[1] **Abdulaziz Aborujilah***

[2] **Samir Hammami**

[3] **Mohammed Hussein Al-Sarem**

[4] **Israa Ibraheem Al_Barazanchi**

Developing a Model for Understanding the Factors that Affect Individuals' Intentions to Share Personal Information

Journal of Electrical Systems

Abstract: - With the outbreak of COVID-19, digital contact tracing (DCT) applications have been implemented to track the transmission of the highly contagious disease. However, there has been significant resistance to using these apps due to individuals' concerns about disclosing personal information. This study aimed to examine individuals' intentions to reveal their details on DCT applications. A conceptual framework was developed incorporating theories of dual calculus, Hofstede's cultural theory, information boundary theory, and individual factors. A quantitative approach was employed, using a random sampling methodology to gather data from 533 respondents. The proposed framework was validated through partial least squares path modeling. The findings revealed that COVID-19-related stress, lack of transparency, and uncertainty avoidance negatively predicted intentions to disclose personal information. Conversely, collectivism, expected community-related outcomes of sharing information, expected personal outcomes of sharing information, and information privacy concerns positively predicted intentions to disclose personal information. This research provides insights into the factors that influence the widespread acceptance of DCT applications and can assist related authorities in ensuring their successful implementation.

Keywords: Digital Contact Tracing, COVID-19-related Stress, Information Privacy Concerns, Dual Calculus, Hofstede's Cultural Theory Partial Least Squares Path Modeling

I. INTRODUCTION

As the COVID-19 pandemic spreads globally, it instigates widespread fear, anxiety, and apprehension among the public, particularly impacting specific groups such as the elderly, caregivers, and individuals with pre-existing health concerns. COVID-19 containment represents a critical challenge [1]. Notably, carriers of COVID-19 can be infectious without exhibiting symptoms, making it essential to trace and inform individuals who have encountered a positive COVID-19 patient. Manual contact tracing methods prove insufficient in effectively monitoring the virus's spread [1]. Digital Contact Tracing (DCT) applications are employed to track individuals' movements in public places, aiding in the implementation of self-isolation restrictions and avoidance of COVID-19 diagnosed cases [2]. However, the use of COVID-19 DCT applications is intricate, as users may undergo surveillance, and the anticipated health benefits are geared towards the greater societal good rather than individual advantages [3]. These applications necessitate the disclosure of personal information to trace interactions and capture locations [4], offering potential efficiency improvements over manual contact tracing. Nevertheless, the implementation of DCT apps raises significant privacy concerns, with individuals fearing the leakage or misuse of their private information [5]. DCT apps require access to confidential usage details, including position history and contact information, for effective contact tracing and prompt disclosure warnings. The apps must strike a balance between gathering necessary information, such as aggregate locations of infected users, and respecting user privacy. However, the more information users disclose, the higher the privacy threats they face [6]. This presents a classic privacy dilemma, requiring an understanding of how individuals weigh trade-offs between privacy and utility. Public opinions on these trade-offs will significantly impact the acceptance rate of these applications [6].While the deployment of DCT applications varies among countries, some nations encounter substantial opposition due to

[1] *Department of Management Information System, College of Commerce & Business Administration, Dhofar University, Salalah, Sultanate of Oman. aaborujilah@du.edu.om

[2] Department of Management Information System, College of Commerce & Business Administration, Dhofar University, Salalah, Sultanate of Oman

[3] College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia; msarem@taibahu.edu.sa

[4] Department of Communication Technology Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq

unresolved concerns about trust, consumer protection, and actual benefits [7]. To the best of the authors' knowledge, not many studies have examined how people reconcile privacy concerns with using contact tracing apps in the context of COVID-19. No such study has been conducted in Malaysia. Previous research has focused on contact tracing, symptom tracking [19][20]–[22], and the correlation between app usage and viral epidemiological spread [23]. Existing work often emphasizes discrepancies between applications in different countries [24], or delves into legal and ethical aspects such as data protection [24], [25], [26]. Addressing the question of how people perceive disclosing personal information in favor of DCT applications is crucial. Considering these concerns supports the decision-making process for the successful adoption of such apps during the COVID-19 pandemic. Understanding these factors provides insights for developers and decision-makers to consider when introducing DCT applications and promoting their adoption [27].

Hypotheses Development

Mobile Applications have revolutionized the way people shop, study, and joey. it's vital to understand how end-users see these services. so, academics are becoming more interested in examining different elements of these Applications [28]. Attempts are being made by several nations to halt or slow the spread of the COVID-19 worldwide pandemic. These efforts include social distance, avoiding crowds, and identifying and isolating cases that have been reported [29]. "Contact tracing" is one of the crucial actions to take in this case [29] [30]. "The discovery and follow-up of individuals who may have been in contact with an affected individual" is how contact tracing is defined [31]. This includes contact identification, listing, and follow-up. A DCT application is a useful tool for reducing the likelihood of interpersonal interaction. It is crucial to the quick isolation of those who are affected. It is crucial to the quick isolation of those who are affected. Additionally, using a stochastic propagation model to simulate the spread of COVID-19, DCT Applications have demonstrated effectiveness in controlling a new epidemic in the majority of cases and lowering the active number of reproduction[30]. Apps like TraceTogether (Singapore) [32], CovidSafe (Australia) [33], Stop-Covid (France) [34], arogya Setu (India) [35], and MySejahtera Malaysia (Malaysia) [36] are examples of DCT applications that have been adopted by various nations.

Accurately identifying potential contacts using the DCT Application is highly beneficial for public safety; nevertheless, user adoption is hampered by the publication of personal information that could violate user confidentially. The majority of information that has been made public may reveal personal information overtly or covertly by fusing together several data sets. Social stigma, online transgressions, and gossip based on vague facts can all result from privacy problems [37][38].

By encouraging users to assess their risk of contracting COVID-19, the Malaysian government launched the MySejahtera application in an effort to track the COVID-19 outbreak throughout the nation. Additionally, this application provides the Ministry of Health (MOH) with the information needed to implement suitable and effective defensive measures [31]. Examining the driving elements and their interactions both internally and externally is necessary to understand how people behave when releasing personal information.

The way that different countries and businesses respond to contact tracing varies greatly. The most well-known are the "data-first" strategy, which places emphasis on maintaining data monitoring and making it available to academics and health authorities, and the "privacy-first" strategy, which offers consumers more control over their personal data[25].

Singapore is one example of a data-first approach; under this strategy, the government keeps a map of all cases that is accessible to the public [39].

A privacy-first strategy is adopted in a number of other countries, including the UK, France, and Australia; it forbids sharing collected data with the general public and grants access to health institutions. There is still variance, though, with some nations agreeing to provide the data to scholars and other interested parties while others enact laws limiting access to the information[40][41]. Implementations by Google and Apple fall firmly on the privacy-first end of the spectrum; they create no open communication or location data archives and only co-locate data. These systems are primarily based on the concept conceived by the Decentralized Privacy-Preserving Proximity Tracing (DP-3 T) protocol and applied in countries like Germany, Italy, and Japan, as well as several U.S. states [25].

There has been pressure on certain major nations to alter their strategies entirely. Germany transitioned entirely to a privacy-first strategy after initially favoring a data-first strategy. In the meantime, significant technological difficulties and issues with their data-first contact tracing applications were encountered by Australia and the United Kingdom [43]. Similar technology problems have surfaced in a number of nations that have chosen to prioritize data. Because of this, it has become necessary to steer clear of Google and Apple's operating system frameworks

and instead develop proprietary software that works around the privacy and security aspects of smartphones [25]. Asia has the widest range of nations that prioritize privacy and data security. The decision-making process must take into account the democratization plan as well as these countries' prior experiences with SARS and MERS [25]. Even in its early stages, the experimental use of digital contact tracing and exposure notification is one of the most contentious and divisive. In order to notify them or medical officials when they come into contact with any specific person, it entails using citizens' personal digital devices, such as cellphones, to track their physical activities and contacts with other citizens [25].

There have been concerns raised about the moral and legal ramifications of digital DCT applications, and stringent guidelines for data collection and use are needed to safeguard the public's right to privacy [44]. Furthermore, public support is the primary determinant of a COVID-19 application's effectiveness [45].

New technology adoption is usually accompanied by high failure rates [6]. Therefore, in order to properly integrate a DCT Application into deconfinement initiatives, it is crucial to assess the criteria that may either favor or discourage its adoption [46]. A global analysis of 40 Android DCT applications' privacy and protection status was conducted by Ruoxi Sun et al. [8]. Due to the usage of risky or non-best practice cryptographic methods, it was discovered that over 50% of applications may be vulnerable to security risks.

Additionally, 72.5% involved processing private data in plain text that an attacker could be able to see. Vulnerabilities that cause security issues, like activating backup permissions and potentially copying unencrypted application data, affect about 40% of applications. Moreover, it is noteworthy that around 75% of the apps contain at least one tracker that may result in serious privacy violations.

There has been discussion over the architecture, data management, efficacy, privacy, and security of the contact tracing application since its inception [9][10]. The majority of these apps seem to protect user privacy, which means that no personally identifiable information (PII) will be shared without the express permission of the user. The aforementioned data demonstrate how the epidemic has altered peoples' decisions about sharing personal information [11]. However, the adoption of these apps has mostly been impacted by privacy concerns over contact tracing [12].

Consequently, the key to using technology to build a lasting relationship is comprehending self-disclosure behavior. To maintain more consistent relationships with their consumers, for instance, businesses would like further information about them, such as names, habits, product preferences, physical locations, and email addresses [13]. The adoption of COVID-19's digital DCT Application was examined in a study by S. Sharma et al. [2], and a survey of the majority of proposed DCT Applications was carried out by N. Ahmed et al. [14], with a greater emphasis on potential security concerns. As this was going on, Jung et al. evaluated the privacy implications associated with the sharing of contact trace data on COVID-19 patients in South Korea [15]. The Extended Unified Theory of Acceptance was used in the study by S. Sharma et al. to investigate people's expectations of these Applications [16]. A few research have concentrated on creating legal justifications for handling personal data during pandemics or drafting legislation to meet privacy concerns [17]. Other research has focused on implementation and usability difficulties [14], or vulnerability and privacy issues in design [18].

Hofstede's Cultural Perspectives

Cultural issues pertain to the prevalent beliefs, viewpoints, and principles within a community. At the global, organizational, community, and individual levels, as well as in the context of information systems, culture plays a major influence in the adoption of new technology [47]. The acceptability and implementation of technology by society is significantly influenced by societal norms and expectations [47], [48].

In light of the foregoing, Hofstede's Cultural Theory can investigate how cultural differences affect perceptions of DCT applications and information privacy [49]. According to Hofstede's [50] theory of culture, collectivism is the extent to which an individual prioritizes the good of society over their own interests. In a collectivist society, decisions and actions are made with the best interests of the community in mind [49][51][52]. According to privacy study based on Hofstede's cultural theory, collectivists are more likely to approve of the sharing of personal information since they value societal welfare [53]. According to this view, individualism is also defined as the extent to which people join groups within a community. Individuals in communities that prioritize individualism are seen as essential components of themselves and their close family members; hence, a high level of individualism indicates that personal goals take precedence over shared objectives [54]. In nations like the US, Australia, and the UK, where individualism is highly valued, people tend to be self-oriented. Nonetheless, in nations like Latin America where people value more affiliation over individualism—collectivist nations—people have a strong desire

to be a part of their communities [55]. In the context of COVID-19 social digital tracking, countries and Individuals and nations differ in cultural dimensions like individualism versus collectivism when it comes to COVID-19 social digital tracking. Shavneet et al.'s study demonstrated the influence of these factors on the adoption of DCT applications during the COVID-19 pandemic. Given the same circumstances under which digital contact tracing applications operate, the following theory is put forth..

H1: Collectivist behavior of individuals positively influences people's attitudes toward disclosing their personal information on DCT Applications.

H2: Collectivist behavior negatively influences people's privacy concern about sharing their personal information on DCT Applications.

The main goal of Hofstede's Cultural Theory is to combine a society's tolerance for ambiguity and uncertainty. It expresses how much a specific culture's populace is accustomed to ambiguity and the unknown. People from cultures that are risk-averse find it difficult to deal with uncertainty. In order to protect themselves from the unknown, societies that avoid high levels of confusion see ambiguity as a danger and uphold the law [31]. Avoiding a lot of ambiguity is common in highly regulated cultures [56]. Data protection becomes more of a concern in strong ambiguity-avoidance cultures, according to Cao and Everard [57]. Higher concerns about identity privacy are a result of avoiding ambiguities, according to another study on privacy [58]. These folks are less likely to do contact tracing and to have positive attitudes. Risk-averse people are less likely to utilize the program because it is new and demands personal information [2]. Given the same circumstances under which digital contact tracing applications operate, the following theory is put forth.

H3: Uncertainty avoidance behavior of individuals postivlay influences people's attitude toward disclosing their personal information on DCT Applications.

Calculus Privacy Perspective

The notion of privacy calculus, which proposes that an individual's decision to disclose information in a particular situation is based on a comparison of perceived risks and anticipated rewards, is a prominent method for evaluating information disclosure activities by individuals [35][60][61][61]. It proves that online self-disclosures are the main focus of the cost-benefit trade-off [62]. The social position hypothesis states that men and women behave differently in social situations because of differing societal and cultural expectations. This leads to differences in the privacy calculation between genders [63].

The willingness of smartphone users to divulge their location and other personal information as a need for the successful launch of mobile location-based advertisements (MLBA) is one example of the privacy calculus use cases [60]. Additionally, this idea has gained widespread acceptance as a means of characterizing consumers' intentions to divulge personal information in a variety of settings, such as social commerce [16], location-based services [65][66][67], and electronic commerce [64].

Regarding the gathering and management of data, the virtual world has presented a number of privacy challenges [68]. Research has shown that when people are concerned about their privacy, they are less inclined to provide personal information on the internet [69]. Among the several behavioral perspectives regarding the exposure of personal information are privacy considerations. The majority of individuals are worried about sharing personal information and are growing more antagonistic toward technologies that can do so [2]. As a result, studies on online privacy protection have focused more on examining and evaluating people's unfavorable opinions regarding data disclosure [70].

According to Ketelaar and van Balen [71], end users' privacy concerns are the reason behind their unfavorable attitude toward disclosing personal information on telephone-embedded surveillance systems. The following theory is put forth in relation to contact tracking applications during the COVID-19 pandemic.

H4: Uncertainty Avoidance positively influence people’s security concerns about sharing their personal information on DCT Applications.

When it comes to the disclosure of personal information, a person decides whether to share personal information after being fully aware of the expected personal consequences [72]. For instance, people consent to disclose their personal data in exchange for specific financial or social benefits, with the understanding that there won't be any unfavorable effects in the future. [73][2]. According to Chung [74], the expected personal outcome is a way for people to support each other by sharing personal information. Furthermore, research by Atkinson et al. [75] revealed that those with less health problems are more willing to provide personal information to virtual health communities

in order to receive psychological support from other members of these communities. It is noteworthy, therefore, that people want to provide personal information in order to benefit themselves.

According to Min et al., people disclose more personal information on social networking sites (SNS) because they believe these platforms are helpful for showcasing themselves [76]. When it comes to mobile applications, customers are more likely to give personal information to the service provider in exchange for tailored offerings like product recommendations or vouchers at a discount. They understand the benefits of providing their information to the mobile app after receiving the services [77]. People are more willing to give their personal information on DCT applications when it comes to COVID-19 because of the personal benefits of information sharing [2]. Given the same circumstances under which digital contact tracing applications operate, the following theory is put forth.

H5: Personal expected outcomes of sharing information positively influence people's attitudes toward disclosing personal information on DCT Applications. Another concept included in the privacy calculus model is the anticipated social benefit of sharing personal data. Its main goal is to explain how attitudes toward disclosing personal information to the public relate to the advantages that the community enjoys [78]. For instance, in the online realm, people can only receive and offer social assistance if they are willing to share their knowledge and personal information for the good of the greater community [79]. It is anticipated that people would make use of contact tracking applications in order to aid the larger community and stop the COVID-19 virus from spreading. Individuals who have a strong emotional bond with their communities are more inclined to lend support and assist in resolving issues [78]. However, it is the individual's responsibility to utilize the app to assist the group and provide location and health information. People who are committed to monitoring positive patient interactions on behalf of the community are probably going to see the application favorably [2]. Given the same circumstances under which digital contact tracing applications operate, the following theory is put forth.

H6: Expected community benefits of sharing information positively influence people's attitude toward disclosing personal information on DCT Applications.

Information Boundary Perspective

The theory of contact privacy management, also known as information border theory, explains how individuals decide what personal information should be disclosed and to whom [80][59]. Petronio is credited with founding this notion [50, 51]. People create guidelines based on research on interpersonal communication to determine what information they are willing to disclose [81]. These guidelines are predicated on the importance of the data to be disclosed, the participant's personality, the surrounding circumstances, and an interconnected risk-benefit analysis. For example, a person with higher privacy sensitivity might not feel at ease disclosing health-related data to health information systems [82]. This gives rise to a novel idea: data-use transparency. Gaining the trust and confidence of users requires transparency. When users have greater control over their personal data and processes are straightforward, reversible, and consistent, users are more likely to feel confident in an application. Users can view the data that has been gathered about them and receive alerts about the methods and purposes of data collection thanks to data-use transparency features [83]. According to earlier studies, using techniques to improve openness may help allay privacy concerns since they promote reciprocity and boost the perception of procedural fairness [65][86]. It also increases people's willingness to pay for services on websites that make their personal information easily accessible and comprehensible[87]. Transparency, though, may also have the opposite outcome. People's level of anxiety may increase dramatically if they become aware of the extent to which information is gathered and utilized [88]. By learning about user behaviors and issues, data can also be used for other advantageous goals (such as enhancing overall service) [82]. However, it can be managed to gain direct financial gain through the selling of information to third parties or through the use of targeted adverts. People are more concerned about what information is collected and how it will be used when services are opaque [85][89]. Transparency-enhancing tactics have been studied in the past in an effort to reduce privacy concerns and boost service usage [83][90][87]. Privacy guarantees are part of this [90]. Control can enhance risk-taking and lessen the sense of danger. This conduct has a stronger real-world basis. Nonetheless, the relationship between control and objective risks is invariably inverse. The impression of power is frequently deceptive; even in the face of significant hazards that may come from information recipients beyond the sender's control, people may feel strongly in control when determining what to tell and to whom [91].

This exemplifies the power paradox. Individuals who believe they have more control over the disclosure of personal information tend to be less aware of how easily such information can be accessed and used by others [91]. The DCT

Application's unclear and opaque nature would ultimately make it more difficult for individuals to assist with digital contact tracking initiatives. Due to the global decline in public trust, a lot of people have thought about the debate over data and privacy balance, which will surely assume the worst of their government's efforts. COVID-19 functions as a formidable barrier to public institution trust on a national and international level[25]. If the authorities can ensure complete transparency and regulatory guarantees against the misuse of data emanating from this ecosystem, the adoption rate among users can be greatly accelerated [83]. As DCT Applications work in a similar context, the following hypothesis is proposed.

H7 Privacy concerns influences positively data transparenc of DCT applications.

H8: Compliance with Data Transparency rules and regulations positively influences people's attitude toward disclosing personal information on DCT applications.

According to earlier studies, people's perceptions of the hazards they face influence their preventive behavior [93][94]. For example, Renwen Zhang's study found that stress-buffering affects people's decision to disclose personal information on Facebook in relation to their activity on social media networks. Most of the time, people would rather share everything with those who give them social support than very little with strangers [95]. Regarding COVID-19, there is evidence of increased levels of depression and post-traumatic stress symptoms (PTSS) after COVID-19 infection, even if there is currently little knowledge on the direct impact of COVID-19 on mental wellness.

Regarding the indirect effects of COVID-19, there is evidence of a rise in anxiety and depression symptoms as well as a detrimental effect on general mental health, especially among medical professionals [96]. Consequently, the likelihood that someone may install the software increases with their level of anxiety regarding the COVID-19 crisis' consequences [46]. Given the same working environment of digital contact tracing applications, the following conjecture is put forth.

H9: Personal stress of COVID-19 influences people's attitudes toward disclosing personal information on DCT Applications.

II.RESEARCH MODEL

Mobile applications have revolutionized the way people shop, study, and engage with others. It is vital to understand how end-users perceive these services, prompting academics to examine various elements of these applications [28]. In the context of the global COVID-19 pandemic, nations are employing different strategies to halt or delay its spread, including social distancing, preventing large gatherings, and identifying and isolating reported cases [29]. A crucial step in this situation is "contact tracing" [29] [30], defined as the discovery and follow-up of individuals who may have been in contact with an affected person, involving the identification, listing, and follow-up of contacts [31]. Digital Contact Tracing (DCT) applications serve as effective tools to minimize potential interactions among individuals and play a crucial role in the rapid isolation of infected individuals. They have demonstrated efficiency in managing new epidemics and reducing the active number of COVID-19 cases through a stochastic propagation model [30]. Different countries, including Singapore, Australia, France, India, and Malaysia, have adopted DCT applications like TraceTogether, CovidSafe, Stop-Covid, Arogya Setu, and MySejahtera Malaysia, respectively. While accurate detection of possible contacts through DCT applications is beneficial for public safety, the disclosure of personal information poses a challenge to user adoption. Privacy risks, such as social stigma and online violations, arise due to the potential misuse or leakage of personal data [37][38]. In Malaysia, the MySejahtera application, launched by the government, aims to track the country's COVID-19 outbreak and provide the Ministry of Health with necessary details for defensive measures [31]. Understanding how people behave toward disclosing personal information involves exploring influencing factors and their internal and external interactions. Notably, different nations and companies exhibit varying approaches to contact tracing. The "data-first" approach emphasizes data preservation and accessibility to health authorities, while the "privacy-first" approach prioritizes user control over their data [25]. The implementation of digital contact tracing has faced ethical and legal concerns, demanding strict conditions on data collection to protect privacy interests [44]. Public support is crucial for the effectiveness of COVID-19 applications [45], and analyzing parameters influencing DCT application adoption is essential for successful implementation [46]. Studies, such as those by Ruoxi Sun et al. [8], have analyzed the security and privacy status of DCT applications globally, revealing potential security threats and handling of confidential information. Privacy concerns, especially related to contact tracing, significantly impact the acceptance of these applications [12]. This study aims to contribute to the understanding of individuals' behavior regarding personal information disclosure during the COVID-19 pandemic in Malaysia.

Hofstede's Cultural Perspectives

Cultural attitudes profoundly impact the adoption of new technology, with Hofstede's Cultural Theory providing insights into information privacy issues and attitudes toward DCT applications [49]. Collectivist behavior positively influences people's attitudes toward disclosing personal information on DCT applications (H1), while it negatively influences privacy concerns (H2). Uncertainty avoidance behavior positively influences people's attitudes toward disclosing personal information (H3).

Calculus Privacy Perspective

The privacy calculus theory, assessing information disclosure actions based on cost-benefit analysis, is applied to DCT applications. Uncertainty avoidance positively influences people's security concerns (H4). Personal expected outcomes of sharing information positively influence attitudes toward disclosing personal information (H5), and expected community benefits of sharing information positively influence attitudes toward disclosure (H6).

Information Boundary Perspective

Information boundary theory explores how individuals decide when, to whom, and what personal information to reveal. Privacy concerns positively influence data transparency (H7), and compliance with data transparency rules positively influences attitudes toward disclosing personal information (H8).

Stress-buffering due to personal stress of COVID-19 positively influences attitudes toward disclosing personal information on DCT applications (H9).

III. Conceptual Framework

The research objective of this study is to examine and explore the variables that form and affect the attitude of individuals in Malaysia towards revealing their personal information on DCT Applications apps. Fig. 1 shows the theoretical model of this study in which "Intention to disclose personal information" was treated as a dependent variable and other constraints as independent variables.

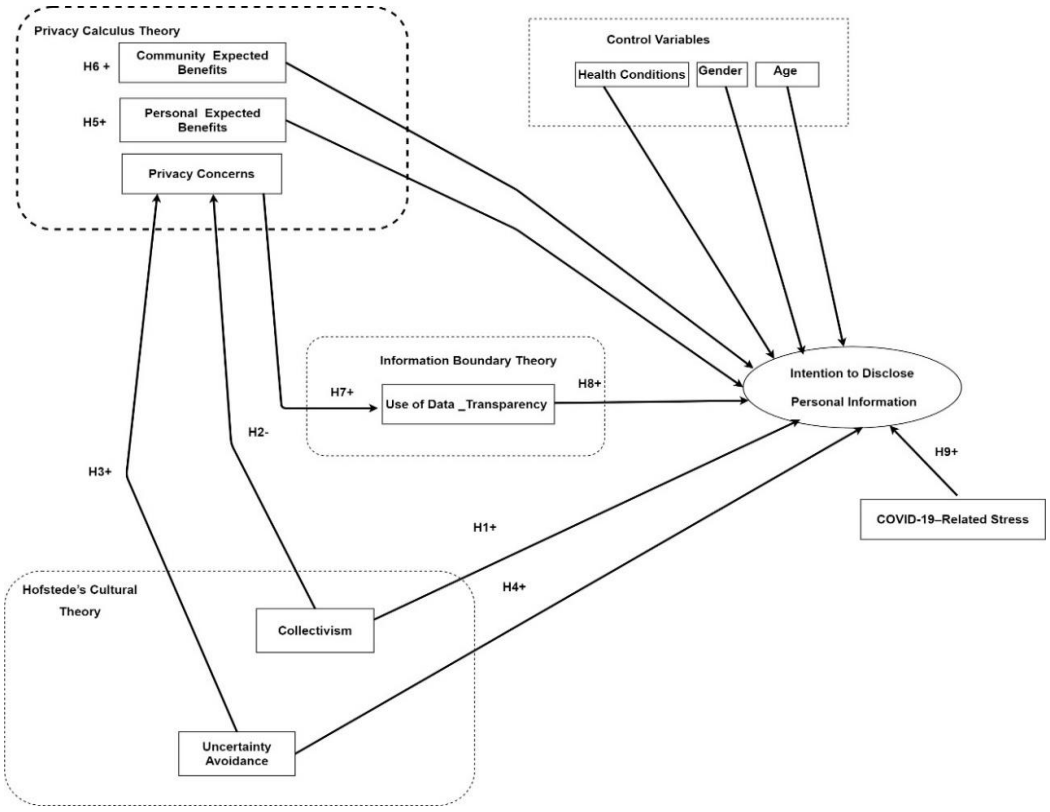

Fig 1: Theoretical Model

IV. Research Method

A full survey was conducted through a Google Form and distributed via social media networks such as Facebook, WhatsApp, and Twitter. The survey aimed to gather insights into the attitudes of individuals, specifically university

students in Malaysia, toward disclosing personal information on DCT applications. The survey yielded a total of 576 participants, and after data cleaning, 533 valid responses were obtained. No incentives were provided to participants, as they were deemed aware of the study's importance.

Participants And Procedures

The research specifically targeted university students in Malaysia, given their familiarity with mobile applications. The majority of university students are also generally in good health conditions, leading to potential disinterest in using DCT applications due to perceived low COVID-19 infection risk.

Sample Selection

The study employed a stratified random sampling method to ensure a representative sample. The target population was students from the University of Kuala Lumpur (UniKL), chosen due to easy access and existing contact with this university. UniKL comprises 12 campuses, 14 institutes, and 140 programs. Students from different levels and institutes were selected, and Table 1 provides details of the sample demographics.

Table 1: Participants Demographic Profile

Qualification	N	%	Gender	N	%
Bachelor	315	58.76866	Female	281	52.42537
Diploma/ Certificate	158	29.47761	Male	255	47.57463
Don't wish to indicate	9	1.679104	Qualification	N	%
Master	13	2.425373	Bachelor	315	58.76866
PhD	10	1.865672	Diploma/ Certificate	158	29.47761
Foundation	31	5.783582	Don't wish to indicate	9	1.679104
			Master	13	2.425373
Age	N	%	PhD	10	1.865672
18-21	252	47.01493	Foundation	31	5.783582
22-31	256	47.76119	Health Status	N	%
32-41	20	3.731343	Excellent	202	37.68657
42-51	7	1.30597	Fair	10	1.865672
52-61	1	0.186567	Good	109	20.33582
			Poor	2	0.373134
			Very good	213	39.73881

Table 2: Research Constructs Abbreviation

Constructs	Abbreviation
Transparency	TP
Collectivism	CS
Information Privacy Concerns	IPC
Expected Personal Outcomes of Sharing	EPO
Expected Community-Related Outcomes of Sharing	ECO
Intention to disclose personal information	IDI
COVID 19 Related Stress	COS
Uncertainty Avoidance	UC

V.RESULTS

Table 3 shows that the loadings for all the items exceeded the recommended value of 0.5. Therefore, the items in the model fulfilled all the requirements except the item IPC2 which was eliminated from the scale due to low loadings.

Table 3: Cross-Loading Values of Research Constructs

Indicators	COS	CS	ECO	EPO	IPC	IDI	TP	UC
COS1	0.889							
COS2	0.778							
COS3	0.910							

CS1		0.768						
CS2		0.785						
CS3		0.851						
CS 1			0.897					
ECO2			0.910					
ECO3			0.822					
EPO1				0.893				
EPO2				0.898				
EPO3				0.860				
IDI1						0.823		
IDI2						0.852		
IDI3						0.842		
IDI4						0.747		
IPC1					0.693			
IPC2					0.478			
IPC3					0.875			
TP1							0.877	
TP2							0.904	
TP3							0.781	
UC1								0.609
UC2								0.780
UC3								0.853
UC4								0.832

Table 4: Confirmatory Factors Values

	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
COS	0.829	0.895	0.741
CS	0.732	0.844	0.643
ECO	0.850	0.909	0.770
EPO	0.860	0.915	0.781
IPC	0.583	0.733	0.50
IDI	0.836	0.889	0.667
TP	0.814	0.891	0.732
UC	0.771	0.855	0.599

Table 5: Discriminant Validity

	COS	CS	ECO	EPO	IPC	IDI	TP	UC
COS	0.861							
CS	0.500	0.802						
ECO	0.440	0.545	0.877					
EPO	0.341	0.523	0.781	0.884				
IPC	0.290	0.382	0.552	0.596	0.701			
IDI	0.429	0.575	0.769	0.715	0.439	0.817		
TP	0.415	0.597	0.470	0.515	0.427	0.465	0.856	
UC1	0.498	0.567	0.404	0.378	0.277	0.419	0.551	0.774

The structural equation model was the SEM analysis' second key procedure. Following the validation of the measurement model, the structural model representation was created by identifying the connections between the constructs. The structural model, according to Hair et al [98], offers details on the relationships between the variables. Hair et al. [98] advised evaluating the structural model by using a bootstrapping approach with a resample

of 5,000 to look at the beta (β), R^2, and associated t-values. They also suggested that the effect sizes (f^2) and predictive relevance (Q^2) be reported. The p-value, according to Sullivan and Feinn [100], indicates if an impact occurs but does not indicate the size of the impact. Figure 1 depicts the PLS bootstrapping (T Statistics) findings obtained using PLS 3.0. Table 6 shows the structural model assessment which provides the indication of the hypothesis tests. Hypotheses H1, H9, and H9 were rejected. COVID19_related_stress, transparency, and uncertainty avoidance insignificantly predicted Intention to Disclose, PI. Collectivism, expected community-related Outcomes of Sharing information, Expected Personal Outcomes of Sharing information, and Information Privacy Concerns predicted Intention to Disclose significantly. Hence, H2, H3, H4, H6, and H9 were accepted with (□□□□□□□□□□□□□t □□□□□□□□□□p < 0.001); (□□□□□□□□□□□□□t □□□□□□□□□□p < 0.001) ; (□□□□□□□□□□□□□t □□□□□□□□□□p < 0.001); and (□□□□□□□□□□□□□t □□□□□□□□□□p < 0.001) respectively. On the other hand, Information Privacy Concerns was found to significantly predict Collectivism, Transparency, and Uncertainty Avoidance. Hence, H5, H7, and H9 were supported with (□□□□□□□□□□□□t □□□□□□□□□□p < 0.001); (□□□□□□□□□□□□□t □□□□□□□□□□p < 0.001); and (□□□□□□□□□□□□□t □□□□□□□□□□p < 0.001) respectively.

Table 6: Hypothesis Testing Results

H		β	T Statistics	P Values	Decision
H1	COS-> IDI	0.053	1.488	0.137	Not supported
H2	CS-> IDI	0.158	3.963	0.000	Supported
H3	ECO-> IDI	0.451	8.451	0.000	Supported
H4	EPO-> IDI	0.256	4.971	0.000	Supported
H5	IPC -> CS	0.388	8.950	0.000	Supported
H6	IPC -> IDI	0.065	3.201	0.001	Supported
H7	IPC -> TP	0.433	10.881	0.000	Supported
H8	IPC-> UC	0.281	5.975	0.000	Supported
H9	TP -> IDI	-0.012	0.346	0.730	Not supported
H9	UC -> IDI	0.031	0.769	0.442	Not supported

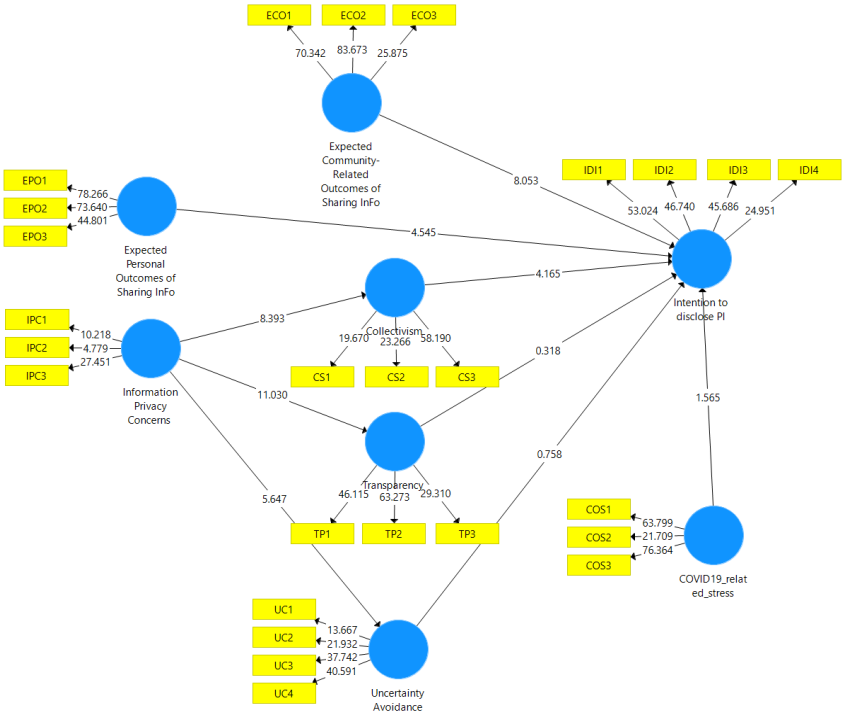

Fig 2: Research Model

A. Model Fit Indicators: Goodness of Fit

According to Hair et al. [100], there has been a controversy about the usage of goodness-of-fit within PLS-SEM. PLS-SEM does not have a well-defined global goodness-of-fit metric; it is mostly used for theoretical testing and confirmation. However, some studies, such as Henseler [101] have begun to construct goodness-of-fit measurements inside the PLS-SEM framework. The standardized root means square residual (SRMR), which evaluates the squared disparity between observed and model-implied correlations, was established by Henseler et al. to assess a model, with values less than 0.08 considered a good fit. Fit values can be used to test the model's fitness if the PLS is consistent. We may infer that the data fits the model well because the SRMR was equal to 0.08. The R^2 value represents how much variance independent variables is explained by independent factors. As a result, a higher R^2 value increases the structural model's prediction power. It's critical to make sure the R^2 values are high enough for the model to have at least some explanatory power [102]. For the explained variance of a given endogenous construct to be considered adequately, Miller and Falk [102] advised that the R^2 values be equal to or greater than 0.10. R^2 is large, according to Cohen [103]When it is more than 0.26 with acceptable power above 0.02, and R^2 is considerable, according to Cohen, when it is bigger than 0.65 with acceptable power above 0.19. In contrast, Hair et al. [100] suggested that R^2 must be more than 0.75 to be considered significant, with acceptable power above 0.25. The structural model's R^2 findings are shown in Table 7, suggesting that all of the R^2 values were high enough for the model to reach an acceptable degree of explanatory power. Exogenous constructs were found to explain 0.65 (65%) of the variation in endogenous construct intention to reveal.

Table 7: Goodness of Fit result

	R Square
Collectivism	0.146
Intention to disclose PI	0.651
Transparency	0.182
Uncertainty Avoidance	0.077

This study also assessed effect sizes (f^2). An effect size determines whether an exogenous latent construct has a substantial, moderate, or weak impact on an endogenous latent construct [104]. Hair et al. [100] recommended testing the change in the R^2 value. [105] Cohen suggested a guideline to measure the magnitude of the f^2 of 0.35 (large effects), 0.15 (medium effects), and 0.02 (small effects). Table 5 shows the results of f^2. Table 8 shows moderation effect values. The effect sizes (f^2) were also evaluated in this study. The effect size of an external latent construct on an endogenous latent construct determines whether it has a significant, moderate, or mild influence [104]. Hair et al. [98] suggested that the change in the R^2 value be tested. [105] Cohen proposed a scale of 0.35 for big effects, 0.15 for medium effects, and 0.02 for tiny effects for calculating the size of the f^2 (small effects) [105]. The results of f^2 are shown in Table 5. The values for the moderating effect are shown in Table 8.

Table 8: Moderation Effect Values

	CS	IDI	TP	UC
COS		0.005		
CS		0.034		
ECO		0.204		
EPO		0.066		
IPC	0.171		0.222	0.083
IDI				
TP		0.000		
UC		0.001		

VI. DISCUSSION

The research delves into the perspectives of Malaysian university students regarding the disclosure of personal information on government-managed tracking applications amid the COVID-19 pandemic. The key findings can be categorized into several themes.

Insignificant Factors

The study identifies that stress related to COVID-19, data transparency, and uncertainty avoidance do not significantly influence the intention to disclose personal information. Notably, there are discrepancies in the findings on transparency and uncertainty avoidance, suggesting a potential high level of trust in government-developed tracking applications or a perception that the collected personal information is less critical.

Significant Factors

On the contrary, factors such as collectivism, expected community-related outcomes, expected personal outcomes, and concerns about information privacy emerge as significant predictors of the intention to disclose personal information. Privacy considerations play a substantial role, aligning with existing research.

Public Trust and Awareness

The study observes that privacy breaches, a concern raised in other studies, are not deemed significant by respondents, possibly attributed to government sponsorship and associated campaigns. The acceptance of tracking applications during the pandemic, despite privacy concerns, stands in contrast to apprehensions highlighted in other research.

Theoretical Contribution

The study makes a theoretical contribution by proposing a comprehensive model integrating dual calculus theory, Hofstede's cultural theory, information boundary theory, and individual factors. It emphasizes the pivotal role of privacy concerns in shaping attitudes and underscores the need for improved coordination among public health authorities in implementing tracking applications.

Implications for Practice

Practical implications underscore recommendations for designers and developers of Digital Contact Tracing (DCT) applications. Strategies include adopting privacy-by-design approaches, enabling user-friendly features like subscription cancellation and data deletion, and implementing clear agreements on transparency and accountability. The study advocates for a privacy-first approach in the development life cycle and stresses the importance of engaging users through various media channels.

VII. Conclusion

The study concludes by summarizing the main insights, emphasizing the significance of privacy in users' willingness to share personal information for COVID-19 control. Recommendations include further research on risk assessment, the establishment of transparent laws and regulations, and the necessity of managing the relationship between DCT application end-users and service providers. Acknowledging limitations in participant demographics, the study suggests exploring other age groups and integrating smart contracts to address privacy concerns. In essence, the discussion highlights the intricate interplay of factors influencing individuals' attitudes toward disclosing personal information on tracking applications, with privacy considerations emerging as a central and nuanced aspect. The findings contribute to both theoretical understanding and practical applications in the dynamic landscape of DCT application development and implementation.

Acknowledgment

This research is supported by Dhofar University in the Sultanate of Oman. We express our sincere gratitude to Dhofar University and the University of Science and Technology in Yemen for their valuable support..

References

[1] R.-M. Chen, “On COVID-19 country containment metrics: a new approach,” J. Decis. Syst., pp. 1–18, 2021.

[2] S. Sharma, G. Singh, R. Sharma, P. Jones, S. Kraus, and Y. K. Dwivedi, “Digital health innovation: exploring adoption of COVID-19 digital DCT Application,” IEEE Trans. Eng. Manag., 2020.

[3] C. Matt, “Campaigning for the greater good?–How persuasive messages affect the evaluation of DCT Application,” J. Decis. Syst., pp. 1–18, 2021.

[4] L. Lenert and B. Y. McSwain, “Balancing health privacy, health information exchange, and research in the context of the COVID-19 pandemic,” J. Am. Med. Informatics Assoc., vol. 27, no. 6, pp. 963–966, 2020.

[5] N. Mohamed and I. H. Ahmad, “Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia,” Comput. Human Behav., vol. 28, no. 6, pp. 2366–2375, 2012.

[6] Y. K. Dwivedi et al., "Research on information systems failures and successes: Status update and future directions," Inf. Syst. Front., vol. 17, no. 1, pp. 143–157, 2015.
[7] S. Trang, M. Trenz, W. H. Weiger, M. Tarafdar, and C. M. K. Cheung, "One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps," Eur. J. Inf. Syst., vol. 29, no. 4, pp. 415–428, 2020.
[8] R. Sun, W. Wang, M. Xue, G. Tyson, S. Camtepe, and D. C. Ranasinghe, "An Empirical Assessment of Global COVID-19 Contact Tracing Application ," arXiv e-prints. p. arXiv:2006.10933, Jun. 01, 2020, [Online]. Available: https://ui.adsabs.harvard.edu/abs/2020arXiv200610933S.
[9] S. Vaudenay, "Centralized or decentralized? the contact tracing dilemma," 2020.
[10] P. Farrell, "Experts raise concerns about security of coronavirus tracing app COVIDSafe," ABC Bews, 2020.
[11] T. Nabity-Grover, C. M. K. Cheung, and J. B. Thatcher, "Inside out and outside in: How the COVID-19 pandemic affects self-disclosure on social media," Int. J. Inf. Manage., vol. 55, p. 102188, 2020.
[12] E. M. Redmiles, "User Concerns & Tradeoffs in Technology-Facilitated Contact Tracing," arXiv Prepr. arXiv2004.13219, 2020.
[13] D. E. Campbell, "A relational build-up model of consumer intention to self-disclose personal information in e-commerce B2C relationships," AIS Trans. Human-Computer Interact., vol. 11, no. 1, pp. 33–53, 2019.
[14] N. Ahmed et al., "A survey of covid-19 DCT Application," IEEE Access, vol. 8, pp. 134577–134601, 2020.
[15] G. Jung, H. Lee, A. Kim, and U. Lee, "Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea," Front. public Heal., vol. 8, 2020.
[16] S. Sharma and R. E. Crossler, "Disclosing too much? Situational factors affecting information disclosure in social commerce environment," Electron. Commer. Res. Appl., vol. 13, no. 5, pp. 305–319, 2014.
[17] R. Becker, A. Thorogood, J. Ordish, and M. J. S. Beauvais, "COVID-19 Research: Navigating the European General Data Protection Regulation," J. Med. Internet Res., vol. 22, no. 8, p. e19799, 2020.
[18] C. Kuhn, M. Beck, and T. Strufe, "Covid Notions: Towards Formal Definitions--and Documented Understanding--of Privacy Goals and Claimed Protection in Proximity-Tracing Services," arXiv Prepr. arXiv2004.07723, 2020.
[19] T. M. Yasaka, B. M. Lehrich, and R. Sahyouni, "Peer-to-peer contact tracing: development of a privacy-preserving smartphone app," JMIR mHealth uHealth, vol. 8, no. 4, p. e18936, 2020.
[20] W. Cheng and C. Hao, "Case-Initiated COVID-19 Contact Tracing Using Anonymous Notifications," JMIR mHealth uHealth, vol. 8, no. 6, p. e20369, 2020.
[21] S. Wang, S. Ding, and L. Xiong, "A new system for surveillance and digital contact tracing for COVID-19: spatiotemporal reporting over network and GPS," JMIR mHealth uHealth, vol. 8, no. 6, p. e19457, 2020.
[22] K. Yamamoto et al., "Health observation app for COVID-19 symptom tracking integrated with personal health records: proof of concept and practical use study," JMIR mHealth uHealth, vol. 8, no. 7, p. e19902, 2020.
[23] D. J. Currie, C. Q. Peng, D. M. Lyle, B. A. Jameson, and M. S. Frommer, "Stemming the flow: how much can the Australian smartphone app help to control COVID-19," Public Heal. Res Pr., vol. 30, no. 2, p. e3022009, 2020.
[24] I. Ekong, E. Chukwu, and M. Chukwu, "COVID-19 mobile positioning data contact tracing and patient privacy regulations: exploratory search of global response strategies and the use of digital tools in Nigeria," JMIR mHealth uHealth, vol. 8, no. 4, p. e19139, 2020.
[25] R. A. Fahey and A. Hino, "COVID-19, digital privacy, and the social limits on data-focused public health responses," Int. J. Inf. Manage., vol. 55, p. 102181, 2020.
[26] Y. Bengio et al., "The need for privacy with public digital contact tracing during the COVID-19 pandemic," Lancet Digit. Heal., vol. 2, no. 7, pp. e342–e344, 2020.
[27] M. Walrave, C. Waeterloos, and K. Ponnet, "Adoption of a DCT Application for containing COVID-19: a health belief model approach," JMIR public Heal. Surveill., vol. 6, no. 3, p. e20572, 2020.
[28] P. Kaur, A. Dhir, S. Talwar, and K. Ghuman, "The value proposition of food delivery apps from the perspective of theory of consumption value," Int. J. Contemp. Hosp. Manag., 2021.
[29] C. Sohrabi et al., "World Health Organization declares global emergency: A review of the 2019 novel coronavirus (COVID-19)," Int. J. Surg., 2020.
[30] J. Hellewell et al., "Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts," Lancet Glob. Heal., 2020.
[31] O. O. Olu et al., "Contact tracing during an outbreak of Ebola virus disease in the Western area districts of Sierra Leone: lessons for future Ebola outbreak response," Front. Public Heal., vol. 4, p. 130, 2016.
[32] H. Stevens and M. B. Haines, "TraceTogether: Pandemic Response, Democracy, and Technology," East Asian Sci. Technol. Soc. An Int. J., vol. 14, no. 3, pp. 523–532, 2020.
[33] D. Watts, "COVIDSafe, Australia's Digital DCT Application: The Legal Issues," Aust. Digit. DCT Application Leg. Issues (May 2, 2020), 2020.
[34] F. Rowe, O. Ngwenyama, and J.-L. Richet, "Contact-tracing apps and alienation in the age of COVID-19," Eur. J. Inf. Syst., pp. 1–18, 2020.

[35] R. Gupta, M. Bedi, P. Goyal, S. Wadhera, and V. Verma, “Analysis of COVID-19 Tracking Tool in India: Case Study of Aarogya Setu Mobile Application,” Digit. Gov. Res. Pract., vol. 1, no. 4, pp. 1–8, 2020.
[36] R. Sun, W. Wang, M. Xue, G. Tyson, S. Camtepe, and D. Ranasinghe, “Vetting Security and Privacy of Global COVID-19 Contact Tracing Application ,” arXiv Prepr. arXiv2006.10933, no. June, pp. 1–13, 2020.
[37] V. Das, “Stigma, contagion, defect: Issues in the anthropology of public health,” Stigma Glob. Heal. Dev. a Res. Agenda, pp. 5–7, 2001.
[38] B. Person, F. Sy, K. Holton, B. Govert, and A. Liang, “Fear and stigma: the epidemic within the SARS outbreak,” Emerg. Infect. Dis., vol. 10, no. 2, p. 358, 2004.
[39] R. Raskar et al., “Apps gone rogue: Maintaining personal privacy in an epidemic,” arXiv Prepr. arXiv2003.08567, 2020.
[40] B. News, “Coronavirus: Essential workers in England to get tests.” .
[41] “BBC News (2020b). Million Australians download virus tracing app,” BBC. .
[42] P. H. O’Neill, T. Ryan-Mosley, and B. Johnson, “A flood of coronavirus apps are tracking us,” Now it’s time to keep track them, 2020.
[43] J. Selby, “Coronavirus latest: NHS start building second Covid-19 DCT Application with Apple and Google after MPs raise ethical issue,” news Pap., 2020.
[44] M. Ienca and E. Vayena, “On the responsible use of digital data to tackle the COVID-19 pandemic,” Nat. Med., vol. 26, no. 4, pp. 463–464, 2020.
[45] J. Abeler, M. Bäcker, U. Buermeyer, and H. Zillessen, “COVID-19 contact tracing and data protection can go together,” JMIR mHealth uHealth, vol. 8, no. 4, p. e19359, 2020.
[46] M. Walrave, C. Waeterloos, and K. Ponnet, “Ready or Not for Contact Tracing? Investigating the Adoption Intention of COVID-19 Contact-Tracing Technology Using an Extended Unified Theory of Acceptance and Use of Technology Model,” Cyberpsychology, Behav. Soc. Netw., 2020.
[47] R. Sharma, G. Singh, and S. Sharma, “Modelling internet banking adoption in Fiji: A developing country perspective,” Int. J. Inf. Manage., vol. 53, p. 102116, 2020.
[48] T. Semrau, T. Ambos, and S. Kraus, “Entrepreneurial orientation and SME performance across societal cultures: An international study,” J. Bus. Res., vol. 69, no. 5, pp. 1928–1932, 2016.
[49] G. Hofstede, “Culture and organizations,” Int. Stud. Manag. Organ., vol. 10, no. 4, pp. 15–41, 1980.
[50] W. O. Bearden, R. B. Money, and J. L. Nevins, “Multidimensional versus unidimensional measures in assessing national culture values: The Hofstede VSM 94 example,” J. Bus. Res., vol. 59, no. 2, pp. 195–203, 2006.
[51] P. Akbar, R. Mai, and S. Hoffmann, “When do materialistic consumers join commercial sharing systems,” J. Bus. Res., vol. 69, no. 10, pp. 4215–4224, 2016.
[52] P. C. Earley and C. B. Gibson, “Taking stock in our progress on individualism-collectivism: 100 years of solidarity and community,” J. Manage., vol. 24, no. 3, pp. 265–304, 1998.
[53] Y. Li, A. Kobsa, B. P. Knijnenburg, and M. H. C. Nguyen, “Cross-cultural privacy prediction,” Proc. Priv. Enhancing Technol., vol. 2017, no. 2, pp. 113–132, 2017.
[54] G. H. Hofstede, G. J. Hofstede, and M. Minkov, Cultures and organizations: Software of the mind, vol. 2. Mcgraw-hill New York, 2005.
[55] M. L. Gallén and C. Peraita, “The effects of national culture on corporate social responsibility disclosure: a cross-country comparison,” Appl. Econ., vol. 50, no. 27, pp. 2967–2979, 2018.
[56] P. G. Patterson, E. Cowley, and K. Prasongsukarn, “Service failure recovery: The moderating impact of individual-level cultural value orientation on perceptions of justice,” Int. J. Res. Mark., vol. 23, no. 3, pp. 263–277, 2006.
[57] J. Cao and A. Everard, “User attitude towards instant messaging: The effect of espoused national cultural values on awareness and privacy,” J. Glob. Inf. Technol. Manag., vol. 11, no. 2, pp. 30–57, 2008.
[58] 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,” J. Manag. Inf. Syst., vol. 27, no. 4, pp. 163–200, 2011.
[59] H. Xu, T. Dinev, J. Smith, and P. Hart, “Information privacy concerns: Linking individual perceptions with institutional privacy assurances,” J. Assoc. Inf. Syst., vol. 12, no. 12, p. 1, 2011.
[60] 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,” Comput. Human Behav., vol. 95, pp. 295–306, 2019.
[61] A. B. Ozturk, K. Nusair, F. Okumus, and D. Singh, “Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework,” Inf. Syst. Front., vol. 19, no. 4, pp. 753–767, 2017.
[62] T. Dienlin and M. J. Metzger, “An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample,” J. Comput. Commun., vol. 21, no. 5, pp. 368–383, 2016.
[63] Y. Sun, N. Wang, X.-L. Shen, and J. X. Zhang, “Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences,” Comput. Human Behav., vol. 52, pp. 278–292, 2015.

[64] H. Li, R. Sarathy, and H. Xu, “The role of affect and cognition on online consumers’ decision to disclose personal information to unfamiliar online vendors,” Decis. Support Syst., vol. 51, no. 3, pp. 434–445, 2011.
[65] H. Xu, H.-H. Teo, B. C. Y. Tan, and R. Agarwal, “The role of push-pull technology in privacy calculus: the case of location-based services,” J. Manag. Inf. Syst., vol. 26, no. 3, pp. 135–174, 2009.
[66] H. Xu, X. R. Luo, J. M. Carroll, and M. B. Rosson, “The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing,” Decis. Support Syst., vol. 51, no. 1, pp. 42–52, 2011.
[67] L. Zhao, Y. Lu, and S. Gupta, “Disclosure intention of location-related information in location-based social network services,” Int. J. Electron. Commer., vol. 16, no. 4, pp. 53–90, 2012.
[68] N. K. Malhotra, S. S. Kim, and J. Agarwal, “Internet users’ information privacy concerns (IUIPC): The construct, the scale, and a causal model,” Inf. Syst. Res., vol. 15, no. 4, pp. 336–355, 2004.
[69] 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 fourth international conference on Communities and technologies, 2009, pp. 265–274.
[70] S. Youn, “Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents,” J. Consum. Aff., vol. 43, no. 3, pp. 389–418, 2009.
[71] 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,” Comput. Human Behav., vol. 78, pp. 174–182, 2018.
[72] C.-M. Chiu, M.-H. Hsu, and E. T. G. Wang, “Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories,” Decis. Support Syst., vol. 42, no. 3, pp. 1872–1888, 2006.
[73] I. Pentina, L. Zhang, H. Bata, and Y. Chen, “Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison,” Comput. Human Behav., vol. 65, pp. 409–419, 2016.
[74] J. E. Chung, “Online social networking for health: how online social networking benefits patients,” 2011.
[75] N. Atkinson, S. Saperstein, and J. Pleis, “Using the internet for health-related activities: findings from a national probability sample,” J. Med. Internet Res., vol. 11, no. 1, p. e5, 2009.
[76] J. Min and B. Kim, “How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost,” J. Assoc. Inf. Sci. Technol., vol. 66, no. 4, pp. 839–857, 2015.
[77] K. Atchariyachanvanich, N. Mitinunwong, and B. Tamthong, “Factors affecting disclosure of personal health information via mobile application,” in 2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), 2017, pp. 203–208.
[78] N. Kordzadeh, J. Warren, and A. Seifi, “Antecedents of privacy calculus components in virtual health communities,” Int. J. Inf. Manage., vol. 36, no. 5, pp. 724–734, 2016.
[79] 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,” 2013.
[80] S. Petronio, Boundaries of privacy: Dialectics of disclosure. Suny Press, 2002.
[81] S. Petronio, “Communication boundary management: A theoretical model of managing disclosure of private information between marital couples,” Commun. theory, vol. 1, no. 4, pp. 311–335, 1991.
[82] S. Karwatzki, O. Dytynko, M. Trenz, and D. Veit, “Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization,” J. Manag. Inf. Syst., vol. 34, no. 2, pp. 369–400, 2017, doi: 10.1080/07421222.2017.1334467.
[83] N. F. Awad and M. S. Krishnan, “The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization,” MIS Q., pp. 13–28, 2006.
[84] S. Y. Ho, “Opportunities and challenges of mobile personalization: An exploratory study.,” in ECIS, 2009, vol. 2009, pp. 1211–1222.
[85] H. Treiblmaier and I. Pollach, “Users’ perceptions of benefits and costs of personalization,” ICIS 2007 Proc., p. 141, 2007.
[86] J. C. Zimmer, R. Arsal, M. Al-Marzouq, D. Moore, and V. Grover, “Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure,” Decis. Support Syst., vol. 48, no. 2, pp. 395–406, 2010.
[87] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, “The effect of online privacy information on purchasing behavior: An experimental study,” Inf. Syst. Res., vol. 22, no. 2, pp. 254–268, 2011.
[88] L. K. John, A. Acquisti, and G. Loewenstein, “Strangers on a plane: Context-dependent willingness to divulge sensitive information,” J. Consum. Res., vol. 37, no. 5, pp. 858–873, 2011.
[89] A. Acquisti and R. Gross, “Predicting social security numbers from public data,” Proc. Natl. Acad. Sci., vol. 106, no. 27, pp. 10975–10980, 2009.
[90] B. Mai, N. M. Menon, and S. Sarkar, “No free lunch: Price premium for privacy seal-bearing vendors,” J. Manag. Inf. Syst., vol. 27, no. 2, pp. 189–212, 2010.
[91] A. Acquisti, I. Adjerid, and L. Brandimarte, “Gone in 15 seconds: The limits of privacy transparency and control,” IEEE Secur. Priv., vol. 11, no. 4, pp. 72–74, 2013.

[92] A. M. Ramakrishnan, A. N. Ramakrishnan, S. Lagan, and J. Torous, “From Symptom Tracking to Contact Tracing: A Framework to Explore and Assess COVID-19 Apps,” Futur. Internet, vol. 12, no. 9, p. 153, 2020.
[93] S. Milne, P. Sheeran, and S. Orbell, “Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory,” J. Appl. Soc. Psychol., vol. 30, no. 1, pp. 106–143, 2000.
[94] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, “A meta-analysis of research on protection motivation theory,” J. Appl. Soc. Psychol., vol. 30, no. 2, pp. 407–429, 2000.
[95] E. Goffman, Stigma: Notes on the management of spoiled identity. Simon and Schuster, 2009.
[96] N. Vindegaard and M. E. Benros, “COVID-19 pandemic and mental health consequences: systematic review of the current evidence,” Brain. Behav. Immun., 2020.
[97] A. S. Acharya, A. Prakash, P. Saxena, and A. Nigam, “Sampling: Why and how of it,” Indian J. Med. Spec., vol. 4, no. 2, pp. 330–333, 2013.
[98] F. B. T. Isip, “WHAT IS THE SLOVIN’S FORMULA?”
[99] I. E. Allen and C. A. Seaman, “Likert scales and data analyses,” Qual. Prog., vol. 40, no. 7, pp. 64–65, 2007.
[100] J. F. Hair, G. T. M. Hult, C. Ringle, and M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 2nd ed. London: Thousand Oaks: SAGE., 2017.
[101] P. M. Bentler and W. Huang, “On Components, Latent Variables, PLS and Simple Methods: Reactions to Rigdon’s Rethinking of PLS,” Long Range Plann., vol. 47, no. 3, pp. 136–145, 2014.
[102] N. Urbach and F. Ahlemann, “Structural Equation Modelling in Information Systems Research Using Partial Least Squares,” J. Inf. Technol. Theory Appl., vol. 11(2), pp. 5–40, 2010.
[103] R. F. Falk and N. B. Miller, A primer for soft modeling. Akron: Ohio: University of Akron Press, 1992.
[104] D. Gefen and E. E. Rigdon, “An Update and Extension to SEM Guidelines for Administrative and Social Science Research,” MIS Q., vol. 35, no. 2, pp. 1–7, 2011.
[105] J. Cohen, “Statistical power analysis for the behavioural sciences. Hillsdale, NJ: Laurence Erlbaum Associates.” Inc, 1988.
[106] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, 2nd ed. London: Routledge, 1988.
[107] S. Fischer-Hübner, J. Angulo, F. Karegar, and T. Pulls, “Transparency, privacy and trust–Technology for tracking and controlling my data disclosures: Does this work?,” in IFIP International Conference on Trust Management, 2016, pp. 3–14.
[108] M. A. Azad et al., “A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Application ,” IEEE Internet Things J., 2020.
[109] H. Wen, Q. Zhao, Z. Lin, D. Xuan, and N. Shroff, “A study of the privacy of covid-19 DCT Application,” in International Conference on Security and Privacy in Communication Systems, 2020, pp. 297–317.
[110] H. Lian, W. Qiu, D. Yan, J. Guo, Z. Li, and P. Tang, “Privacy-preserving spatial query protocol based on the Moore curve for location-based service,” Comput. Secur., vol. 96, p. 101845, 2020.
[111] B. Rathore and R. Gupta, “A fuzzy based hybrid decision-making framework to examine the safety risk factors of healthcare workers during COVID-19 outbreak,” J. Decis. Syst., pp. 1–34, 2021.
[112] B. Yoo, N. Donthu, and T. Lenartowicz, “Measuring Hofstede’s five dimensions of cultural values at the individual level: Development and validation of CVSCALE,” J. Int. Consum. Mark., vol. 23, no. 3–4, pp. 193–210, 2011.
[113] 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,” Inf. Manag., vol. 55, no. 4, pp. 482–493, 2018, doi: 10.1016/j.im.2017.11.003.