced by the attitude towards individuals' information disclosure [28]. This study suggests that attitudes towards sharing personal information like one's location and whom they have met will positively influence the behavioral intention of an individual to adapt to the contact tracing application. Based on the studies and theoretical premises, it is hypothesized:

H10*: Attitude positively influences DCT app adoption.*

K. Subjective norms

Subjective norm is the social normative pressures perceived by individuals, which affects their intention to perform an action and engage in a behavior. Existing privacy literature has not paid sufficent attention to subjective norms in an online context. The need to conform to friends, colleagues, and family with regards to information disclosure influences an individual's intention to share personal information. Dai and Palvi [69] conducted a cross-cultural study in the USA and China on mobile commerce adoption, which confirmed that subjective norm influences people's intention to adopt mobile commerce in China. This is due to the collectivistic culture in China. Similarly, another study on online information privacy concerns suggests that individuals' subjective norms for disclosure influence their behavioral intention

to disclose personal information [28]. Considering that contact tracing application users will be sharing personal information with the developers, the following hypothesis is suggested:

H11: Subjective norms positively influences DCT app adoption.

L. Privacy self-efficacy

Since the conceptualization of self-efficacy, it has typically been used to explain the behaviors of individuals in the virtual world [70, 71]. Existing literature on information privacy highlights that self-efficacy shows a relationship that influences the behavioural intention of individuals [72, 73]. The likelihood of an individual to perform a task increases with high self-efficacy. According to Keith et al. [74], higher self-efficacy is crucial to understand the importance of technology use. Similarly, a study on digital traces of mobile phones confirmed that privacy self-efficacy positively influences the behavioral intention to use protective settings [75]. Consistent with the privacy and information-related literature, this study argues that privacy self-efficacy can assist in determining the DCT adoption intention. That is, individuals need to believe in their ability to protect their information privacy before intending to adopt the contact tracing application.

H12: Privacy self-efficacy positively influences DCT app adoption.

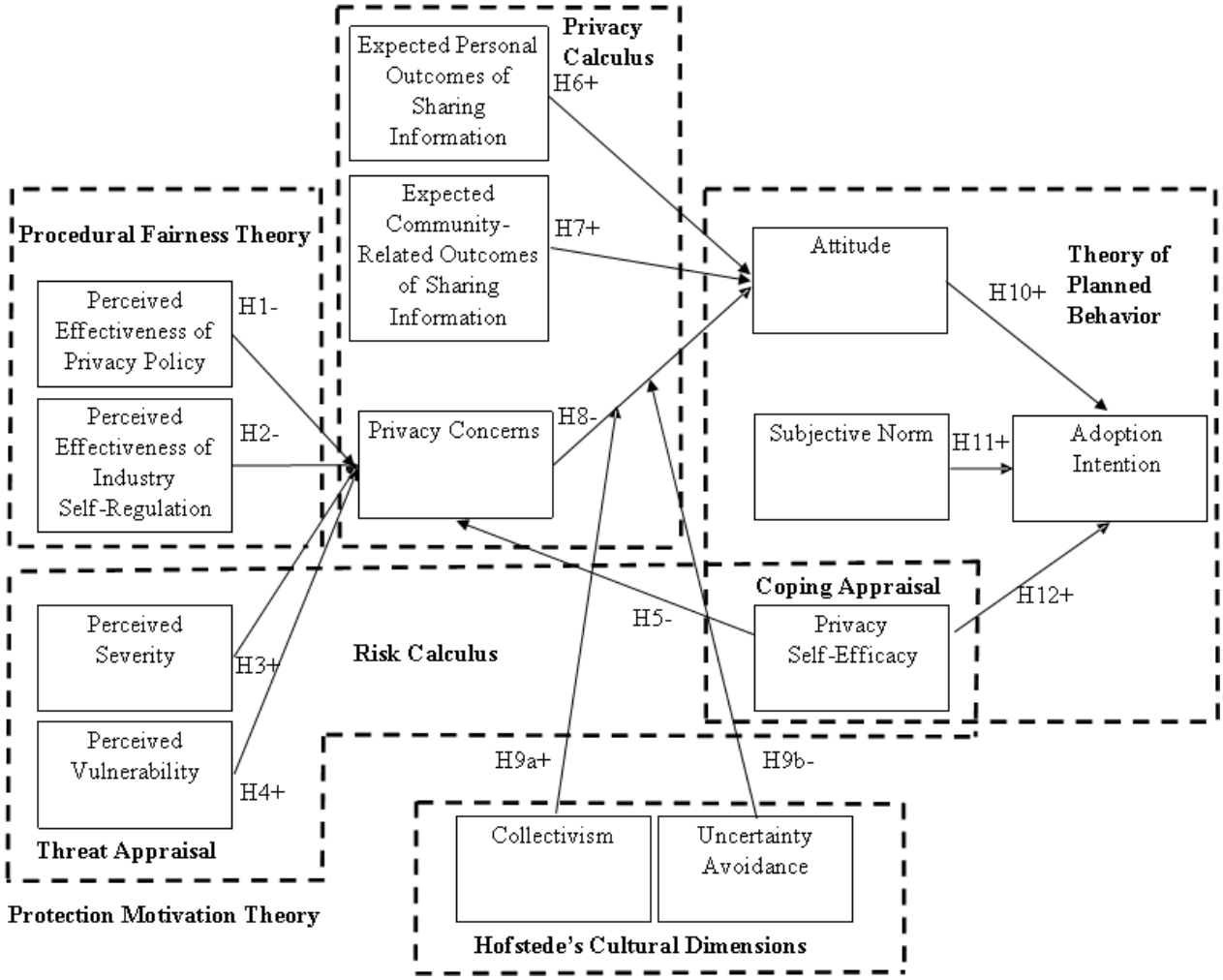

Fig. 1. Conceptual Framework

IV. RESEARCH METHOD

A. Participants and Procedure

Before conducting the full survey, a pilot test was conducted with 10 Ph.D. students at the University of the South Pacific. Based on the results of this test, minor changes were made to the phrasing of the items. Following this, the full survey was conducted on Facebook. Facebook is the most popular social networking site in Fiji [18]. The largest social group related to COVID-19 on Facebook is called "Fiji CoronaVirus Awareness Community" with 36,642 members. A list of all members was extracted from the group. From this list, 2,000 members were randomly selected. An invitation email was sent to these members containing the link to the questionnaire. From this, a total of 714 responses were collected. Table 2 below depicts the demographic profile of the respondents.

TABLE 2
DEMOGRAPHIC PROFILE

Characteristics	N	%
Gender		
Female	277	60.5
Male	432	38.8
Do not wish to indicate	5	0.7
Age		
18 – 21 years	146	20.5
22-31 years	296	41.5
32-41 years	180	25.2
42-51 years	52	7.28
52 -61 years	36	5.04
62 years and above	1	0.14
Do not wish to indicate	3	0.42
Qualification		
Primary School	-	-
Secondary School	266	37.3
Diploma/Certificate	95	13.3
Bachelors education	298	41.7
Postgraduate education	30	4.2
Others	25	3.5
Do not wish to indicate	-	-

B. Measures

The scales used to measure items were validated by prior studies. They were appropriately modified to the context of this study. A seven point Likert scale was used for this study as it is more reliable in capturing the perceptions of respondents [76]. Appendix A lists the measurement items for this study and the studies from which they were adopted. From the data that was collected, reliability and validity (both convergent and discriminant validity) were confirmed. The table in Appendix B shows that the reliability and validity conditions were met. The descriptive analysis of the measures is presented in Table 3.

TABLE 3
DESCRIPTIVE ANALYSIS OF THE MEASURES

Variable/Adopted	Measurement items	Mean	SD
Collectivism (COL)	COL1	5.06	1.77
	COL2	4.83	1.85
	COL3	4.84	1.8
	COL4	4.63	1.85
	COL5	4.38	1.82
	COL6	4.27	1.96
Uncertainty Avoidance (UAV)	UAV1	6.13	1.21
	UAV2	6.54	0.91
	UAV3	6.53	0.85
	UAV4	6.25	0.91
	UAV5	6.46	0.81
Attitude (ATT)	ATT1	5.37	1.43
	ATT2	5.32	1.44
	ATT3	5.13	1.57
	ATT4	4.93	1.53
	ATT5	4.72	1.58
Subjective Norm (SUB)	SUB1	4.53	1.54
	SUB2	4.41	1.58
	SUB3	4.77	1.64
	SUB4	4.61	1.61
Privacy Self-Efficacy (PSE)	PSE1	5.46	1.39
	PSE2	5.66	1.34
	PSE3	5.24	1.47
Perceived Effectiveness of Privacy Policy (PEPP)	PEPP1	5.06	1.42
	PEPP2	5.07	1.47
	PEPP3	5.07	1.42
Perceived Effectiveness of Industry Self-Regulation (PEIR)	PEIR1	5	1.24
	PEIR2	4.92	1.32
	PEIR3	5.03	1.28
Perceived Severity (PSV)	PSV1	5.66	1.32
	PSV2	5.78	1.28
	PSV3	5.31	1.53
Perceived Vulnerability (PVN)	PVN1	4.76	1.51
	PVN2	4.63	1.5
	PVN3	4.82	1.51
Information Privacy Concerns	IPC1	4.47	1.5
(IPC)	IPC2	4.37	1.48
	IPC3	4.23	1.56
Expected Personal Outcomes of Sharing (EPOS)	EPOS1	4.92	1.36
	EPOS2	4.66	1.46
	EPOS3	4.62	1.34

	EPOS4	4.71	1.42
Expected Community-Related Outcomes of Sharing (ECRPS)	ECRPS1	4.88	1.39
	ECRPS2	4.97	1.32
	ECRPS3	4.11	1.57
	ECRPS4	4.89	1.39
Adoption Intention (ADI)	ADI1	4.83	1.53
	ADI2	4.81	1.5
	ADI3	4.79	1.54
	ADI4	4.67	1.56
	ADI5	4.96	1.57

Table 4 below also confirms the confirmatory factor analysis results for the constructs used in this survey.

TABLE 4
CONFIRMATORY FACTOR ANALYSIS RESULTS FOR REFINED MEASUREMENT ITEMS

Factor and item description	Model and item indices				
	SL	CR	SMC	AVE	MSV
Collectivism					
COL1	0.866		0.217		
COL2	0.769		0.313		
COL3	0.827	0.798	0.683	0.408	0.1
COL4	0.772		0.595		
COL5	0.864		0.318		
COL6	0.785		0.342		
Uncertainty Avoidance					
UAV1	0.776		0.221		
UAV2	0.807		0.651		
UAV3	0.908	0.874	0.825	0.589	0.101
UAV4	0.712		0.507		
UAV5	0.812		0.66		
Attitude					
ATT1	0.889		0.79		
ATT2	0.917		0.841		
ATT3	0.928	0.951	0.86	0.797	0.544
ATT4	0.916		0.839		
ATT5	0.818		0.669		
Subjective Norm					
SUB1	0.866		0.749		
SUB2	0.879	0.934	0.773	0.781	0.544
SUB3	0.905		0.819		
SUB4	0.918		0.842		
Privacy Self-Efficacy					
PSE1	0.789		0.623		
PSE2	0.864	0.872	0.746	0.695	0.25
PSE3	0.843		0.711		
Perceived Effectiveness of Privacy Policy					
PEPP1	0.854	0.915	0.729	0.782	0.571

PEPP2	0.9		0.811		
PEPP3	0.879		0.773		
Perceived Effectiveness of Industry Self-Regulation					
PEIR1	0.801		0.642		
PEIR2	0.861	0.882	0.741	0.713	0.571
PEIR3	0.869		0.756		
Perceived Severity					
PSV1	0.879		0.623		
PSV2	0.926	0.852	0.746	0.666	0.101
PSV3	0.604		0.711		
Perceived Vulnerability					
PVN1	0.797		0.773		
PVN2	0.946	0.899	0.857	0.749	0.31
PVN3	0.859		0.365		
Information Privacy Concerns					
IPC1	0.789		0.623		
IPC2	0.9	0.864	0.81	0.68	0.31
IPC3	0.788		0.621		
Expected Personal Outcomes of Sharing					
EPOS1	0.773		0.598		
EPOS2	0.876	0.881	0.768	0.651	0.656
EPOS3	0.723		0.523		
EPOS4	0.854		0.729		
Expected Community-Related Outcomes of Sharing					
ECRPS1	0.872		0.76		
ECRPS2	0.907	0.8	0.823	0.542	0.656
ECRPS3	0.73		0.053		
ECRPS4	0.721		0.52		
Adoption Intention					
ADI1	0.94		0.884		
ADI2	0.934		0.872		
ADI3	0.948	0.967	0.898	0.853	0.481
ADI4	0.911		0.83		
ADI5	0.88		0.775		

An examination of common method bias (CMB) was performed using a common latent factor. Results showed no significant changes to the loadings with the addition of this factor to the model. An empirical test of this showed that the common method variance was 30.25 percent. This was less than the 50 percent recommended threshold by Podsakoff et al. [77], showing that CMB does not impact the validity of the results. Results from the confirmatory factor analysis (x^2 (1146) = 2362.631 ($p<0.001$), x^2/df= 2.062, CFI = 0.921; GFI = 0.834 TLI = 0.913; RMSEA = 0.041) were within the suggested criteria.

V. RESULTS

The hypothesis formulated in this study were tested against the empirical data. First, the direct effects were tested. PEPP ($\beta = -0.216$, $P < 0.01$) was found to have a negative influence of IPC while PVN ($\beta = 0.514$, $P < 0.001$) were noted to have a positive effect of IPC. EPOS ($\beta = 0.548$, $P < 0.001$), and ECRPS ($\beta = 0.157$, $P < 0.001$) were found to positively influence ATT while IPC ($\beta = -0.165$, $P < 0.001$) was identified to have a negative influence on ATT. ATT ($\beta = 0.536$, $P < 0.001$), SUB ($\beta = 0.327$, $P < 0.001$), and PSE ($\beta = 0.103$, $P < 0.01$) were found to have a positive influence on ADI.

Second, the tests for moderators (H9a and H9b) came up with the following findings. Quasi-moderator constructs of COL and UA were found to have a positive influence on ADI. COL was found to dampen the negative relationship between IPC and ATT. Therefore, H1, H4, H5, H6, H7, H8, H9a, H10, H11, and H12 were supported while H2, H3, and H9b were rejected. Figure 3 depicts the results for H9a. Figure 4 presents the structural model results.

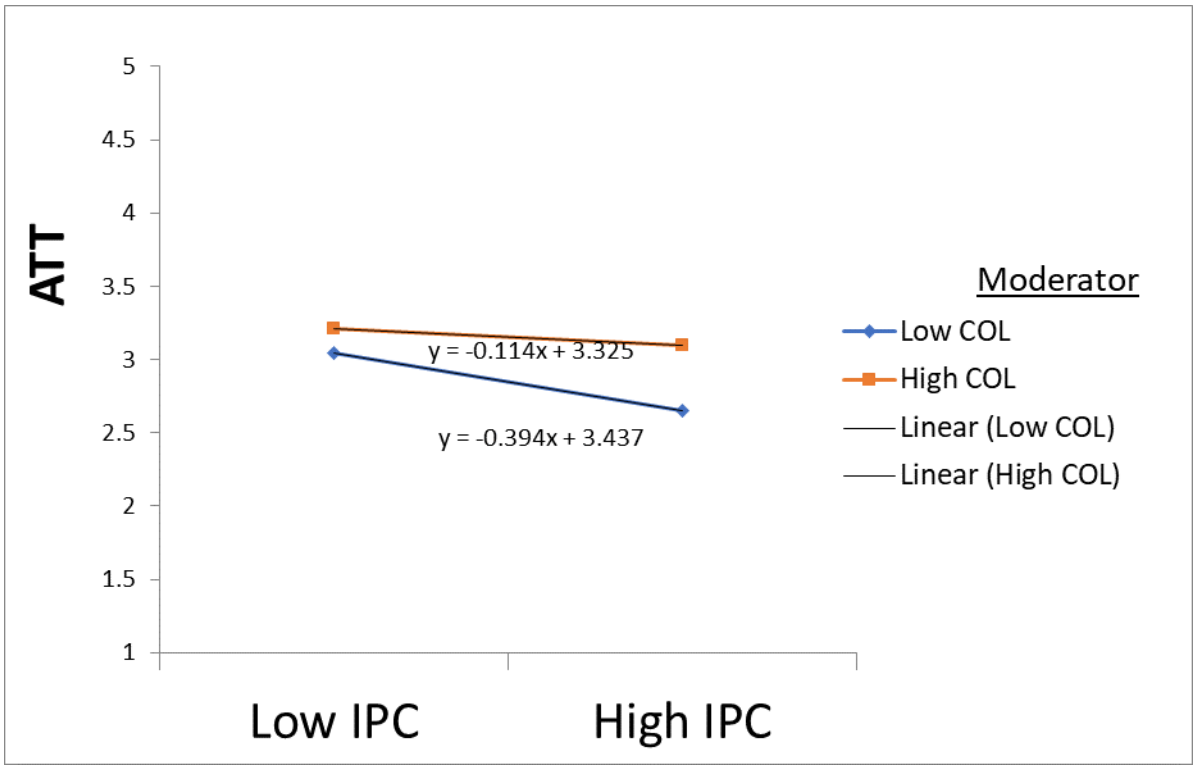

Fig. 2. Moderation Results (H9a)

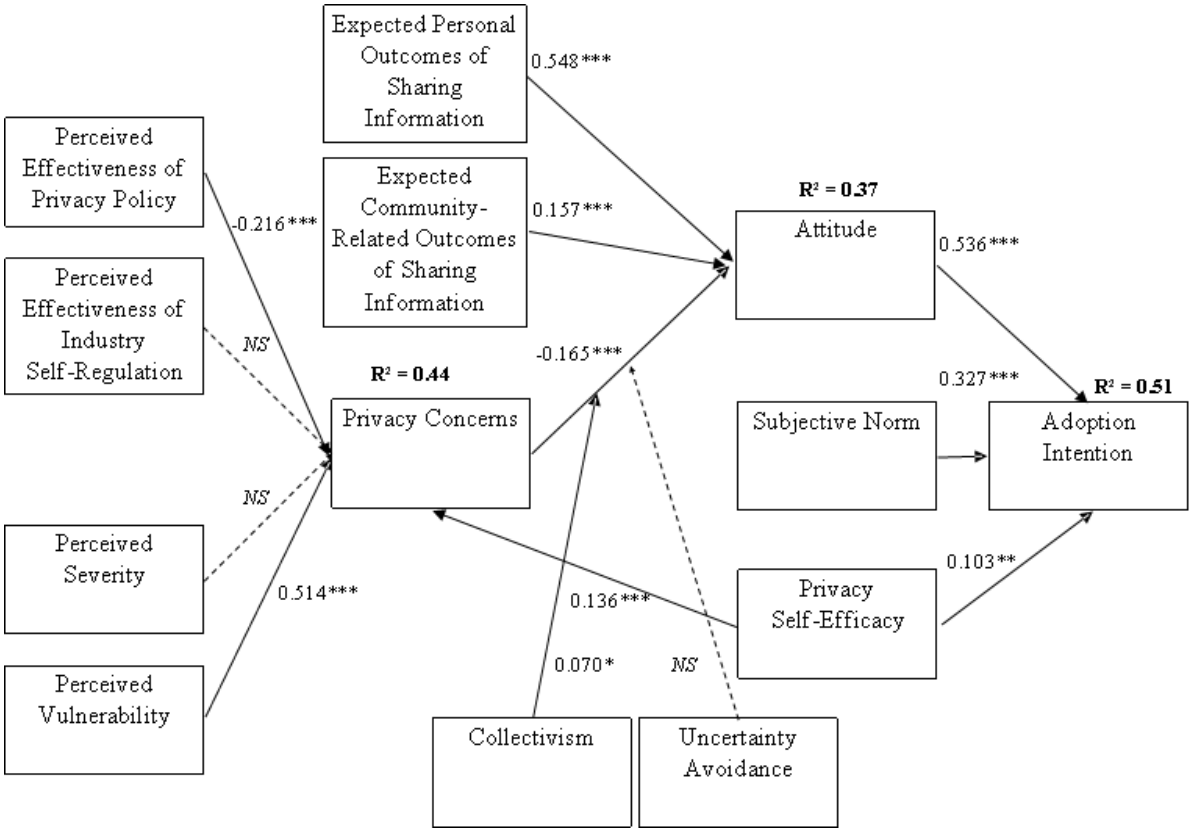

Fig. 3. Structural model results

VI. DISCUSSION

Looking at the explanatory power (R^2) of the model, 44 percent variance was explained by IPC, while 37 percent of variance was explained by ATT. The R^2 value of ADI was 0.51. All values apart from IPC exceeded the recommended values of 40 percent by Straub et al. [78]. According to Chin et al. [79], this can still be classified as moderate. Empirical results from this study support the negative relationship between perceived effectiveness of privacy policy and its influence on privacy concerns relating to DCT apps. This implies that individuals are more open to sharing their personal information when they are informed of its use and feel that this information will be protected. This result is consistent with Gong et al. [39], which highlighted that privacy policy addressed an individual's privacy concerns.

Perceived effectiveness of industry self-regulation was not found to influence privacy concerns relating to DCT apps significantly. This highlights that seals by independent certifying agencies like TRUSTe and VeriSign did not assure individuals about the misuse of their personal

information. This result was not consistent with the findings by Wang and Herrando [40] and Gong et al. [39]. This is potentially due to digital tracing apps being typically controlled by the government and independent certifying agencies are not involved. Perceived severity was not found to influence privacy concerns relating to DCT apps significantly. This implies that for information collected by location tracing apps, individuals perceive that misuse of their information would not have served consequences. This result contradicts the findings by Zhang et al. [10] and Wang et al. [13]. This could be because the respondents of this study are from a developing country where they are not aware of the severity of the impact of personal information misuse.

Results from this study confirmed the positive relationship between perceived vulnerability and privacy concerns relating to DCT apps. This shows that respondents demonstrate awareness regarding the possible threats involved in disclosing personal information. This result is consistent with the findings by Dinev and Hart [46] and Zhang et al. [10]. Empirical results from this study confirmed that perceived privacy self-efficacy negatively influences privacy concerns relating to DCT. This implies that individuals are confident in their ability to manage privacy issues and safeguard their personal information with location tracing applications. This is consistent with Li [28] and Zhang et al. [10]. The positive relationship between expected personal outcomes of sharing information positively influences attitude towards DCT apps. This implies that individuals are more likely to share their personal information using DCT apps as it yields them personal benefits. Similar results were found by Chung [53] who argued that individuals share personal information when there is a likelihood of a personal outcome. These findings are consistent with the results by Atkinson et al. [54] who found that individuals with poor health conditions tend to disclose personal information on virtual health communities to seek social support from others in the communities.

Results from this study also confirmed that expected community-related outcomes of sharing information positively influence attitude towards DCT apps. This result highlights that individuals are willing to share personal information on DCT apps due to the benefit it derives for the community. This can be in terms of identifying victims who could have been in contact with a COVID-19 positive individual. This finding is consistent with the results found by Kordzadeh et al. [55] and Wickramasinghe et al. [56]. Empirical results from this study have confirmed that privacy concerns negatively influence attitude towards DCT apps. This shows that individuals are less likely to share personal information on DCT apps when they are

concerned about information privacy. This is consistent with the findings of Ketelaar and van Balen [58] on phone-embedded tracking.

Results from this study found that the relationship between privacy concerns and attitude is weaker in cultures that are high in collectivism. This demonstrates that the strong sense of community in a collectivist society results in decisions and actions that would benefit the community. As such, individuals have a more positive attitude towards DCT apps. A similar finding was noted by Li et al. [61]. The relationship between privacy concerns and attitude is stronger in cultures with low uncertainty avoidance was not found significant in this study. This result was not consistent with findings by Cao and Everard [80] and Lowry et al. [20]. Studies have primarily shown that societies with high uncertainty avoidance consider ambiguity as a threat and follow regulations to safeguard themselves from the unknown [62]. The inconsistent results can be because of the high degree of threat posed by the COVID-19 virus. This could have caused individuals to pay less emphasis on privacy concerns and more on the benefits that could be derived from the adoption of DCT apps.

Empirical results have confirmed the positive influence of attitude on DCT app adoption. This highlights a positive attitude towards DCT apps can result in their increased likelihood of adopting this technology. A similar finding was derived from Li [28]. Subjective norm were also found to positively influence DCT app adoption by this study. This shows that social pressures perceived by individuals affect their intention to adopt. Li [28] study on online information privacy concerns also found that individuals' subjective norms influence their behavioral intention to disclose personal information. The findings of this study confirm that privacy self-efficacy positively influences DCT app adoption. This shows that an individual's confidence in their ability to manage privacy issues and safeguard personal information increases their willingness to adopt DCT applications. They would feel that their knowledge of mobile phones would ensure that their privacy is protected, and they would be able to delete the application when the COVID-19 pandemic is over.

A. Theoretical contribution

This study is the first to combine Procedural Fairness Theory, Dual Calculus Theory, Protection Motivation Theory, Theory of Planned Behavior, Hofstede's Cultural Dimension Theory to test an individual's intention to adopt DCT apps empirically. Due to the differences in emphasis of these theories, a study incorporating multiple theories could lead to a more holistic understanding of the phenomenon [28, 81]. The resulting model provides a comprehensive

understanding of privacy concerns in a time when the world is faced with a global pandemic. This study takes into account both the antecedents to privacy concerns, which remain an under-researched area in the literature [10], and the consequences of privacy concerns that lead to the adoption of DCT apps. Futhermore, this is one of the first studies to contribute in this regard.

Contradictory findings have resulted from studies relating to privacy and information disclosure. While individuals are engaged in rational decision making when it comes to weighing the cost and benefits of disclosing information [9, 10], other studies have derived irrational decision making where individuals have given little to no regard to the risk of disclosures [11]. The findings of this study highlight the contextual nature of privacy-related decision making and provide the first empirical evidence regarding individuals' decision making during the COVID-19 pandemic. This research has also contributed theoretically to understanding information disclosure and privacy dilemma in the context of developing countries where research is limited. Such contextual differences are essential to understand information systems behavior as developing countries like Fiji differ in terms of economic, cultural, and technological infrastructure, and legal environment [19]. Studies have highlighted the importance of culture and personality traits in influencing individuals' privacy concerns [9]. This study was able to contribute to this understanding by incorporating cultural dimensions of collectivism and uncertainty avoidance to test privacy concerns and attitudes towards DCT apps. Thus, this study responds to calls of researchers to incorporate cultural values to further understand privacy concerns. Theory building literature has highlighted the importance of testing models and instruments in different country contexts to effectively understand the role of context and its influence on theories [82-84]. This study has provided novel empirical evidence from a developing country perspective that provides an improved understanding of how decision making in technology acceptance is influenced by factors such as economy, cultural, technological infrastructure, and the legal environment. This will help to understand the difference in adoption of DCT apps in different countries globally.

B. Implications for practice

This study has multiple practical implications that would effectively assist policymakers in DCT development in various countries and cultures. Results demonstrate that perceived effectiveness of privacy policy negatively influences privacy concerns. Therefore, the privacy statement regarding the DCT app needs to be transparent and informative. It should stipulate exactly when the collected data will be accessed and how it will be used. Results from this

study have shown that this will reduce privacy concerns for individuals. The second dimension of procedural fairness theory about industry self-regulation was not found to be significant. This could imply that individuals' privacy concerns are not influenced by seals issued by independent certifying agencies like TRUSTe and VeriSign to developers and organizations. This could be because, in this case, the government, rather than a private organization or app developers, have access to personal data.

Looking at the influence of threat appraisals on privacy concerns, only perceived vulnerability was found to be significant. This implies that individuals perceived that their information collected by DCT apps is likely to be misused. However, as a result, it demonstrates that perceived severity was not found significant; this could imply that individuals do not perceive the negative concerns of severity to be an issue. As such, app developers could decrease privacy concerns by ensuring that DCT apps keep data stored on individuals' phones rather than the cloud and only access data if an individual is found to be infected by COVID-19.

The findings of this study highlight that both expected personal outcome and expected community outcomes positively influences attitude towards DCT apps. However, upon closer inspection of the results, it is apparent that the benefit of personal outcomes is far more substantial than community outcomes. This implies the need for governments that are looking to implement DCT apps to highlight both the personal and community benefits of adopting this app. The results of this study have illustrated privacy concerns regarding DCT apps. This highlights the requirement to consider the antecedences giving rise to privacy concerns. App developers and those charged with its successful implementation should appreciate that privacy concerns are the only barrier that needs to be addressed to automate contact tracing efforts. Therefore, every effort needs to be made to reduce this concern to increase the adoption rate.

Cultural differences play an essential part in privacy and information disclosure concerns. This has been confirmed by the results of this study. It has been found that with cultures that are high in collectivism, there is a decreased impact of privacy concerns on attitude towards DCT apps. This implies that implementation of DCT apps would be faced with less resistance in collectivist countries like Brazil, China, India, Japan, Korea, and those in the Pacific when compared to countries with a more individualistic culture like in the USA, Europe, and Australia.

The results of this study have shown that attitude is a significant predictor of DCT app adoption intention. This implies the need for app developers and implementors to form a favorable

attitude towards these apps to increase adoption intention. The antecedents of perceived personal and community-related outcomes, together with privacy concerns, could highlight the factors that need to be considered when developing a favorable attitude. Subjective norms were also found to influence adoption intention towards DCT apps. This shows the importance of word-of-mouth in encouraging adoption intention. Privacy self-efficacy was also found to influence adoption intention for DCT apps positively. This result highlights the importance of individuals believing in their ability to protect their information privacy before intending to adopt this app. Therefore, the app developers and implementors need to inform potential users of how privacy will be protected as well as for instructions on uninstalling the app when this pandemic has passed.

VII. CONCLUSION, LIMITATIONS, AND DIRECTIONS FOR FUTURE RESEARCH

This study, recognises certain limitations that provide the basis for future research. First, the ultimate dependent variable is the adoption intention of COVID-19 applications. Behavioral intention does not always lead to actual behavior [85]. It is recommended that a combination of pre-test and post-test measures be employed in future studies. Second, data collection was conducted on Facebook. Despite random sampling being employed, not all individuals with mobile phones are on Facebook. Future studies can use other methods of data collection. Third, the respondents were mostly young. Future studies could benefit from analysis COVID-19 contact tracing application adoption intention with different age groups. Finally, despite a comprehensive model being developed to understand contact tracing application adoption intention, the R^2 value indicates that future research needs to consider other factors to increase the predictive power of the model. To conclude, the imposition of such technology should only be justified as necessary in the circumstances like pandemics for the protection of public health. DCT apps should be one of the tools, among other preventive and detective measures such as decontamination, hygiene, and social distancing against the fight with COVID-19.

REFERENCES

[1] Z. He, "What further should be done to control COVID-19 outbreaks in addition to cases isolation and contact tracing measures?," *BMC Medicine,* vol. 18, no. 1, pp. 1-3, 2020.

[2] S. Kraus, T. Clauss, M. Breier, J. Gast, A. Zardini, and V. Tiberius, "The economics of COVID-19: initial empirical evidence on how family firms in five European countries cope with the corona crisis," *International Journal of Entrepreneurial Behavior & Research,* 2020, doi: 10.1108/IJEBR-04-2020-0214.

[3] S. Kraus, N. Roig-Tierno, and R. B. Bouncken, "Digital innovation and venturing: an introduction into the digitalization of entrepreneurship," *Review of Managerial Science*, vol. 13, pp. 519-528, 2019, doi: 10.1007/s11846-019-00333-8.

[4] L. Lenert and B. Y. McSwain, "Balancing health privacy, health Information exchange and research in the context of the COVID-19 pandemic," *Journal of the American Medical Informatics Association,* 2020, doi: 10.1093/jamia/ocaa039.

[5] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *International Journal of Information Management,* vol. 45, pp. 13-24, 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

[6] P. B. Lowry, T. Dinev, and R. Willison, "Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda," *European Journal of Information Systems,* vol. 26, no. 6, pp. 546-563, 2017.

[7] Z. D. Ozdemir, H. Jeff Smith, and J. H. Benamati, "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study," *European Journal of Information Systems,* vol. 26, no. 6, pp. 642-660, 2017.

[8] C. Clark, A. Davila, M. Regis, and S. Kraus, "Predictors of COVID-19 Voluntary Compliance Behaviors: An International Investigation," *Journal Global Transitions,* vol. 2, 76-82, 2020, doi.org/10.1016/j.glt.2020.06.003.

[9] A. Gutierrez, S. O'Leary, N. P. Rana, Y. K. Dwivedi, and T. Calle, "Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor," *Computers in Human Behavior,* vol. 95, pp. 295-306, 2019, doi: 10.1016/j.chb.2018.09.015.

[10] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu, "Health information privacy concerns, antecedents, and information disclosure intention in online health communities," *Information & Management,* vol. 55, no. 4, pp. 482-493, 2018.

[11] S. Barth and M. D. De Jong, "The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review," *Telematics and Informatics,* vol. 34, no. 7, pp. 1038-1058, 2017.

[12] J.-M. Lee and J.-Y. Rha, "Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce," *Computers in Human Behavior,* vol. 63, pp. 453-462, 2016, doi: 10.1016/j.chb.2016.05.056.

[13] T. Wang, T. D. Duong, and C. C. Chen, "Intention to disclose personal information via mobile applications: A privacy calculus perspective," *International Journal of Information Management,* vol. 36, no. 4, pp. 531-542, 2016.

[14] L. Yu, H. Li, W. He, F.-K. Wang, and S. Jiao, "A meta-analysis to explore privacy cognition and information disclosure of internet users," *International Journal of Information Management,* vol. 51, p. 102015, 2020, doi: 10.1016/j.ijinfomgt.2019.09.011.

[15] I. Pentina, L. Zhang, H. Bata, and Y. Chen, "Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison," *Computers in Human Behavior,* vol. 65, pp. 409-419, 2016, doi: 10.1016/j.chb.2016.09.005.

[16] B. Johnson, *The US's draft law on contact tracing apps is a step behind Apple and Google*, June 2020. Accessed on: June 28, 2020. [Online]. Available: https://www.technologyreview.com/2020/06/02/1002491/us-covid-19-contact-tracing-privacy-law-apple-google/

[17] N. Slack, G. Singh, and S. Sharma, "Impact of perceived value on the satisfaction of supermarket customers: developing country perspective," *International Journal of Retail & Distribution Management,* 2020, doi: 10.1108/ijrdm-03-2019-0099.

[18] S. Sharma, G. Singh, and A. S. Aiyub, "Use of Social Networking Sites by SMEs to engage with their customers: A developing country perspective," *Journal of Internet Commerce,* vol. 19, no. 1, pp. 62-81, 2020.

[19] R. Sharma, G. Singh, and S. Sharma, "Modelling internet banking adoption in Fiji: A developing country perspective," *International Journal of Information Management,* vol. 53, p. 102-116, 2020, doi: 10.1016/j.ijinfomgt.2020.102116.

[20] P. B. Lowry, J. Cao, and A. Everard, "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures," *Journal of Management Information Systems,* vol. 27, no.4, pp. 163-200, 2011.

[21] L. Kim, *Australia's COVIDSafe contact tracing app already has more than a million downloads,* April 2020. Accessed on: May 2, 2020. [Online]. Available: https://www.theverge.com/2020/4/26/21237598/australia-coronavirus-contact-tracing-privacy

[22] Radio New Zealand, *Covid-19: New Zealand contact tracing app due within two weeks,* April 2020. Accessed on: May 2, 2020. [Online]. Available:

https://www.rnz.co.nz/news/national/415214/covid-19-new-zealand-contact-tracing-app-due-within-two-weeks

[23] News Wires, *France rolls out COVID-19 tracing app amid privacy debate*, June 2020. Accessed on: June 27, 2020. [Online]. Available: https://www.france24.com/en/20200602-france-rolls-out-covid-19-tracing-app-amid-privacy-debate

[24] P. H. O'Neil, T. Ryan-Mosley, and B. Johnson, *A flood of coronavirus apps are tracking us. Now it's time to keep track of them,* May 2020. Accessed on: June 27, 2020. [Online]. Available: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

[25] A. Susu, "COVID-19: Fiji acquires contact tracing software," in *The Fiji Times*, 2020.

[26] R. S. Laufer and M. Wolfe, "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of Social Issues,* vol. 33, no. 3, pp. 22-42, 1977.

[27] Z. Jiang, C. S. Heng, and B. C. Choi, "Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions," *Information Systems Research,* vol. 24, no. 3, pp. 579-595, 2013.

[28] Y. Li, "Theories in online information privacy research: A critical review and an integrated framework," *Decision Support Systems,* vol. 54, no.1, pp. 471-481, 2012.

[29] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes,* vol. 50, no. 2, pp. 179-211, 1991.

[30] T. Semrau, T. Ambos, and S. Kraus, "Entrepreneurial orientation and SME performance across societal cultures: An international study," *Journal of Business Research,* vol. 69, no. 5, pp. 1928-1932, 2016.

[31] G. Hofstede, "Culture and organizations," *International Studies of Management & Organization,* vol. 10, no. 4, pp. 15-41, 1980.

[32] G. Hofstede, "Values survey module 1994 manual," *Institute for Research on Intercultural Cooperation: Maastrict, The Netherlands,* 1994.

[33] M. Srite and E. Karahanna, "The role of espoused national cultural values in technology acceptance," *MIS Quarterly,* vol. 30, no. 3, pp. 679-704, 2006.

[34] M. J. Culnan and R. J. Bies, "Consumer privacy: Balancing economic and justice considerations," *Journal of Social Issues,* vol. 59, no. 2, pp. 323-342, 2003.

[35] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research,* vol. 15, no. 4, pp. 336-355, 2004.

[36] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in *Proceedings of the 27th Annual Computer Security Applications Conference*, 2011, pp. 103-112.

[37] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information privacy concerns: Linking individual perceptions with institutional privacy assurances," *Journal of the Association for Information Systems,* vol. 12, no. 12, p. 1, 2011.

[38] L. Zhao, Y. Lu, and S. Gupta, "Disclosure intention of location-related information in location-based social network services," *International Journal of Electronic Commerce,* vol. 16, no. 4, pp. 53-90, 2012.

[39] X. Gong, K. Z. Zhang, C. Chen, C. M. Cheung, and M. K. Lee, "What drives self-disclosure in mobile payment applications? The effect of privacy assurance approaches, network externality, and technology complementarity," *Information Technology & People,* 2019, doi: 10.1108/ITP-03-2018-0132.

[40] Y. Wang and C. Herrando, "Does privacy assurance on social commerce sites matter to millennials?," *International Journal of Information Management,* vol. 44, pp. 164-177, 2019, doi: 10.1016/j.ijinfomgt.2018.10.016.

[41] P. B. Lowry, G. Moody, A. Vance, M. Jensen, J. Jenkins, and T. Wells, "Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers," *Journal of the American Society for Information Science and technology,* vol. 63, no. 4, pp. 755-776, 2012.

[42] R. LaRose, N. Rifon, S. Liu, and D. Lee, "Understanding online safety behavior: A multivariate model," in *The 55th Annual Conference of the International Communication Association, New York City*, 2005.

[43] N. Mohamed and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Computers in Human Behavior,* vol. 28, no. 6, pp. 2366-2375, 2012.

[44] R. LaRose and N. J. Rifon, "Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior," *Journal of Consumer Affairs,* vol. 41, no.1, pp. 127-149, 2007.

[45] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change1," *The Journal of Psychology,* vol. 91, no.1, pp. 93-114, 1975.

[46] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents-measurement validity and a regression model," *Behaviour & Information Technology,* vol. 23, no. 6, pp. 413-422, 2004.

[47] A. Bandura, "Social foundations of thought and action," *Englewood Cliffs, New Jersey*, 1986.

[48] A. Bandura, "Social cognitive theory: An agentic perspective," *Annual Review of Psychology,* vol. 52, no. 1, pp. 1-26, 2001.

[49] N. J. Rifon, R. LaRose, and S. M. Choi, "Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures," *Journal of Consumer Affairs,* vol. 39, no. 2, pp. 339-362, 2005.

[50] S. Youn, "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents," *Journal of Consumer Affairs,* vol. 43, no. 3, pp. 389-418, 2009.

[51] M. Z. Yao, R. E. Rice, and K. Wallis, "Predicting user concerns about online privacy," *Journal of the American Society for Information Science and Technology,* vol. 58, no. 5, pp. 710-722, 2007.

[52] C.-M. Chiu, M.-H. Hsu, and E. T. Wang, "Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories," *Decision Support Systems,* vol. 42, no. 3, pp. 1872-1888, 2006.

[53] J. Chung, "Online social networking for health: how online social networking benefits patients," in *Proceedings of the International Communication's Association Virtual Conference*, 2011.

[54] N. Atkinson, S. Saperstein, and J. Pleis, "Using the internet for health-related activities: findings from a national probability sample," *Journal of Medical Internet Research,* vol. 11, no. 1, 2009.

[55] N. Kordzadeh, J. Warren, and A. Seifi, "Antecedents of privacy calculus components in virtual health communities," *International Journal of Information Management,* vol. 36, no. 5, pp. 724-734, 2016.

[56] N. Wickramasinghe, S. Y. Teoh, C. Durst, and J. Viol, "Designing a consumer health 2.0 application to analyse the relationship between on-line social networks and health-related behaviours," in *Proceedings of the 24th Australasian Conference on Information Systems*, 2013.

[57] A. L. Young and A. Quan-Haase, "Information revelation and internet privacy concerns on social network sites: a case study of facebook," in *Proceedings of the 4th International Conference on Communities and Technologies*, pp. 265-274, 2009.

[58] P. E. Ketelaar and M. van Balen, "The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking," *Computers in Human Behavior,* vol. 78, pp. 174-182, 2018, doi: 10.1016/j.chb.2017.09.034.

[59] P. Akbar, R. Mai, and S. Hoffmann, "When do materialistic consumers join commercial sharing systems," *Journal of Business Research,* vol. 69, no. 10, pp. 4215-4224, 2016.

[60] P. C. Earley and C. B. Gibson, "Taking stock in our progress on individualism-collectivism: 100 years of solidarity and community," *Journal of Management,* vol. 24, no. 3, pp. 265-304, 1998.

[61] Y. Li, A. Kobsa, B. P. Knijnenburg, and M. C. Nguyen, "Cross-cultural privacy prediction," *Proceedings on Privacy Enhancing Technologies,* vol. 2017, no. 2, pp. 113-132, 2017.

[62] R. E. Crossler, F. K. Andoh-Baidoo, and P. Menard, "Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of US and Ghana," *Information & Management,* vol. 56, no. 5, pp. 754-766, 2019.

[63] P. G. Patterson, E. Cowley, and K. Prasongsukarn, "Service failure recovery: The moderating impact of individual-level cultural value orientation on perceptions of justice," *International Journal of Research in Marketing,* vol. 23, no. 3, pp. 263-277, 2006.

[64] J. Cao and A. Everard, "User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy," *Journal of Global Information Technology Management*, vol. 11, no. 2, pp. 30-57, 2008

[65] I. Ajzen, "Nature and operation of attitudes," *Annual Review of Psychology,* vol. 52, no.1, pp. 27-58, 2001.

[66] H. Ajzen and M. Fishbein, "Understanding attitudes and predicting social behavior," 1980.

[67] X. Lin and X. Wang, "Examining gender differences in people's information-sharing decisions on social networking sites," *International Journal of Information Management,* vol. 50, pp. 45-56, 2020, doi: 10.1016/j.ijinfomgt.2019.05.004.

[68] C. M. Angst and R. Agarwal, "Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion," *MIS Quarterly,* vol. 33, no. 2, pp. 339-370, 2009.

[69] H. Dai and P. C. Palvi, "Mobile commerce adoption in China and the United States: a cross-cultural study," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* vol. 40, no. 4, pp. 43-61, 2009.

[70] D. Compeau, C. A. Higgins, and S. Huff, "Social cognitive theory and individual reactions to computing technology: A longitudinal study," *MIS Quarterly,* vol.23, no. 2, pp. 145-158, 1999.

[71] D. R. Compeau and C. A. Higgins, "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly,* vol. 19, no. 2, pp. 189-211, 1995.

[72] M. Warkentin, A. C. Johnston, and J. Shropshire, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems,* vol. 20, no. 3, pp. 267-284, 2011.

[73] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security,* vol. 31, no.1, pp. 83-95, 2012.

[74] M. J. Keith, S. C. Thompson, J. Hale, P. B. Lowry, and C. Greer, "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior," *International Journal of Human-Computer Studies,* vol. 71, no. 12, pp. 1163-1173, 2013.

[75] R. E. Crossler and F. Belanger, "Why would I use location-protective settings on my smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap," *Information Systems Research,* vol. 30, no. 3, pp. 995-1006, 2019.

[76] R. Chen, J. Wang, T. Herath, and H. R. Rao, "An investigation of email processing from a risky decision-making perspective," *Decision Support Systems,* vol. 52, no. 1, pp. 73-81, 2011.

[77] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies," *Journal of Applied Psychology,* vol. 88, no. 5, p. 879-903, 2003.

[78] D. Straub, M.-C. Boudreau, and D. Gefen, "Validation guidelines for IS positivist research," *Communications of the Association for Information Systems,* vol. 13, no.1, pp. 380-427, 2004.

[79] W. W. Chin, R. A. Peterson, and S. P. Brown, "Structural equation modeling in marketing: Some practical reminders," *Journal of Marketing Theory and Practice,* vol. 16, no. 4, pp. 287-298, 2008.

[80] J. Cao and A. Everard, "Influence of culture on attitude towards instant messaging: Balance between awareness and privacy," in *International Conference on Human-Computer Interaction*, 2007, pp. 236-240.

[81] A. Schwarz, M. Mehta, N. Johnson, and W. W. Chin, "Understanding frameworks and reviews: a commentary to assist us in moving our field forward by analyzing our past," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* vol. 38, no. 3, pp. 29-50, 2007.

[82] M. Alvesson and D. Kärreman, "Constructing mystery: Empirical matters in theory development," *Academy of Management Review,* vol. 32, no. 4, pp. 1265-1281, 2007.

[83] S. A. Brown, A. R. Dennis, and V. Venkatesh, "Predicting collaboration technology use: Integrating technology adoption and collaboration research," *Journal of Management Information Systems,* vol. 27, no. 2, pp. 9-54, 2010.

[84] V. Venkatesh, J. Y. Thong, and X. Xu, "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology," *MIS Quarterly,* vol. 36, no. 1, pp. 157-178, 2012.

[85] L. Yu, M. K. Duffy, and B. J. Tepper, "Consequences of downward envy: A model of self-esteem threat, abusive supervision, and supervisory leader self-improvement," *Academy of Management Journal,* vol. 61, no. 6, pp. 2296-2318, 2018.

[86] B. Yoo, N. Donthu, and T. Lenartowicz, "Measuring Hofstede's five dimensions of cultural values at the individual level: Development and validation of CVSCALE," *Journal of International Consumer Marketing,* vol. 23, no. 3-4, pp. 193-210, 2011.

[87] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly,* vol. 27, no. 3, pp. 425-478, 2003.

APPENDIX A

Construct/Adopted from:
Collectivism [86]
Individuals should sacrifice self-interest for the group.
Individuals should stick with the group even through difficulties.
Group welfare is more important than individual rewards.
Group success is more important than individual success.
Individuals should only pursue their goals after considering the welfare of the group.
Group loyalty should be encouraged even if individual goals suffer.
Uncertainty Avoidance [86]
It is important to have instructions spelt out in detail so that I always know what I'm expected to do.
It is important to closely follow instructions and procedures.
Rules and regulations are important because they inform me of what is expected of me.
Standardized work procedures are helpful.
Instructions for operations are important.
Attitude [66]
Installing contact-tracing apps on my mobile phone is a good idea.
Installing contact-tracing apps on my mobile phone is a wise idea.
I like the idea of Installing contact-tracing apps on my mobile phone.
Installing contact-tracing apps on my mobile phone would be pleasant.
Installing contact-tracing apps on my mobile phone is appealing.
Subjective Norm [87]
I think my friends and/or colleagues believe that I should install contact-tracing apps on my mobile phone.
People who influence my behaviour think that I should install a contact-tracing app on my mobile phone.
People who are important to me think I should install a contact-tracing app on my mobile phone.
I think my friends and/or colleagues believe that I should install a contact-tracing app on my mobile phone.
Privacy Self-Efficacy [10]
Protecting my information privacy is easy for me.
I have the capability to protect my information privacy.
I am able to protect my information privacy without much effort.
Perceived Effectiveness of Privacy Policy [37]
I feel confident that the contact-tracing app's privacy statements reflect their commitments to protect my personal information.
With their privacy statements, I believe that my personal information will be kept private and confidential by contact-tracing apps.

I believe that contact-tracing app's privacy statements are an effective way to demonstrate their commitments to privacy.

Perceived Effectiveness of Industry Self-Regulation [37]

I believe that the privacy seal of approval programs such as VeriSign and TRUSTe will impose sanctions for contact-tracing apps noncompliance with its privacy policy.

Privacy seal of approval programs such as VeriSign and TRUSTe will stand by me if my personal information is misused during and after using contact-tracing apps.

I am confident that the privacy seal of approval programs such as VeriSign and TRUSTe is able to address the violation of the information I provided to contact-tracing apps.

Perceived Severity [10]

If my information privacy is invaded, it would be severe.

If my information privacy is invaded, it would be serious.

If my information privacy is invaded, it would be significant.

Perceived Vulnerability [10]

My information privacy is at risk of being invaded.

It is likely that my information privacy will be invaded.

It is possible that my information privacy will be invaded.

Information Privacy Concerns [10]

I believe that submitting information through contact-tracing apps on my mobile phone would not advisable at all.

Information through contact-tracing apps on my mobile phone would be abused for sure once submitted.

Information through contact-tracing apps on my mobile phone would be shared or sold to others once submitted.

Expected Personal Outcomes of Sharing [52]

Sharing my personal information through contact-tracing apps will help me connect with people who have similar health experiences.

Sharing my personal information through contact-tracing apps is good for my well-being.

Personal benefits of talking about my personal information through contact-tracing apps will be trivial.

There are advantages to me from communicating my personal information through contact-tracing apps.

Expected Community-Related Outcomes of Sharing [52]

Sharing my personal information through contact-tracing apps will help other community members.

Personal information that I communicate through contact-tracing apps will benefit members with similar health conditions.

Disclosing my personal information is worthless for the health community.

The personal information I share is valuable to members of this health community.

Adoption Intention [87]

I intend to install contact-tracing apps on my mobile phone in the future.

I predict that I would install contact-tracing apps on my mobile phone in the future.

I plan to install contact-tracing apps on my mobile phone in the near future.

I will always try to install contact-tracing apps on my mobile phone.

I will recommend to others to install contact-tracing apps on my mobile phone.

APPENDIX B

	A	**CR**	**AVE**	**MSV**	**Max R(H)**	**ATT**	**SUB**	**PSE**	**PEPP**	**PEIR**	**PSV**	**PVN**	**IPC**	**EPOS**	**ECRPS**	**ADI**	**COL**	**UAV**
ATT	0.951	0.951	0.797	0.544	0.957	**0.893**												

SUB	0.940	0.934	0.781	0.544	0.939	0.738***	**0.884**											
PSE	0.870	0.872	0.695	0.250	0.876	0.322***	0.263***	**0.834**										
PEPP	0.909	0.915	0.782	0.571	0.918	0.651***	0.605***	0.500***	**0.884**									
PEIR	0.880	0.882	0.713	0.571	0.885	0.534***	0.562***	0.411***	0.756***	**0.844**								
PSV	0.827	0.852	0.666	0.101	0.916	0.157***	0.166***	0.195***	0.164***	0.277***	**0.816**							
PVN	0.899	0.899	0.749	0.310	0.924	0.033	0.078†	0.078†	-0.072†	0.068	0.317***	**0.866**						
IPC	0.861	0.864	0.680	0.310	0.885	-0.096*	0.023	0.124**	-0.098*	0.076†	0.223***	0.557***	**0.825**					
EPOS	0.881	0.881	0.651	0.656	0.893	0.542***	0.515***	0.312***	0.519***	0.536***	0.125**	0.180***	0.126**	**0.807**				
ECRPS	0.736	0.800	0.542	0.656	0.903	0.468***	0.459***	0.231***	0.463***	0.482***	0.186***	0.186***	0.025	0.810***	**0.736**			
ADI	0.966	0.967	0.853	0.481	0.969	0.688***	0.645***	0.300***	0.693***	0.583***	0.104**	0.048	-0.101*	0.666***	0.633***	**0.924**		
COL	0.786	0.798	0.408	0.100	0.840	0.159***	0.187***	0.126**	0.162***	0.209***	0.104*	0.202***	0.202***	0.264***	0.317***	0.181***	**0.639**	
UAV	0.833	0.874	0.589	0.101	0.905	0.318***	0.262***	0.282***	0.249***	0.241***	0.251***	0.063	0.033	0.187***	0.201***	0.204***	0.133**	**0.767**