IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 7, 2020, accepted December 20, 2020, date of publication December 30, 2020, date of current version January 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3048163

Should I Disclose My Personal Data? Perspectives From Internet of Things Services

DEBAJYOTI PAL[1], SUREE FUNILKUL[1], AND XIANGMIN ZHANG[2]

[1]School of Information Technology, King Mongkut's University of Technology Thonburi, Bangkok 10140, Thailand
[2]School of Information Science, Wayne State University, Detroit, MI 48202, USA

Corresponding authors: Debajyoti Pal (debajyoti.pal@mail.kmutt.ac.th) and Suree Funilkul (suree@sit.kmutt.ac.th)

This work was supported in part by the King Mongkut's University of Technology Thonburi (KMUTT) Research Funding.

ABSTRACT This work proposes a theoretical framework for explaining the end users' willingness to disclose their personal information to the IoT service providers, despite the known privacy risks. The Communication Privacy Management Theory and Privacy Trust Behavioral Intention Model are used as the backbone for the presented framework. The model is empirically validated by collecting data from 924 participants residing in Thailand and Singapore who are active users of at least one type of IoT service: smart home, smart healthcare or smart cities. The results suggest that trust, perceived privacy risks, perceived benefits and the level of information sensitivity affect the users' willingness to disclose their personal information. Certain cultural differences are also noticed from the two different country samples. Based upon the results, the research implications are discussed, and suggestions provided.

INDEX TERMS Information sensitivity, IoT services, personal data, privacy, trust.

I. INTRODUCTION

The Internet of Things (IoT) provide us with a variety of applications and services aiming to improve our quality of life. IoT has enabled the interconnection of billions of *"smart objects"* around us through the Internet, each of which possess a unique identifier, along with basic computing and communication functionalities [1]. The global IoT market is experiencing a steep rise and expected to reach around 1.6 trillion US dollars by 2025, almost a ten-fold increase compared to 2019 [2]. At the same time the total number of connected IoT devices worldwide is expected to have a five-fold increase to 75.44 billion, when compared to the current year [3]. This tremendous increase in the number of inter-connected *"smart objects"* implies that in the near future all the existing consumer electronic devices including the televisions, refrigerators, air-conditioners, kitchen appliances, fitness wearables to even the smart-lights will produce a huge volume of personal-identifiable information, therefore creating the possibilities of unprecedented security and privacy risks for the users. These IoT *"smart objects"* are smart enough to sense, collect, store, and analyze the users' personal data like their conversations, personal habits, health conditions, social interactions and even their financial transactions. Therefore, privacy is a big concern and one of the major barriers towards the adoption of the IoT services [4].

From the perspective of information privacy while providing the IoT services, primarily there are three types of stakeholders: a) the end users from whom personal data is collected, b) data aggregators, who are responsible for collecting and processing the end user data, and c) third-party entities i.e. those who benefit from or use the processed data for certain benefits. All the three stakeholders are benefitted from the IoT services in different ways. For example, the end users are benefitted from greater personalized IoT services like health monitoring [5], [6], personalized recommendation systems [7], smart city services [8], [9] or even intelligent smart homes [10], while the data aggregators and third-party entities can use the processed data to improve upon their current services or even provide newer ones [11]. However, considering the growing popularity of the IoT services, which in turn is resulting in a greater collection and analysis of personal data, it raises serious questions with regards to the end user privacy. The users of the IoT services do not realize the extent of personal information being collected, processed and analyzed upon. Since the collected information is often shared with relevant third parties (in most cases without an

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

end user consent), it can result in an irreversible damage or tampering of personal data, thereby resulting in serious privacy breaches. Therefore, privacy and security related research with respect to IoT services is of utmost importance and should be prioritized in order to ensure the trustworthy functioning of IoT.

Extant research focuses mainly on the technical aspects of privacy protection in an IoT environment, as in [12], [13]. Another segment of research focuses on the end user perceptions of IoT services [14]–[18], especially on the user adoption aspect and the experiences related to the use of the IoT services, rather than the privacy and security concerns. A few recent studies try addressing the security and privacy concerns in an IoT context [19]–[21], however there is no concrete conclusion as to what factors motivate the users to disclose their personal information, despite knowing the privacy risks. Likewise, very little is known about the sensitivity of the collected personal information from these personalized IoT services along with the mental model of the users (from a risk/benefit perspective) and the influence of culture in this aspect.

In this work, we focus on the privacy, and trust issues of different IoT services in a comprehensive manner and investigate the factors that prompt the end users to disclose their personal information in return for the personalized IoT services. Smart home, smart healthcare and smart cities are three most popularly used IoT services across the globe [22]. The type of information that is aggregated from these three services are varied: data from smart homes is concerned with the various activities of the users together with the energy consumption in a domestic setting, smart healthcare domain deals with more sensitive personal information of the users; particularly related to their health, while the smart cities mainly collect the users' location data along with other anonymous information for providing various e-citizen facilities. By considering data from these three different domains, it helps us to present a generic IoT service, which inherently contains a wide variety of information along with different levels of information sensitivity and personalization level. This work proposes a privacy and trust-oriented framework for IoT services based upon the Communication Privacy Management (CPM) Theory, Privacy Trust Behavioral Intention (PTBI) Model and the Hofstede's Cultural Dimension (HCD) Theory. An attempt is made to answer the following research questions:

RQ_1: Based upon the CPM theory and the PTBI model what are the factors affecting the disclosure of personal information of the IoT services?

RQ_2: Based on HCD theory how does culture affect the relationships between the various factors proposed in the research framework?

RQ_3: How does information sensitivity affect the users' intention to disclose their personal information of the IoT services?

For answering the above research questions data is collected from a large-scale survey spanning two countries (Thailand and Singapore). The collected data is analyzed using a Structural Equation Modelling approach. Results suggest that trust, perceived privacy risks and the level of information sensitivity affect the users' willingness to disclose their personal information. The users are more relaxed towards information that they consider to be less sensitive and do not mind sharing those with other third parties, as long as they get certain benefits out of such disclosures. The effect of culture is also prominent having both direct and indirect effects (via privacy control) on the willingness to disclose personal information.

The remaining article is organized as follows: Section II discusses about the research context and the background, Section III presents the research hypotheses, the research methodology is discussed in Section IV, results in Section V, Section VI provides the general discussions, while the conclusion and future work is presented in Section VII.

II. RESEARCH CONTEXT AND THEORETICAL BACKGROUND

A. RESEARCH CONTEXT

This study presents the personal informatics of the IoT services based on a user centric approach focusing specifically on the privacy and trust issues, an area where current research is lagging [23]. The success of the IoT services depends to a large extent on the value the users give to these services. This in turn is dependent on the extent of personal information that the users are willing to disclose, knowing the existing privacy risks. Therefore, the information sensitivity along with the benefits and risks of such personal information disclosure are extremely important factors for the current context. The IoT services are of different types and the characteristics of the data also different depending upon the IoT applications. Smart home, smart healthcare and smart cities are three of the most actively researched IoT domains [22] that capture the variety and heterogeneity of this platform, and hence taken up in this work. The data collected by these three domains vary with respect to their information sensitivity and personalization levels, and hence are a complete representation of the current state of IoT services.

B. PRIVACY CONCERNS: GENERAL OR CONTEXTUAL

Majority of the privacy-oriented Information Systems (IS) literatures have treated this aspect as a generic one that is concerned with the end users' personal information disclosure [24], [25]. However, with the emergence of newer technologies like IoT that has resulted in a plethora of new innovative applications and services being enjoyed by the users; there is a greater need for dealing with privacy in a more context-specific manner. The need for this contextual aspect of privacy is also echoed through some recent works by authors in [26], [27]. The privacy aspects in an IoT environment has a much bigger scope than *'who has access to whose and what type of information'*. Availability of cheap yet powerful computing services along with the recent advancements in artificial intelligence and machine learning makes it possible to analyze huge volumes of data from varied sources and types for getting specific insights like lifestyle pattern, commodity consumption, health insights or even the sexual orientation of the users [26]. Therefore, the privacy aspect in an IoT environment is challenging, and hence deserves a context-specific treatment, which has been done in this work by proposing the theoretical framework.

C. COMMUNICATION PRIVACY MANAGEMENT (CPM) THEORY

The proposed framework in this work is grounded on the CPM theory originally proposed by authors in [28]. This theory makes use of a boundary metaphor for explaining the motivations behind information disclosure governed by certain boundary rules. Majority of the CPM theory based research has been done for interpersonal scenarios like patient-doctor or parent-child relationships [28], [29], though recently this theory has been used for explaining the privacy concerns in various information and communication technology (ICT) contexts like e-commerce [30], e-health [31], social networking sites [32], [33] and e-learning [34]. Therefore, although the root of this theory is based in an offline environment, yet it has been used, empirically tested and validated for online contexts too. The CPM theory follows a rule-based approach containing three main elements: boundary rule formation, boundary condition and turbulence, all three being evident in online privacy management scenarios [35].

The boundary rule formation depends on five criteria: cost-benefit ratio, context, motivations, gender and culture [28]. In this research, the context criteria is excluded because we focus specifically on the IoT services context. Based on the rule formation, when the users disclose their personal information, they expect it to be kept in some protective domain, wherein a particular company or service provider becomes the custodian of the information and are responsible for the privacy and safety of this information as per the privacy policies. A boundary turbulence can occur when there are privacy breaches or when these custodians use the data for their benefits without taking the user's consent. The research framework that we propose is guided by the CPM theory as applied by authors in [35] and integrated with the PTBI model for answering the research questions. A more exhaustive discussion about the CPM theory can be obtained from the works in [29], [36].

In summary, the following conclusions can be drawn from the CPM theory. Initially, every individual has a well-defined personal privacy space with defined boundaries. These defined privacy boundaries are dependent on the application context, an individual's privacy perception(s) along with a risk control assessment. Second, during the process of personal information disclosure, the individuals expect that their data will be safely dealt with by the relevant companies/service providers, who act as the data (private information) custodians as per the standard privacy policies. Third, in case of any privacy disputes or violations i.e. boundary turbulence, the individuals will seek to take corrective measures e.g. by filing complaints with relevant authorities.

D. PRIVACY TRUST BEHAVIORAL INTENTION (PTBI) MODEL

Originally proposed by authors in [37], the PTBI model adds the concept of trust to the privacy paradigm and checks whether privacy affects the trust levels, which in turn affects the behavioral intention of the end users. Thus, the main contribution of the PTBI model is the empirical validation of privacy as a trust antecedent, which has been done in an e-commerce context [37]. Later, authors in [38] used this framework for checking the online privacy concerns and trust in the online websites. Trust is one of the central aspects that can decide the success or failure of any new technology or service [39]. In the IoT services context, if a user wants more personalization, then a greater amount of information is needed, and hence trust is a necessity between all the concerned stakeholders that will increase the willingness to disclose the personal information and consequently make these services a success. Since, trust has been a critical component to the success of smart homes [40], smart healthcare [41], [42] and smart cities [43], hence it is reasonable to include this construct for the proposed model.

Figure. 1 shows the proposed framework.

III. HYPOTHESES DEVELOPEMENT

A. PERSONAL INFORMATION DISCLOSURE (PID)

The primary objective of this work is to investigate the willingness of the end users to disclose their personal information in return for the personalized IoT services. Extant literature defines self-disclosure as "*the revelation of personal information such as name, preferences and demographics by an individual to another entity*" [44]. The sensitivity of the collected personal information is different for the different IoT services. For e.g., the smart homes are mainly concerned with automating various tasks for greater user convenience, simple video monitoring of the residents or even tracking the energy consumption of the household. Smart healthcare on the other hand tend to gather more sensitive information related to various health and psychological parameters of the individuals. The smart city services generally gather anonymous data from the citizens for providing various types of public utility services. In all the three cases, the end users receive some form of services in lieu of the information shared; however, the sensitivity of the information varies as per the usage context. This varying level of information sensitivity is unique to the IoT services context, and hence for this work we sub-categorize PID into two different types: (a) personal information disclosure- more sensitive (PID-MS), and (b) personal information disclosure- less sensitive (PID-LS). Data related to health and financial transactions are regarded as the sensitive ones, while all others are treated as less sensitive. This sub-categorization of PID enables us

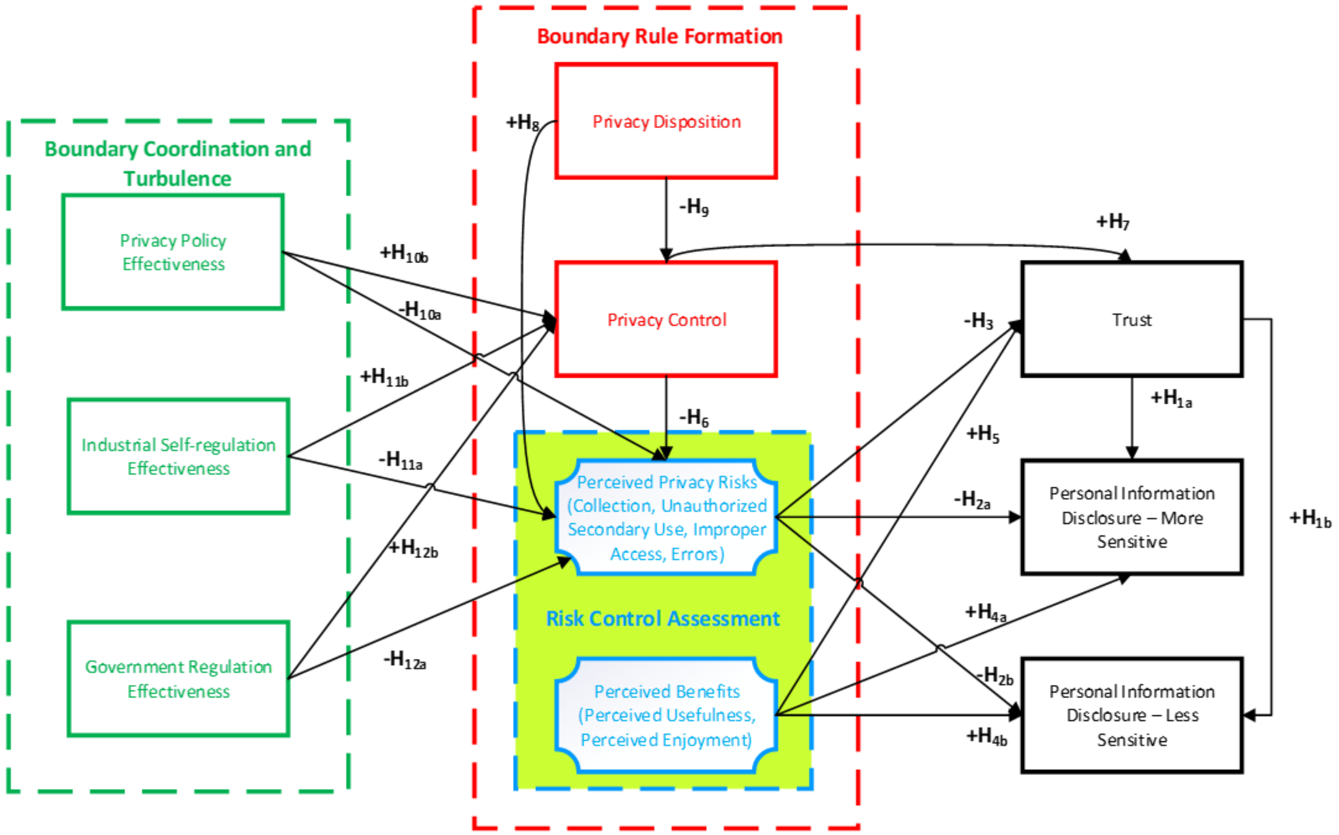
Boundary Rule Formation
Boundary Coordination and Turbulence
Privacy Policy Effectiveness
Industrial Self-regulation Effectiveness
Government Regulation Effectiveness
Privacy Disposition
Privacy Control
Perceived Privacy Risks (Collection, Unauthorized Secondary Use, Improper Access, Errors)
Risk Control Assessment
Perceived Benefits (Perceived Usefulness, Perceived Enjoyment)
Trust
Personal Information Disclosure – More Sensitive
Personal Information Disclosure – Less Sensitive
$+H_8$
$-H_9$
$+H_7$
$+H_{10b}$
$-H_{10a}$
$+H_{11b}$
$-H_{11a}$
$+H_{12b}$
$-H_{12a}$
$-H_6$
$-H_3$
$+H_5$
$+H_{1a}$
$+H_{1b}$
$-H_{2a}$
$+H_{4a}$
$-H_{2b}$
$+H_{4b}$

FIGURE 1. Proposed research framework for IoT services.

to have a holistic view of the IoT services considering their variety by including the sensitivity variation.

B. TRUST (TST)

Trust is a widely discussed construct in IS literature and considered to be a strong predictor of any type of user behavior [45]. As discussed before, the essence of trust, as presented in the PTBI model is considered in this research. The sequential relationship of the privacy, trust, intention chain is explored as per the standard PTBI framework. Trust in this work is defined as *"the end users' overall belief in the IoT service providers related to the delivery of trusted services"*. The technology empowering the IoT services is still maturing, and therefore there are several security vulnerabilities [46] that makes these services less trustable. In addition to the technology shortcomings, recently there have been several reports of unethical usage of personal data collected by the IoT service providers for their own financial benefits [47], [48]. Although privacy policies are in place, yet often due to the limited knowledge and ignorance of the users, the IoT service providers take undue advantage, thereby spoiling their credibility and reputation. If the users' loose trust in the IoT service providers, they will be less willing to disclose their personal information, which is undesirable. Thus, the following hypotheses:

H_{1a}: Trust positively affects the end users' willingness of disclosing more sensitive personal information

H_{1b}: Trust positively affects the end users' willingness of disclosing less sensitive personal information

C. BOUNDARY RULE FORMATION

As per CPM theory [28], personal information disclosure has its own benefits and risks, and therefore a contextual risk-control assessment should be done for opening/closing the privacy boundaries. When individuals disclose their personal information, they feel that they give away something that belongs to them, and therefore should have control over it, even after the disclosure [30]. Therefore, information disclosure is always associated with certain risks, which invokes the notion of creating a protective privacy boundary based on certain rules that depends on the application context [28], [30]. Next, the constructs relevant to the boundary rule formation are presented along with their relationships.

Numerous IS literatures consider perceived privacy risks (PPR) to be an important determinant of the information disclosure as well as the usage intention scenario [14], [15], [49], [50]. Authors in [51] have identified four major categories of privacy risks in relation to the information disclosure practices as: collection, unauthorized secondary use, improper access and errors. The individuals will be exposed to higher PPR levels if (a) they perceive that the service is gathering too much personal data, (b) unauthorized third parties have access to the personal data for some undisclosed reasons, or (c) if the personal data is erroneous [52]. Their results suggest that it is better to represent PPR as a second order construct, rather than a correlated set of first order factors. Based upon the works done in [51], [52] this work proposes four facets of PPR (collection, unauthorized secondary use, improper access and errors) and models them as a second order construct. Collection is defined as "*the end users' concerns related to the collection of extensive amounts of personal information by the IoT service providers*". Unauthorized secondary use refers to the *"end users' concerns that information collected for one purpose will be used by unauthorized third parties for undisclosed purposes"*. Improper access means *"the end users' concerns that the personal data collected by the IoT service providers will be accessed by other unauthorized third parties"*. Lastly, errors refer to the *"end users' concerns that inadequate procedures are used for ensuring the safety of the stored personal data collected by the IoT service providers against accidental or deliberate modifications"*. Ideally, prior to collecting information from the people, the companies should inform them as to how the collected information will be used. This will enable the end users' to better assess their privacy risks associated with information disclosure and improve their overall system trust perception. Authors in [53] suggest that individuals who are concerned more about their privacy risks are likely to read online privacy statements more than people who are less concerned, thereby signifying the importance of the trust mechanism. Therefore, it is hypothesized:

H_{2a}: Perceived privacy risks negatively affect the end users' willingness of disclosing more sensitive personal information

H_{2b}: Perceived privacy risks negatively affect the end users' willingness of disclosing less sensitive personal information

H_3: Perceived privacy risks negatively affects the end user trust

Perceived benefits (PBT) is the second construct that is used for the boundary rule formation. It is related to the financial rewards, personalization, social benefits and the motivation of the end users for using any service in return for personal information [25]. Despite knowing the risks of information disclosure, people will use a technology or service only if they are motivated enough to do so [54]. Motivation can manifest itself in two forms: intrinsic and extrinsic [54]. Only when users perceive certain benefits, they will be motivated to use a technology [14]. As per extant research, perceived usefulness and perceived enjoyment mostly reflect the benefit aspect and act as the base behind user motivation [55], [56]. For this work, perceived usefulness is defined as *"the degree to which a person believes that using IoT services will enhance his/her job performance"*. Perceived enjoyment is defined as *"the degree to which a person believes that using IoT services will be pleasurable and satisfying"*. Similar to PPR, PBT is also proposed as a second order construct. It is expected that if the users perceive benefits by using the IoT services, they will tend to trust the service providers more and voluntarily disclose their personal information. Therefore,

H_{4a}: Perceived benefits positively affect the end users' willingness of disclosing more sensitive personal information

H_{4b}: Perceived benefits positively affect the end users' willingness of disclosing less sensitive personal information

H_5: Perceived benefits positively affects the end user trust

Privacy control (PVC) is another main element of the CPM theory. The individuals believe that they are the sole owners of their personal information, and hence they should be the ones to control their privacies [28], [35], even if they give access to *'authorized others'* for using their personal data. Thus, in this work PVC is defined as "*a perceptual construct reflecting an individual's beliefs in his/her ability to manage the release and dissemination of personal information"* [35]. The essence of PVC is therefore twofold: first it refers to the individual's belief that they have full control over their personal information, and second, that they have full control over their personal information even after sharing the data with the service providers. PVC is one of the most important and widely used construct in privacy related studies [25], [35], [57]. The results from various empirical studies suggest that the individuals will have less privacy concerns and more trust on the service providers when they have a greater sense of control over the release and management of their personal information [25], [35], [57], [58]. Hence, the hypotheses:

H_6: Privacy control negatively affects the perceived privacy risks

H_7: Privacy control positively affects the end user trust

Privacy disposition (PVD) is the last relevant factor related to the boundary rule formation [28], [35]. It is a personality attribute that reflects the individuals' need to maintain a protective boundary that is a container of their personal information space. Thus, in this work PVD is defined as *"an individual's general tendency to preserve his/her personal information space or to restrain disclosure of personal information across a broad spectrum of situations and contexts"* [35]. In line with the CPM theory, PVD determines the boundary opening and closing rules, thus having a direct effect on the risk control assessment. Individuals having higher PVD values will value their privacy more than the ones having a lower score. Thus, individuals belonging to the former group will perceive higher privacy risks and concerns and feel that they have less control over their personal information. Individuals belonging to the second group are more open to share their personal information and have less concerns related to privacy risks [35]. Therefore, it is hypothesized:

H_8: Privacy disposition positively affects the perceived privacy risks

H_9: Privacy disposition negatively affects the privacy control

D. BOUNDARY CONDITION AND TURBULENCE

After an individual discloses his/her personal information with other entities, all of them become the co-owners of the information [28], [29], [36], and therefore a proper co-ordination is needed between them for ensuring the safety of the collected data. In such a shared environment, institutional assurance is a salient factor that influences the individual's decision of opening or closing their personal boundaries [35]. Extant research shows the effectiveness of such institutional mechanisms for assuring the end users about the safety of their private information [59], [60]. Company privacy policy, industry self-regulation, and government regulation are some of the most featured and effective institutional mechanisms considered by current research [59]–[61], and therefore examined in this work.

The company privacy policies play an important role in addressing the end user privacy concerns, else they will suffer reputational losses [62]. Extant privacy literatures suggest that collection of personal information by companies or service providers is perceived to be fair when the consumer is vested with notice and voice [35]. Privacy policy is a mechanism by which the companies can inform the consumers about the various ways their data will be used and means that will be taken to safeguard the collected information from misuse, loss or alteration. In this work, privacy policy effectiveness (PPE) is defined as *"the extent to which the end users believe in the accuracy, reliability, and effectiveness of the IoT service providers privacy practices as mentioned in their privacy policy"*. Recent studies have suggested that privacy policies between the consumers and the companies help in reducing the privacy risks [35], [58] and increase the consumers perceived privacy control [53]. Based on the above argument it is hypothesized:

H_{10a}: Privacy policy effectiveness negatively affects the perceived privacy risks

H_{10b}: Privacy policy effectiveness positively affects the privacy control

Industry self-regulation is the second type of institutional assurance. This type of initiative is generally undertaken by industrial groups or certifying agencies [63]. The basic purpose of such regulations is to reduce the risks in the consumers' minds by framing some policies that will protect their online privacies. These rules and policies are in addition to the existing government regulations and confirm that the business is conducted as per a fair information procedure. For example, the IoT World Alliance (a partnership between the leading telecommunication providers globally), the Trusted IoT Alliance – TIoTA (an ecosystem of more than 50 companies), and IoT Security Foundation – IoTSF are some of the global initiatives taken to assure the privacy practices specifically in the IoT services environment.

In this work, industrial self-regulation effectiveness (ISE) is defined as *"the extent to which the individuals believe that the independent IoT industrial groups, consortiums and certifying agencies are able to assist them in protecting their online privacies when they disclose their personal information"* [35]. Extant research shows that industry self-regulation programs can limit the companies' ability to behave in negative ways, and therefore create a positive environment [64]. These regulations help in improving the consumers' perception of privacy control [58], [60] and reduce the perceived privacy risks [35], [65]. Therefore, it is hypothesized:

H_{11a}: Industrial self-regulation effectiveness negatively affects the perceived privacy risks

H_{11b}: Industrial self-regulation effectiveness positively affects the privacy control

When a technology or service is new, there are more concerns associated with it, when compared to a matured service. Therefore, additional privacy preserving mechanisms should be present in such scenarios. Regulations from the government in the form of acts or legislations has been found out to be a common practice for reducing the risks of information loss [66]–[67]. However, not all people perceive that these initiatives from the government can really protect their privacy [68]. Therefore, the effectiveness of the government regulations (GRE) can help to shape the mindset of the users with respect to their privacy risks and privacy control. Hence:

H_{12a}: Government regulation effectiveness negatively affects the perceived privacy risks

H_{12b}: Government regulation effectiveness positively affects the privacy control

E. THE CULTURAL EFFECT: HOFSTEDE'S CULTURAL DIMENSION

As per CPM theory, culture has a prominent effect on the privacy perception and information disclosure scenario [28]. Empirical results from existing cross-country studies suggest that there is a close association between culture and privacy [69]. Hofstede's 6-D cultural model [70] is extremely popular, where the authors propose six different cultural dimensions and it has been adopted by several existing works [38], [69], [71].

This work considers the moderating effect of culture from the uncertainty avoidance index (UAI) dimension of Hofstede. There are two main reasons behind selecting UAI as the cultural dimension. First, the UAI dimension fits well to the IoT context taken up in this work. As per [70], UAI is defined as *"the degree to which the members of a society feel uncomfortable with uncertainty and ambiguity"*. The IoT technologies are still maturing due to which there are known security and privacy issues, which makes their future success uncertain. Therefore, how open a society will be in embracing the different services provided by this technology in future is ambiguous. Second, this study has been conducted in Thailand (UAI score = 64) and Singapore (UAI score = 8). As per the report published on Hofstede's website for the cross-country scores, as evident from above Thailand and Singapore have the biggest difference in the UAI dimension when compared to the remaining five. A higher UAI score suggests that the countries maintain rigid codes of belief and behavior and are intolerant of unorthodox behavior and ideas [70]. Therefore, fundamentally there must be a cultural difference between these two countries for the UAI dimension. Prior works in [71], [72] suggest that the UAI is more closely related to the trust in the overall system. Accordingly, the following cultural hypotheses are proposed:

H_{13a}: Culture moderates the relationship between trust and the end users' willingness of disclosing more sensitive personal information, such that lower UAI value country (Singapore) will have a stronger positive relationship than the higher UAI value country (Thailand)

H_{13b}: Culture moderates the relationship between trust and the end users' willingness of disclosing less sensitive personal information, such that lower UAI value country (Singapore) will have a stronger positive relation than the higher UAI value country (Thailand)

F. INFORMATION SENSITIVITY (INS)

Information sensitivity is related to the degree of privacy concern that a user might have while revealing a specific type of information in a specific situation [73]. Information which is riskier or uncomfortable to reveal is considered to be more sensitive [73]. Extant research shows that the users are less willing to disclose certain types of information like personal health information, credit card or bank details, or even their private conversations [73]–[75]. However, in order to provide the users with accurate and timely information, personal data must be disclosed. Clearly there is a tradeoff between the sensitivity of the disclosed information versus the personalization obtained from the IoT services in return. If the end users assign greater value to their personal information it will increase their perception of privacy risks, and they will be more hesitant to disclose it [76]. If the sensitivity in high enough, it is possible that the users will avoid disclosing their information altogether [76], which will be detrimental for the IoT services. Hence, it is hypothesized:

H_{14a}: The relationship between perceived privacy risks and the personal information disclosure (more sensitive) will be negatively stronger that the relationship between perceived privacy risks and the willingness of personal information disclosure (less sensitive)

Information sensitivity also has a close relationship with end user trust [77]. If the level of information sensitivity is high, then the presence of trust is even more critical that situations where the level of information sensitivity is low [77], [78]. Thus, it is hypothesized:

H_{14b}: The relationship between trust and the personal information disclosure (more sensitive) will be positively stronger than the relationship between trust and the willingness of personal information disclosure (less sensitive)

G. CONTROL VARIABLES

CPM theory along with other privacy related research suggests a number of other factors that must be added as control variables since they have a high influence on the privacy concerns [28], [35]. Therefore, in order to eliminate the variances explained by them this work uses age [38], [79], gender [38], privacy awareness [80] and educational level as the control variables.

IV. METHODOLOGY

A. SAMPLE AND PROCEDURE

As mentioned previously this work focuses on a two-country study of Thailand and Singapore. A survey is conducted across the three most popular IoT services (smart home, smart healthcare and smart cities). The reason behind choosing Thailand and Singapore as target countries are threefold. First, as per the UAI dimension of the HCD theory there is a remarkable difference in the scores between the two countries. Therefore, in this specific aspect the two countries are expected to be culturally different. Second, Thailand is considered to be a developing country, whereas Singapore is a developed country, which might have an effect in terms of accepting new technologies, the infrastructure available and also the privacy perception of the people. Third, since they are different countries, therefore the institutional assurances provided, specifically that of the government regulations will be different. As a consequence, the effectiveness of such regulations may be different for both the countries, that might in turn influence the privacy disclosure scenario.

For data collection, an online survey method is used for both the countries. It is a requirement that the target respondents are active users of at least one of the forms of IoT services taken up in this work out of the three. For this, a screening question is used like "*Are you currently using any form of smart home, smart healthcare or smart city services/applications?*". Those who answered 'yes' are only allowed to complete the remaining survey. Including actual users of IoT services for the sample has the following advantages. First, including actual users help to simulate the real-life usage scenario better. Second, being actual users, they can simultaneously create a mental model with regards to the benefits and risks of using the IoT services and shape an overall perception regarding the same. Third, for some of the factors that are considered while evaluating the boundary coordination and turbulence, like, government regulation effectiveness or industrial self-regulation can be better understood and appreciated only by those who are regular users of IoT services. Therefore, in this work we chose to include actual users of IoT services, and not futuristic users. Before the actual survey administration, a small in-house pilot testing is done with 10 subjects, all of them having considerable prior experiences in using IoT services for checking the understandability and easy comprehensibility of the questionnaire. Based upon the recommendations, some of the questionnaire items are revised before the actual survey. A mixture of convenience and snowball sampling techniques are used for the purpose of survey distribution. The survey invitations are distributed by using various social-media platforms, mainly Facebook, personal instant messaging applications (WhatsApp, Line and WeChat) and personal e-mails. It is mentioned in the survey that if the respondents want, they can

TABLE 1. Demographic information of the respondents.

Measure	Item	Sample (Thailand) N = 519		Sample (Singapore) N = 405		Sample (Combined) N = 924	
		Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Gender	Male	327	63 %	211	52.1 %	538	58.2 %
	Female	192	37 %	194	47.9 %	386	41.8 %
Age	Less than 20 years	34	6.5 %	38	9.4 %	72	7.8 %
	20 – 29 years	205	39.5 %	137	33.9 %	342	37 %
	30 – 39 years	183	35.3 %	125	30.8 %	308	33.3 %
	40 – 49 years	87	16.8 %	79	19.5 %	166	18 %
	50 years or more	10	1.9 %	26	6.4 %	36	3.9 %
Education	High school	36	6.9 %	39	9.6 %	75	8.1 %
	Bachelors	244	47 %	155	38.3 %	399	43.2 %
	Masters	137	26.4 %	128	31.6 %	265	28.7 %
	Doctoral	32	6.2 %	17	4.2 %	49	5.3 %
	Vocational	70	13.5 %	66	16.3 %	136	14.7 %
Frequency of using IoT services	Occasionally	43	8.3 %	57	14.1 %	100	10.8 %
	Sometimes	128	24.7 %	91	22.5 %	219	23.8 %
	Often	132	25.4 %	113	27.9 %	245	26.5 %
	Usually	115	22.1 %	107	26.4 %	222	24 %
	Always	101	19.5 %	37	9.1 %	138	14.9 %
Most used IoT services	Smart home	162	31.2 %	168	41.5 %	330	35.7 %
	Smart healthcare	251	48.4 %	143	35.3 %	394	42.6 %
	Smart cities	106	20.4 %	94	23.2 %	200	21.7 %
Privacy awareness	Concerned	331	63.8 %	206	50.9 %	537	58.1 %
	Not concerned	188	36.2 %	199	49.1 %	387	41.9 %

further forward the survey to their friends, relatives or other acquaintances who are IoT service users. Total 562 responses are obtained from Thailand and 423 responses from Singapore. After cleansing, the final amount of usable data for analysis is 519 for Thailand and 405 for Singapore, making a total of 924 usable responses for the combined sample. The demographic information is shown in Table 1.

B. SCALE DEVELOPMENT

All the items used for measurement in this study are adapted from previous privacy related literatures and rephrased to suite the present research context. The 5-point Likert scale is used for item measurements (strongly disagree to strongly agree). The complete questionnaire details along with the relevant references are provided in Table 2.

V. RESULTS

A. PARTIAL LEAST SQUARES STRUCTURAL EQUATION MODELLING (PLS-SEM)

PLS-SEM is used for the purpose of data analysis. The samples from Thailand and Singapore are compared based on the cultural dimension. For the purpose of data analysis both samples are combined due to the following main reasons. First, both the population sample represent active IoT service users, and hence they have already disclosed their personal information to the IoT service providers. Second, most of the research hypotheses that are proposed in this work are relevant for both the sample population. Therefore, combining the samples will be helpful in generalizing the results and findings of this work. Additionally, a larger sample size means more demographic variation in terms of the age, gender, culture, privacy awareness and previous privacy experience that should better represent a real world IoT service usage scenario. Third, as per the HCD theory there are certain similar cultural dimensions between the two countries. For example, both the countries represent a collectivist and feminine society (based upon almost similar individualism and feminine scores). Because of all the mentioned reasons above both the samples are merged for the purpose of overall data analysis.

The reason behind selecting PLS as the algorithm in this study has several reasons. First, this technique is aimed to maximize the variance explained by the latent variables. Thus, its primary objective is to predict the target constructs [82]. Since the objective of this study is to predict the factors influencing the personal information disclosure scenario, therefore PLS is ideally suited for this purpose. Second, PLS has a high accuracy in estimating the second-order formative constructs without specific modifications [82]–[84]. Third, PLS allows the simultaneous testing of all the mediation effects and minimum bias, which is superior to a simple linear regression where each mediation path is tested individually.

B. DESCRIPTIVE STATISTICS AND THE MEASUREMENT MODEL

A Confirmatory Factor Analysis (CFA) is conducted for checking the convergent validity of each item in the SmartPLS 3.0 software. The convergent validity is assessed from a triple viewpoint of the factor loadings of each item in the measurement model, the composite reliability (CR) and the average variance extracted (AVE) [82]. The following criteria are checked: (a) a CR value of at least 0.6, and (b) AVE value of greater than 0.5 as per the Fornell Larcker criterion [83]. The internal consistency of the questionnaire is also measured by evaluating the Cronbach's Alpha (α) values, all of which

TABLE 2. Questionnaire details.

Construct	Items	Description
Trust ([81])	TST_1	The IoT service providers are trustworthy
	TST_2	I trust the IoT service providers as they keep my best interests in mind
	TST_3	The IoT service providers will go to any extent for protecting my privacy
	TST_4	I believe that the IoT service providers handle my personal information securely and efficiently
Personal Information Disclosure ([57])	$PID–MS_1$	I am willing to provide my financial information like bank and credit card details for using the IoT services
	$PID–MS_2$	I am willing to share data my personal health records for getting better health recommendations and staying fit
	$PID–LS_1$	I am willing to share my real time location information for using the IoT services
	$PID–LS_2$	I do not mind revealing my name, address or other social security details for getting better citizen services
Perceived Privacy Risks: Collection/Unauthorized Secondary Use/Improper Access/Errors ([50-52]	CLC_1	I am concerned that the IoT service providers are collecting too much personal information about me
	CLC_2	It bothers me to give so much personal information to so many IoT service providers
	USU_1	The IoT service providers should never share my personal information with third parties without my authorization
	USU_2	The IoT service providers should never sell my personal information to other companies for their benefit
	USU_3	The IoT service providers should not use my personal information for any purpose without my approval
	IMA_1	The IoT service providers should put more efforts for preventing unauthorized access to personal information
	IMA_2	The IoT service providers should ensure that unauthorized person cannot access data of their customers
	IMA_3	Using stronger security mechanisms by the IoT service providers will improve the safety of personal information
	ERR_1	IoT service providers must give more efforts to verify the accuracy of personal information stored in their databases
	ERR_2	IoT service providers should take more steps to ensure the accuracy of personal information stored in their files
	ERR_3	All personal information present in the IoT service providers' database must be double checked for accuracy- no matter how much it costs
Perceived Benefits: Perceived Usefulness/Perceived Enjoyment [14]	PCU_1	Using the IoT services helps improving my daily work/life performance
	PCU_2	Using the IoT services helps me accomplish my work more quickly and efficiently
	PCU_3	Using the IoT services enhances the effectiveness of my work
	PCE_1	I enjoy using the different IoT services provided by my IoT service provider
	PCE_2	Using the IoT services is great fun
	PCE_3	I experience a lot of pleasure while using the IoT services
Privacy Control [35]	PVC_1	I believe that I have control over my how my personal information is used by the IoT service providers
	PVC_2	I believe that I have control over what personal information is released by the IoT service providers
	PVC_3	I am doubtful of having control over my personal information that I provide to the IoT service providers
	PVC_4	I think that I have control over what personal information is released by the IoT service providers
Privacy Disposition [35]	PVD_1	Compared to others, I am more sensitive about the way my IoT service provider handles my personal information
	PVD_2	To me, it is the mos important thing to keep my information privacy
	PVD_3	Compared to others, I am not so much concerned about the threats to my information privacy
Privacy Policy Effectiveness [35, 38]	PPE_1	With their privacy statements, I believe that my personal information will be kept private and confidential by the IoT service providers
	PPE_2	I believe that the IoT service provider's privacy statements are an effective way to demonstrate their commitments to privacy
	PPE_3	I feel confident that the IoT service provider's privacy statements reflect their commitments to protect my personal information
Industrial Self-regulation Effectiveness [35, 60]	ISE_1	I believe that the privacy seal of approval programs will impose sanctions on the IoT service providers for non-compliance with privacy policies
	ISE_2	The privacy seal provided by the competent IoT certifying authorities will stand by me if my personal information disclosed to the IoT service providers is misused
	ISE_3	I am confident that the privacy seal of the IoT certifying authorities is able to address violations of the information I provide to the IoT service providers
Government Regulation Effectiveness [35]	GRE_1	I believe that existing government laws will impose sanctions on the IoT service providers for non-compliance with privacy policies
	GRE_2	I believe that the existing legislative acts will help protect my personal information that I disclose to the IoT service providers from misuse
	GRE_3	I am confident that the government is able to address violations of my personal information that I disclose to the IoT service providers

are above the recommended level of 0.7 [82]. Table 3 shows the result details of the CFA analysis.

For examining the discriminant validity, the AVE value of each construct is compared with the shared variances between factors. The Fornell Larcker criteria for discriminant validity states that the variance extracted for each item must be greater than any squared correlation among the items, implying that the items are empirically distinct [83]. Alternatively, the square root of AVE for each item must be more than the correlation coefficient between the other items. Table 4 shows the results of discriminant validity test where all the conditions are satisfied (diagonal elements representing the square root of AVE are greater than the off-diagonal elements). Thus, the measurement model achieves both reliability and construct validity.

Since this is a survey study, there can be a threat from the Common Method Variance (CMV), which needs to be examined. For this, two statistical tests are done. First a

TABLE 3. Result of CFA analysis for the measurement model.

Construct	Mean	Std. Dev	AVE	CR	VIF Values	Cronbach's α
TST	3.96	1.48	0.74	0.92	1.66	0.86
PID – MS	2.94	1.61	0.88	0.94	1.95	0.87
PID – LS	3.78	1.72	0.60	0.75	2.25	0.79
PPR: CLC (Second Order)	3.44	0.87	0.73	0.93	2.47	0.77
PPR: USU (Second Order)	3.21	0.92	0.84	0.94	1.25	0.88
PPR: IMA (Second Order)	3.69	1.14	0.87	0.95	1.93	0.86
PPR: ERR (Second Order)	4.01	0.95	0.79	0.94	1.34	0.82
PBT: PCU (Second Order)	4.36	1.39	0.54	0.78	1.34	0.75
PBT: PCE (Second Order)	4.14	1.57	0.67	0.86	1.82	0.82
PVC	3.57	1.63	0.79	0.94	1.77	0.88
PVD	4.26	1.37	0.72	0.83	1.93	0.81
PPE	3.97	1.55	0.85	0.94	1.56	0.91
ISE	3.95	1.53	0.83	0.94	1.71	0.90
GRE	3.66	1.67	0.85	0.94	1.92	0.91

TABLE 4. Test for discriminant validity and inter-item correlation matrix.

	TST	PID-MS	PID-LS	CLC	USU	IMA	ERR	PCU	PCE	PVC	PVD	PPE	ISE	GRE
TST	**0.86**													
PID-MS	0.32	**0.94**												
PID-LS	0.51	0.45	**0.77**											
CLC	-0.49	-0.17	-0.31	**0.85**										
USU	-0.42	-0.22	-0.25	0.02	**0.92**									
IMA	-0.38	-0.26	-0.36	0.13	0.15	**0.93**								
ERR	-0.35	-0.17	-0.31	0.15	0.19	0.11	**0.89**							
PCU	0.29	0.28	0.29	-0.09	-0.24	-0.29	-0.08	**0.73**						
PCE	0.27	0.13	0.32	-0.11	-0.27	-0.32	-0.12	0.22	**0.82**					
PVC	0.57	0.19	0.11	-0.32	-0.30	-0.33	-022	0.19	0.26	**0.89**				
PVD	0.62	0.06	0.17	0.28	0.31	0.35	0.21	0.18	0.22	-0.25	**0.85**			
PPE	0.28	0.17	0.28	-0.24	-0.37	-0.29	-0.35	0.33	0.19	0.29	0.30	**0.92**		
ISE	0.25	0.23	0.25	-0.29	-0.32	-0.26	-0.31	0.30	0.15	0.26	0.28	0.31	**0.91**	
GRE	0.33	0.16	0.32	-0.27	-0.33	-0.22	-0.29	0.27	0.16	0.22	0.32	0.34	0.35	**0.92**

Harman's Single factor Test is conducted to examine whether a single factor emerges from the factor analysis or some other construct accounts for majority of the covariances among all the constructs [84]. Results show that the dominant construct explains around 31% of the covariance, which is lesser than the recommended level of 50% [84], indicating that for the present case CMV is not likely to be a major cause of concern. Second, a full collinearity test is performed for determining the presence of any construct having Variance Inflation Factor (VIF) values of equal to or greater than 3.3 [85]. Results show VIF values for all the constructs ranging between 1.20 to 2.46, again ruling out the presence of CMV. In addition, the inter-item correlation matrix (Table 4) is also analyzed for highly correlated factors, because CMV can be a problem for correlation values of greater than 0.9 (apart from the square root of the AVE) [87]. No such evidence is found.

C. STRUCTURAL MODEL: THE PATH COEFFICIENTS

After the measurement model, the structural model is tested by evaluating the path coefficients (β values) for all the proposed hypotheses. Since the framework has two second order formative constructs (PPR and PBT), while doing the path coefficient evaluation the two-step analysis approach for latent variables (repeated indicator approach) as outlined by authors in [87] is followed. The bootstrapping method is used for assessing the significance of the path coefficients with a large re-sampling size of 5000, as recommended in [88]. All the proposed hypotheses are valid, except H_{11a} and H_{12a} as evident from the results for the combined sample presented in Table 5. The structural model is shown in Figure. 2.

D. PLS MULTI-GROUP ANALYSIS

The PLS Multi Group Analysis is performed for analyzing the significant statistical differences for each of the path coefficients that might be present in the country-specific samples. The multi group analysis is performed as per the procedure outlined in [89]. As before, the same 5000 re-sampling size is used for the bootstrapping method. The results of this analysis are presented in Table 6. A particular result is significant if the p-value is either less than 0.05 or greater than 0.95 (at 5% error level) for a specific difference between the path coefficients.

The results indicate the presence of some significant differences for some of the paths. For example, the two samples differ significantly with respect to the trust and the willingness of disclosing more sensitive as well as less sensitive personal information (hypotheses $\mathbf{H_{13a}}$ and $\mathbf{H_{13b}}$) to the IoT

TABLE 5. Results of the structural model (combined sample).

Hypothesis		β Value	T Statistics	Significance Level	Status
Theoretical Constructs	H_{1a}: TST -> PID–MS	0.16	3.45	$p < 0.001$	Supported
	H_{1b}: TST -> PID-LS	0.18	4.41	$p < 0.001$	Supported
	H_{2a}: PPR -> PID-MS	-0.19	4.95	$p < 0.001$	Supported
	H_{2b}: PPR -> PID-LS	-0.09	2.46	$p < 0.05$	Supported
	H_3: PPR -> TST	-0.25	5.75	$p < 0.001$	Supported
	H_{4a}: PBT -> PID-MS	0.10	2.66	$p < 0.01$	Supported
	H_{4b}: PBT -> PID-LS	0.46	11.79	$p < 0.001$	Supported
	H_5: PBT -> TST	0.48	16.21	$p < 0.001$	Supported
	H_6: PVC -> PPR	-0.13	2.75	$p < 0.01$	Supported
	H_7: PVC -> TST	0.34	9.54	$p < 0.001$	Supported
	H_8: PVD -> PPR	0.39	11.55	$p < 0.001$	Supported
	H_9: PVD -> PVC	-0.21	5.62	$p < 0.01$	Supported
	H_{10a}: PPE -> PPR	-0.22	5.70	$p < 0.001$	Supported
	H_{10b}: PPE -> PVC	0.26	5.77	$p < 0.001$	Supported
	H_{11a}: ISE -> PPR	-0.04	0.78	$p > 0.05$	**Not supported**
	H_{11b}: ISE -> PVC	0.24	5.73	$p < 0.001$	Supported
	H_{12a}: GRE -> PPR	-0.07	0.99	$p > 0.05$	**Not supported**
	H_{12b}: GRE -> PVC	0.27	6.81	$p < 0.001$	Supported
Covariates	Age -> PID-MS	0.01	0.25	$p > 0.05$	**Not supported**
	Age -> PID-LS	0.03	0.59	$p > 0.05$	**Not supported**
	Age -> PPR	0.08	1.01	$p < 0.05$	Supported
	Gender -> PID-MS	-0.01	0.24	$p > 0.05$	**Not supported**
	Gender -> PID-LS	-0.01	0.25	$p > 0.05$	**Not supported**
	Gender -> PPR	-0.03	0.56	$p > 0.05$	**Not supported**
	Privacy Awareness -> PID-MS	0.15	4.26	$p < 0.05$	Supported
	Privacy Awareness -> PID-LS	0.02	0.34	$p > 0.05$	**Not supported**
	Privacy Awareness -> PPR	0.05	0.80	$p > 0.05$	**Not supported**
	Education -> PID-MS	-0.11	2.69	$p < 0.05$	Supported
	Education -> PID-LS	-0.05	0.81	$p > 0.05$	**Not supported**
	Education -> PPR	0.03	0.54	$p > 0.05$	**Not supported**

service providers. The next section provides a detailed discussion about the results including the theoretical and practical implications.

VI. DISCUSSION

A. RESULT ANALYSIS

The results that are obtained show that overall, the willingness to disclose personal information is affected by three main factors: trust, privacy risks and perceived benefits.

In agreement with the CPM theory the results from this study show that the end users do a risk benefit analysis of their personal information disclosure and take a decision based upon what they feel will maximize their benefits by taking minimum risks [30]. In case of less sensitive information, the perceived privacy risks of information disclosure are much lower $(H2_b, \beta = -0.09, p < 0.05)$ than the perceived benefits $(H4_b, \beta = 0.46, p < 0.001)$. On the contrary, in case of more sensitive personal information the effect of privacy risks on the information disclosure $(H2_a, \beta = -0.19, p < 0.001)$ is more prominent when compared to the effects of perceived benefits $(H4_a, \beta = 0.10, p < 0.01)$. The users use different types of IoT services, and the sensitivity of the collected personal information is different for each usage context. Therefore, it can be assumed that the users are still reluctant to disclose information which they consider to be of critical and sensitive nature, and they perceive very little benefits of information disclosure in such a scenario.

In line with the above arguments and as evident from the PLS path coefficients it can be concluded that hypothesis H_{14a} is supported. Therefore, it is safe to assume that the users do not perceive much threats to their privacy when they disclose less sensitive information to the IoT service providers. The boundary conditions of the privacy perceptions are much more relaxed in this situation, and the users may not mind even if the IoT service providers share their information with other third parties, as long as they get some benefits out of such disclosures. However, the scenario is entirely different in case of more sensitive information. The users perceive significant threats and hence are uncomfortable to share their sensitive data with the IoT service providers. There are benefits associated with this scenario too as perceived by the users like getting deeper health insights, better connectivity with health professionals, or even making easy payments via smart devices, however the privacy risks still outweigh the benefits obtained. Thus, in agreement with previous studies it is established that personal information disclosure is situation specific and depends on the sensitivity level, even though there can be benefits of such disclosures [73]–[77].

The existence of different types of personal information better explains the willingness of the users in disclosing their data to the IoT service providers. It is safe to argue

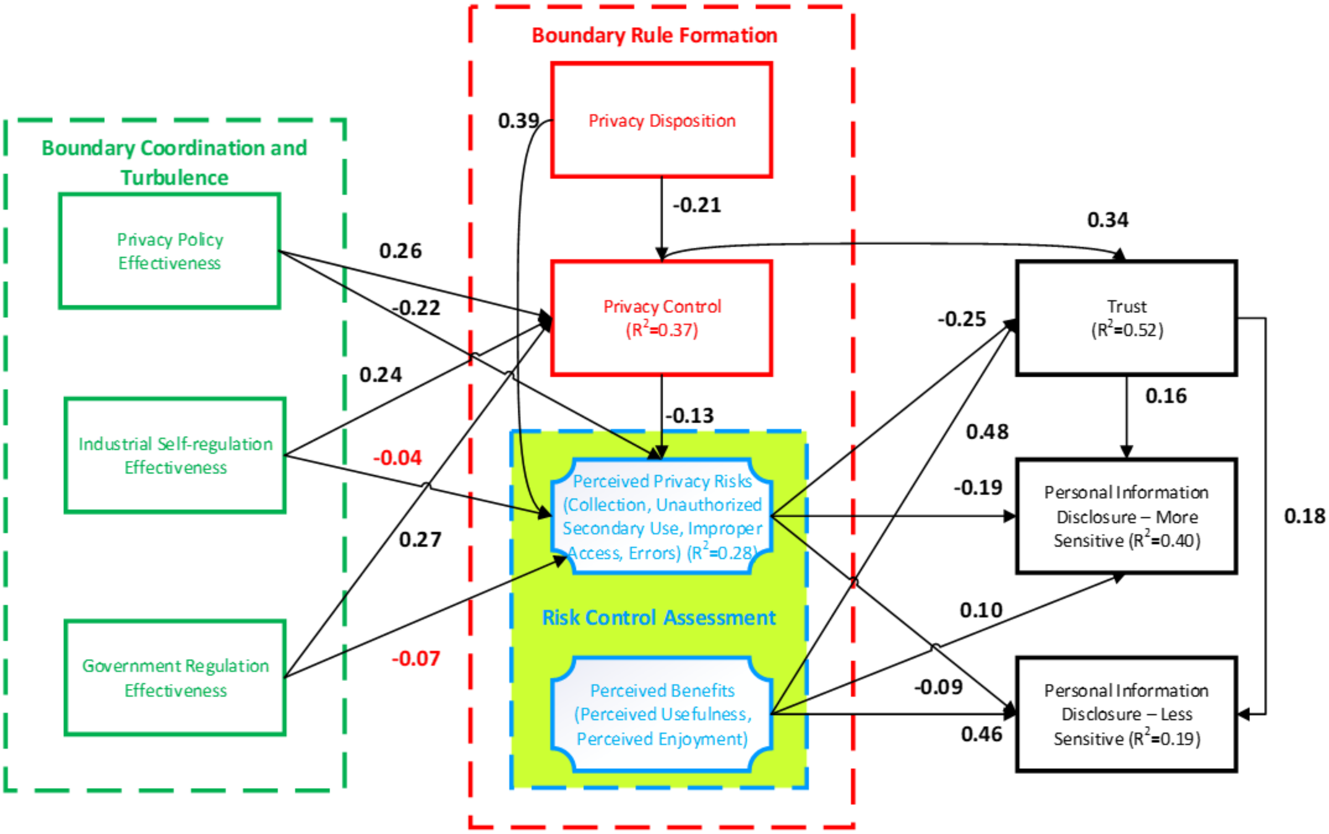
Boundary Rule Formation
Privacy Disposition
0.39
-0.21
Boundary Coordination and Turbulence
Privacy Policy Effectiveness
0.26
-0.22
Privacy Control (R²=0.37)
0.34
Trust (R²=0.52)
-0.25
0.24
Industrial Self-regulation Effectiveness
-0.13
0.16
0.48
-0.04
Perceived Privacy Risks (Collection, Unauthorized Secondary Use, Improper Access, Errors) (R²=0.28)
-0.19
Personal Information Disclosure – More Sensitive (R²=0.40)
0.18
0.27
Risk Control Assessment
0.10
Government Regulation Effectiveness
-0.07
Perceived Benefits (Perceived Usefulness, Perceived Enjoyment)
-0.09
0.46
Personal Information Disclosure – Less Sensitive (R²=0.19)

FIGURE 2. The structural model.

that the risks are much more apparent in the case of more sensitive information rather than less sensitive one. Despite the risks, the level of personalization that the users receive in return of sharing their personal details with the IoT service providers creates a positive perception, especially if the disclosed information is less sensitive. This explains that why the users are willing to disclose their personal information to the IoT service providers despite the known privacy concerns, because this "personal information" is most likely referring to the less sensitive information instead of the more sensitive information. Additionally, some of the control variables (age, privacy awareness and education) have an effect on the disclosure of more sensitive personal information. Therefore, irrespective of the information type it is clear that still the users have certain concerns with regards to their privacy, the scenario being more prominent for information having greater sensitivity.

Trust has a significant positive effect on the personal information disclosure of both types of information viz. less sensitive ($H_{1\,b}, \beta = 0.18, p < 0.001$) and more sensitive ($H_{1\,a}, \beta = 0.16, p < 0.001$). This means that when the users have a high level of trust in the IoT service providers they will willingly disclose their personal information in return of the personalized services. It is interesting to note that hypothesis H_{14b} is only partially supported. While, trust does positively affect the information disclosure scenario, however its effect is stronger for less sensitive information in case of the combined sample. Only for the sample from Singapore, the effect of trust on the willingness to disclose personal information is stronger for the more sensitive type when compared to the less sensitive type. This difference of results between the two countries clearly indicates the significance of culture as specified by the UAI dimension. Since IoT services are relatively new there are several known vulnerabilities [46], and therefore the perception of a society as a whole towards using something whose future is uncertain and ambiguous relies heavily on its culture. A greater UAI score for Thailand is indicative of a more closed and orthodox society in terms of new behavior and ideas [70]. The results further suggest that trust in the IoT service providers can be greatly enhanced by increasing the levels of privacy control ($H_7, \beta = 0.34, p < 0.001$) and lowering the perceptions of the privacy risks ($H_3, \beta = -0.25, p < 0.001$). The perceived privacy risks itself is negatively affected by the privacy policy effectiveness ($H_{10\,a}, \beta = -0.22, p < 0.001$) and privacy control ($H_6, \beta = -0.13, p < 0.01$), while privacy disposition has a positive effect ($H_8, \beta = -0.39, p < 0.001$). Out of the three institutional assurance mechanisms, privacy policy seems to be one of the most effective ones as it helps to reduce the privacy risks ($H_{10\,a}, \beta = -0.22, p < 0.001$), and also increase the privacy control ($H_{10\,b}, \beta = 0.26, p < 0.001$). This agrees with results from previous research in [38]. Considering the personalized nature of the IoT services wherein the users need to disclose a lot of their personal

TABLE 6. Multi group analysis of the structural model.

Hypothesis		PLS- Multi Group Analysis	
		Path Coefficient Difference (Thailand – Singapore)	MGA Significance Level (Thailand vs. Singapore)
Theoretical Constructs	H_{1a}: TST -> PID–MS	0.24 (Thailand 0.01, Singapore = 0.25)	0.99 (Significant)
	H_{1b}: TST -> PID-LS	0.05	0.74 (Not Significant)
	H_{2a}: PPR -> PID-MS	0.06	0.80 (Not Significant)
	H_{2b}: PPR -> PID-LS	0.05	0.21 (Not Significant)
	H_3: PPR -> TST	0.04	0.75 (Not Significant)
	H_{4a}: PBT -> PID-MS	0.06	0.21 (Not Significant)
	H_{4b}: PBT -> PID-LS	0.13	0.93 (Not Significant)
	H_5: PBT -> TST	0.08	0.89 (Not Significant)
	H_6: PVC -> PPR	0.11	0.90 (Not Significant)
	H_7: PVC -> TST	0.01	0.42 (Not Significant)
	H_8: PVD -> PPR	0.10	0.93 (Not Significant)
	H_9: PVD -> PVC	0.12	0.91 (Not Significant)
	H_{10a}: PPE -> PPR	0.02	0.41 (Not Significant)
	H_{10b}: PPE -> PVC	0.01	0.51 (Not Significant)
	H_{11a}: ISE -> PPR	0.02	0.42 (Not Significant)
	H_{11b}: ISE -> PVC	0.07	0.23 (Not Significant)
	H_{12a}: GRE -> PPR	0.04	0.66 (Not Significant)
	H_{12b}: GRE -> PVC	0.29 (Thailand = 0.12, Singapore = 0.41)	1.00 (Significant)
Covariates	Age -> PID-MS	0.04	0.71 (Not Significant)
	Age -> PID-LS	0.03	0.31 (Not Significant)
	Age -> PPR	0.14 (Thailand = -0.02, Singapore = 0.12)	0.97 (Significant)
	Gender -> PID-MS	0.06	0.14 (Not Significant)
	Gender -> PID-LS	0.11 (Thailand = -0.01, Singapore = -0.10)	0.04 (Significant)
	Gender -> PPR	0.15 (Thailand = -0.03, Singapore = 0.12)	0.99 (Significant)
	Privacy Awareness -> PID-MS	0.02	0.39 (Not Significant)
	Privacy Awareness -> PID-LS	0.01	0.56 (Not Significant)
	Privacy Awareness -> PPR	0.08	0.13 (Not Significant)
	Education -> PID-MS	0.23 (Thailand = 0.01, Singapore = -0.22)	0.01
	Education -> PID-LS	0.04	0.75 (Not Significant)
	Education -> PPR	0.05	0.24 (Not Significant)

information [14]–[18], they tend to read and examine the privacy policies critically in a comprehensive manner to ensure the safety of their disclosed information. When the users feel that they have greater control over their privacy, the privacy risks will be reduced.

For the two other institutional mechanisms industry self-regulation and government regulation, both have a strong positive effect on the privacy control (H_{11b}, $\beta = 0.24$, $p<0.001$ and H_{12b}, $\beta = 0.27$, $p<0.001$) Collectively the results show that all the three forms of institutional assurances taken up in this work help in increasing the users' privacy control perceptions. However, hypotheses H_{11a} and H_{12a} are not supported as evident from the results (H_{11a}, $\beta =-0.04$, $p>0.05$ and H_{12a}, $\beta =-0.07$, $p>0.05$). This implies that the current state of industry and government regulations are not powerful enough for mitigating the privacy risks. Additionally, privacy disposition positively influences the privacy risks ($H_8, \beta = -0.39, p < 0.001$). This result is similar to the key findings of some of the previous research in [28], [35].

Results from the PLS-MGA analysis suggest that the sample from the two countries differ along two path relationships: a) trust and disclosure of more sensitive personal information, and b) government regulation and privacy control. Thus, the effect of culture is prominent having both direct and indirect effects (via privacy control) on the willingness to disclose personal information. These findings reaffirm the importance of culture as postulated by the CPM theory itself.

B. IMPLICATIONS FOR RESEARCH

There are several theoretical implications from the results of this study. First, the CPM theory is extended and validated in the IS domain, specifically in the context of IoT services. To the best of our knowledge, applying CPM theory as the base framework and extending it with the trust concept for explaining the willingness of information disclosure in any ICT context is rather few. As pointed out in the literature review section, the basic essence of this theory was to apply it in various inter-personal contexts [28], [29], although later it was used for certain ICT contexts also [30]–[34]. Considering the importance of this theory, particularly in privacy-oriented research, we strongly feel that it has not been investigated much. Therefore, in this work an effort has been made to use the CPM theory as a guideline and integrate it with the notion of trust along with the most popular institutional assurance mechanisms in place today and applying it to the IoT services context. In doing so, the explanatory power of the model is improved within the scope of this research.

Second, considering the close relationship between trust, privacy and disclosure of personal information, this work extends CPM theory with the PTBI model. The original PTBI model along with other research based on it have empirically validated privacy to be an important trust antecedent [37], [38]. Considering the newness of the IoT services we strongly felt the need of coupling privacy and trust into one single model for explaining the information disclosure scenario. The results are positive because trust is found to be an important concept and it successfully explains the willingness of the users to disclose their personal information to the IoT service providers. Since the IoT services are new, the number of empirical works related either to the adoption of these services or understanding the user behavior are rather limited [14]–[21]. Moreover, the scope of IoT is broad covering a wide variety of services, each having different levels of information sensitivity making this application area unique. This work might be one of the earlier attempts in understanding the behavior of the IoT service users, particularly with regards to their privacy concerns and perceived risks of their personal information disclosure.

Third, the CPM theory is also extended from an information sensitivity perspective. As explained before, the success of the IoT services will depend to a great extent on the amount of personal information that the users share with their IoT service providers for getting personalized services. Depending upon the type of information the user must share, the privacy concerns can vary. However, current CPM theory-based works do not consider this angle of information sensitivity. Therefore, by extending CPM theory to include different levels of information sensitivity (more sensitive and less sensitive) maybe will lead to its further improvement by enhancing its explanatory power.

Lastly, the importance of the cultural aspect that has been mentioned in the original CPM theory, but not considered by majority of the existing CPM theory-based researches, is accounted for in this work. The Hofstede's cultural dimension model is used as the reference for examining the culture effect and results show that it has effect on two path relationships. Therefore, the importance of culture in the CPM theory is validated, particularly for the UAI dimension that has been considered in this work. Hence, now there is empirical evidence that CPM theory can be integrated and extended successfully with HCD theory.

C. IMPLICATIONS FOR PRACTICE

Based upon the results some potential insights are provided for the IoT service providers. The service providers must provide its users with comprehensive privacy protection mechanisms that will ensure that their personal information is safe and confidential. In fact, this is more relevant to information which is of more sensitive nature. The users are always worried of the fact that the information they share with their IoT service providers will be stolen, or even sold to other organizations for the purpose of profit making. Although, the findings indicate that the users are less concerned about their privacy while disclosing less sensitive personal information, yet safeguarding mechanisms should still exist. Even if the users have a slightest level of doubt regarding their privacy for any information type, they will not trust the IoT service providers completely. Therefore, trust is a very important aspect and the IoT service providers should focus more on this mutual trust building process by trying to reduce the risk perceptions as much as possible. Privacy control also has a significant impact on trust. Although, increasing the perception of privacy control is a challenging task, yet its importance in improving the trust levels cannot be undermined, especially for Thailand. The Thai society has a high UAI score of 64, which means that they value certainty [70]. Such societies feel uncomfortable with uncertainty and ambiguity [70], and therefore they value an environment of trust where the risk perceptions are minimal. Therefore, privacy control must be highly visible among the Thai users so that they are confident about their full privacy control over their information that they disclose to the IoT service providers.

Perceived benefits have a positive impact on trust as well as the willingness to disclose both types of personal information. This indicates that the users are concerned about the benefits of using IoT services, and the IoT service providers must emphasize such benefits along with the value of using these services. For example, the benefits of IoT usage like time savings, improved work performance, greater convenience and health monitoring among others should be advertised by the IoT service providers. In addition, the IoT service providers must also be aware of the enjoyment aspect of the perceived benefits and wherever appropriate seek to improve the hedonic levels by incorporating elements of fun, joy, creativity, pleasure and excitement. At the same time, the IoT service providers must employ stricter security protection mechanisms, like using stronger yet lightweight encryption functions for safeguarding the users' data. The problem is for non-technical users they will not be able to appreciate these efforts being taken from the service provider's end, not only due to the high level of technicalities involved in such procedures, but also due to their own lack of knowledge and expertise. Therefore, it is necessary to increase the awareness among the end users regarding the benefits of such techniques not only by the IoT service providers, but also by the available institutional mechanisms of a country.

Observing the importance of the privacy policies, these must explicitly mention as to how the personal information will be handled by the IoT service providers, and in the untoward incident of any information leakage whom the users can approach for remedies. In fact, the existing privacy policies should be improved and made more user-centric by nature to increase the sense of privacy control along with reducing the risks of privacy loss. Keeping in mind the cultural variations, instead of creating "*one fit all*" version of the privacy policies, they should be customized based on the specific requirements of a specific country. For example, in case of countries like Thailand, which has a high UAI score, the privacy policies must be more detailed and stricter imposing harsh punishments on those who violate the users' privacy. This will enable gaining the confidence of the end users and make them trust the IoT platform more. Strangely, the results show that industry self-regulation does not help to reduce the privacy concerns. However, this does not undermine the efforts made by the IoT industry along with the money and effort that are being put to make this platform more secure and free from risks. Based upon the results, we strongly feel that there is a lack of user knowledge and awareness related to the existence of organizations like TIoTA or IoTSF and the efforts that are being put by them for improving the security of the IoT platform. Therefore, educating and promoting awareness through proper channels are necessary to reduce the privacy risks among the end users.

As per the results, the effectiveness of the government regulation in reducing the privacy concerns is insignificant. This indicates limited regulatory control from the government with regards to personal data protection. For example, in Thailand the Personal Data Protection Act (PDPA) was just published in 2019 and will be effective from 2020. Similarly, for Singapore its data protection law is also relatively new and needs to mature more. Especially for Thailand, considering its higher UAI index score, immediate enforcement of PDPA is the need of the hour. Even if such laws exist, it makes little sense if the users are not aware of these. Therefore, such regulations need to be made public to all the IoT service users.

VII. LIMITATIONS AND CONCLUSION

To conclude, this work attempts to develop a framework and empirically evaluate the end users' personal information disclosure scenario in an IoT context based upon the CPM theory and the PTBI model. The results are tested from a two-country study of Thailand and Singapore. Trust, perceived privacy risks and perceived benefits are the factors which have the most prominent effects on the personal information disclosure. The privacy risks vary with the information sensitivity and has a greater significance in case of more sensitive information. For less sensitive information, the perceived benefits outweigh the perceived privacy risks, indicating that the users are not that much concerned while disclosing information that they consider to be less sensitive to the IoT service providers. The three types of institutional mechanisms considered in this work have a positive influence on the privacy control, however industry self-regulation and government regulations are not effective for reducing the privacy concerns. This indicates that the legislative laws related to the protection of user data privacy are still in an infant stage and needs more maturity.

Next the limitations of this work are highlighted. First, for this research a cross-sectional survey is used. However, it might not be the most appropriate method to use specially in the IoT context. The entire IoT ecosystem is rapidly evolving, and therefore the user behavior can change over time due to the dynamic nature of this environment. This can have a great effect on the privacy concerns. For example, if there is some news about any major security lapse or privacy breaches, it is surely going to influence the user behavior. Therefore, future studies can extend upon this work by not only adding more measures, but also employing a longitudinal approach of data collection to better take into account the transient nature of user behavior change. Second, this study uses a mixture of convenience and snowball sampling techniques for generalizing the samples from each country as much as possible. However, still there is a chance that the considered sample may not be representative of the entire population. Therefore, future studies should use a random sampling method when the aspect of culture is involved. Third, based upon extant research for examining the cultural variations the HCD theory is used as the reference [38], [69], [71]. However, we selected the country-wise HCD indicators which gives a national level measure and not the individual level cultural variations, which can be another limitation. Moreover, in addition to HCD theory, there is another well-known cultural framework known as the NATID (National Identity) scale [90]. It will be interesting to compare the cultural aspects based on these two different theories for further work. Finally, the statistical analysis only provides a numerical basis, while the interpretation of the results is our subjective appraisal.

REFERENCES

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012.

[2] Statista. *Global IoT Market Size 2017-2025*. Accessed: Sep. 11, 2019. [Online]. Available: https://www.statista.com/statistics/976313/global-iot-market-size/

[3] Statista. *Internet of Things–Number of Connected Devices Worldwide 2015-2025*. Accessed: Sep. 11, 2019. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[4] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, "The Internet of Things (IoT) and its impact on individual privacy: An australian perspective," *Comput. Law Secur. Rev.*, vol. 32, no. 1, pp. 4–15, Feb. 2016.

[5] S. U. Amin, M. S. Hossain, G. Muhammad, M. Alhussein, and M. A. Rahman, "Cognitive smart healthcare for pathology detection and monitoring," *IEEE Access*, vol. 7, pp. 10745–10753, 2019.

[6] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "RFID technology for IoT-based personal healthcare in smart spaces," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 144–152, Apr. 2014.

[7] A. Felfernig, S. Polat-Erdeniz, C. Uran, S. Reiterer, M. Atas, T. N. T. Tran, P. Azzoni, C. Kiraly, and K. Dolui, "An overview of recommender systems in the Internet of Things," *J. Intell. Inf. Syst.*, vol. 52, no. 2, pp. 285–309, 2019.

[8] A. Gyrard, A. Zimmermann, and A. Sheth, "Building IoT-based applications for smart cities: How can ontology catalogs help?" *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3978–3990, Oct. 2018.

[9] S. Kolozali, D. Kuemper, R. Tonjes, M. Bermudez-Edo, N. Farajidavar, P. Barnaghi, F. Gao, M. Intizar Ali, A. Mileo, M. Fischer, and T. Iggena, "Observing the pulse of a city: A smart city framework for real-time discovery, federation, and aggregation of data streams," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2651–2668, Apr. 2019.

[10] W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, "Implemented IoT-based self-learning home management system (SHMS) for singapore," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2212–2219, Jun. 2018.

[11] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[12] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 42–51, Mar. 2018.

[13] D. Pal, C. Arpnikanondt, M. A. Razzaque, and S. Funilkul, "To trust or not-trust: Privacy issues with voice assistants," *IT Prof.*, vol. 22, no. 5, pp. 46–53, Sep. 2020.

[14] C.-L. Hsu and J. C.-C. Lin, "Exploring factors affecting the adoption of Internet of Things services," *J. Comput. Inf. Syst.*, vol. 58, no. 1, pp. 49–57, Sep. 2016.

[15] D. Pal, S. Funilkul, V. Vanijja, and B. Papasratorn, "Analyzing the elderly users' adoption of smart-home services," *IEEE Access*, vol. 6, pp. 51238–51252, 2018.

[16] M. Lee, "An empirical study of home IoT services in South Korea: The moderating effect of the usage experience," *Int. J. Hum.–Comput. Interact.*, vol. 35, no. 7, pp. 535–547, Jun. 2018.

[17] D. Pal, B. Papasratorn, W. Chutimaskul, and S. Funilkul, "Embracing the smart-home revolution in Asia by the elderly: An end-user negative perception modeling," *IEEE Access*, vol. 7, pp. 38535–38549, 2019.

[18] D. Pal, C. Arpnikanondt, S. Funilkul, and W. Chutimaskul, "The adoption analysis of voice-based smart IoT products," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10852–10867, Nov. 2020.

[19] C. Park, Y. Kim, and M. Jeong, "Influencing factors on risk perception of IoT-based home energy management services," *Telematics Informat.*, vol. 35, no. 8, pp. 2355–2365, Dec. 2018.

[20] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, "The Internet of Things (IoT) and its impact on individual privacy: An australian perspective," *Comput. Law Secur. Rev.*, vol. 32, no. 1, pp. 4–15, Feb. 2016.

[21] C.-L. Hsu and J. C.-C. Lin, "An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives," *Comput. Hum. Behav.*, vol. 62, pp. 516–527, Sep. 2016.

[22] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019.

[23] D.-H. Shin, "Conceptualizing and measuring quality of experience of the Internet of Things: Exploring how quality is perceived by users," *Inf. Manage.*, vol. 54, no. 8, pp. 998–1011, Dec. 2017.

[24] 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, Dec. 2004.

[25] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quart.*, vol. 35, no. 4, pp. 989–1016, Dec. 2011.

[26] P. F. Wu, J. Vitak, and M. T. Zimmer, "A contextual approach to information privacy research," *J. Assoc. Inf. Sci. Technol.*, vol. 71, no. 4, pp. 485–490, Apr. 2020, doi: 10.1002/asi.24232.

[27] B. B. Gupta, S. Yamaguchi, and D. P. Agrawal, "Advances in security and privacy of multimedia big data in mobile and cloud computing," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 9203–9208, Apr. 2018.

[28] S. S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure*, 2nd ed. New York, NY, USA: State Univ. of New York Press, 2002.

[29] S. Petronio, "Brief status report on communication privacy management theory," *J. Family Commun.*, vol. 13, no. 1, pp. 6–14, Jan. 2013.

[30] M. J. Metzger, "Communication privacy management in electronic commerce," *J. Comput.-Mediated Commun.*, vol. 12, no. 2, pp. 335–361, Jan. 2007.

[31] S.-A.-A. Jin, "'To disclose or not to disclose, that is the question': A structural equation modeling approach to communication privacy management in e-health," *Comput. Hum. Behav.*, vol. 28, no. 1, pp. 69–77, Jan. 2012.

[32] N. Zlatolas, T. Welzer, M. Hölbl, M. Heričko, and Kamišalić, "A model of perception of privacy, trust, and self-disclosure on online social networks," *Entropy*, vol. 21, no. 8, p. 772, Aug. 2019, doi: 10.3390/e21080772.

[33] W. Xie and K. Karan, "Consumers' privacy concern and privacy protection on social network sites in the era of big data: Empirical evidence from college students," *J. Interact. Advertising*, vol. 19, no. 3, pp. 187–201, Sep. 2019, doi: 10.1080/15252019.2019.1651681.

[34] R. J. Sidelinger, M. C. Nyeste, P. E. Madlock, J. Pollak, and J. Wilkinson, "Instructor privacy management in the classroom: Exploring instructors' ineffective communication and student communication satisfaction," *Commun. Stud.*, vol. 66, no. 5, pp. 569–589, Jun. 2015.

[35] 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, pp. 798–824, Dec. 2011, doi: 10.17705/1jais.00281.

[36] J. T. Child, P. M. Haridakis, and S. Petronio, "Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use," *Comput. Hum. Behav.*, vol. 28, no. 5, pp. 1859–1872, Sep. 2012.

[37] C. Liu, J. T. Marchewka, J. Lu, and C. S. Yu, "Beyond concern—A privacy-trust-behavioral intention model of e-commerce," *Inf. Manage.*, vol. 42, pp. 289–304, Jan. 2005.

[38] K.-W. Wu, S. Y. Huang, D. C. Yen, and I. Popova, "The effect of online privacy policy on consumer privacy concern and trust," *Comput. Hum. Behav.*, vol. 28, no. 3, pp. 889–897, May 2012.

[39] J. Ejdys, "Building technology trust in ICT application at a university," *Int. J. Emerg. Markets*, vol. 13, no. 5, pp. 980–997, Nov. 2018.

[40] H. Yang, H. Lee, and H. Zo, "User acceptance of smart home services: An extension of the theory of planned behavior," *Ind. Manage. Data Syst.*, vol. 117, no. 1, pp. 68–89, Feb. 2017.

[41] D. Pal, S. Funilkul, N. Charoenkitkarn, and P. Kanthamanon, "Internet-of-Things and smart homes for elderly healthcare: An end user perspective," *IEEE Access*, vol. 6, pp. 10483–10496, 2018.

[42] V. Kulshrestra and S. Verma, "Role of trust in the ubiquitous healthcare system: Challenges and opportunities," *Sensors Health Monitor.*, vol. 5, pp. 191–212, Jan. 2019.

[43] S. Chatterjee and A. K. Kar, "Effects of successful adoption of information technology enabled services in proposed smart cities of india: From user experience perspective," *J. Sci. Technol. Policy Manage.*, vol. 9, no. 2, pp. 189–209, Jul. 2018.

[44] Y. Moon, "Intimate exchanges: Using computers to elicit self-disclosure from consumers," *J. Consum. Res.*, vol. 26, no. 4, pp. 323–339, Mar. 2000.

[45] C. V. Slyke, J. T. Shim, R. Johnson, and J. Jiang, "Concern for information privacy and online consumer purchasing," *J. Assoc. Inf. Syst.*, vol. 7, no. 6, pp. 415–444, Jun. 2006.

[46] B. Ali and A. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, Mar. 2018.

[47] S. Tzafestas, "Ethics and law in the Internet of Things world," *Smart Cities*, vol. 1, no. 1, pp. 98–120, Oct. 2018.

[48] (Mar. 6, 2019). *How Companies Profit and Use Your Personal Data*. Accessed: Nov. 8, 2019. [Online]. Available: https://cbscreening.co.uk/news/post/your-personal-data-and-how-companies-use-it/

[49] 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. Manage.*, vol. 55, no. 4, pp. 482–493, Jun. 2018.

[50] C.-L. Hsu and J. C.-C. Lin, "An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives," *Comput. Hum. Behav.*, vol. 62, pp. 516–527, Sep. 2016.

[51] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quart.*, vol. 20, no. 2, pp. 167–196, 1996.

[52] K. A. Stewart and A. H. Segars, "An empirical examination of the concern for information privacy instrument," *Inf. Syst. Res.*, vol. 13, no. 1, pp. 36–49, Mar. 2002.

[53] G. R. Milne and M. J. Culnan, "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," *J. Interact. Marketing*, vol. 18, no. 3, pp. 15–29, Jan. 2004.

[54] J. Doll and I. Ajzen, "Accessibility and stability of predictors in the theory of planned behavior.," *J. Personality Social Psychol.*, vol. 63, no. 5, pp. 754–765, 1992.

[55] K.-Y. Lin and H.-P. Lu, "Why people use social networking sites: An empirical study integrating network externalities and motivation theory," *Comput. Hum. Behav.*, vol. 27, no. 3, pp. 1152–1161, May 2011.

[56] H. Van der Heijden, "User acceptance of hedonic information systems," *MIS Quart.*, vol. 28, no. 4, pp. 695–704, 2004.

[57] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents-measurement validity and a regression model," *Behav. Inf. Technol.*, vol. 23, no. 6, pp. 413–423, 2004.

[58] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Org. Sci.*, vol. 10, no. 1, pp. 104–115, Feb. 1999.

[59] D. H. McKnight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology," *Inf. Syst. Res.*, vol. 13, no. 3, pp. 334–359, Sep. 2002.

[60] M. J. Culnan, "Protecting privacy online: Is self-regulation working?" *J. Public Policy Marketing*, vol. 19, no. 1, pp. 20–26, Apr. 2000.

[61] 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 Quart.*, vol. 30, no. 1, pp. 13–28, Mar. 2006.

[62] Z. Tang, Y. Hu, and M. D. Smith, "Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor," *J. Manage. Inf. Syst.*, vol. 24, no. 4, pp. 153–173, Apr. 2008.

[63] D. Zwick and N. Dholakia, ''Models of privacy in the digital age: Implications for marketing and E-commerce,'' Res. Inst. Telecommun. Inf. Marketing, Univ. Rhode Island, Kingston, RI, USA, Tech. Rep., Sep. 1999.

[64] A. H. Barkatullah and Djumadi, ''Does self-regulation provide legal protection and security to e-commerce consumers?'' *Electron. Commerce Res. Appl.*, vol. 30, pp. 94–101, Jul. 2018.

[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 service,'' *J. Manage. Inf. Syst.*, vol. 26, no. 3, pp. 135–173, 2009.

[66] D. Pal, S. Funilkul, and V. Vanijja, ''The future of smartwatches: Assessing the end-users' continuous usage using an extended expectation-confirmation model,'' *Universal Access Inf. Soc.*, vol. 19, pp. 261–281, Oct. 2018, doi: 10.1007/s10209-018-0639-z.

[67] N. J. King and V. T. Raja, ''Protecting the privacy and security of sensitive customer data in the cloud,'' *Comput. Law Secur. Rev.*, vol. 28, no. 3, pp. 308–319, Jun. 2012.

[68] A. Y. Chiou, J. C. Chen, and C. Bisset, ''Cross cultural perceptions on privacy in the United States, Vietnam, Indonesia, and Taiwan,'' in *Cyber Crime: Concepts, Methodologies, Tools and Applications*. Hershey, PA, USA: IGI Global, 2012, pp. 727–741, doi: 10.4018/978-1-61350-323-2.ch402.

[69] H. Krasnova, N. F. Veltri, and O. Günther, ''Self-disclosure and privacy calculus on social networking sites: The role of culture,'' *Bus. Inf. Syst. Eng.*, vol. 4, no. 3, pp. 127–135, Jun. 2012.

[70] G. Hofstede, ''Dimensionalizing cultures: The hofstede model in context,'' *Online Readings Psychol. Culture*, vol. 2, no. 1, pp. 3–25, Dec. 2011.

[71] S. Cockcroft and S. Rekker, ''The relationship between culture and information privacy policy,'' *Electron. Markets*, vol. 26, no. 1, pp. 55–72, Feb. 2016.

[72] 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. Manage. Inf. Syst.*, vol. 27, no. 4, pp. 163–200, Apr. 2011.

[73] S. Yang and K. Wang, ''The influence of information sensitivity compensation on privacy concern and behavioral intention,'' *ACM SIGMIS Database, Adv. Inf. Syst.*, vol. 40, no. 1, pp. 38–51, Jan. 2009, doi: 10.1145/1496930.1496937.

[74] S. Ward, K. Bridges, and B. Chitty, ''Do incentives matter? An examination of On-line privacy concerns and willingness to provide personal and financial information,'' *J. Marketing Commun.*, vol. 11, no. 1, pp. 21–40, Mar. 2005.

[75] A. Easwara Moorthy and K.-P.-L. Vu, ''Privacy concerns for use of voice activated personal assistant in the public space,'' *Int. J. Hum.-Comput. Interact.*, vol. 31, no. 4, pp. 307–335, Apr. 2015.

[76] B. A. Huberman, E. Adar, and L. R. Fine, ''Valuating privacy,'' *IEEE Secur. Privacy Mag.*, vol. 3, no. 5, pp. 22–25, Sep. 2005.

[77] G. Bansal, F. Zahedi, and D. Gefen, ''The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online,'' *Decis. Support Syst.*, vol. 49, no. 2, pp. 138–150, May 2010.

[78] G. Bansal, F. M. Zahedi, and D. Gefen, ''Do context and personality matter? Trust and privacy concerns in disclosing private information online,'' *Inf. Manage.*, vol. 53, no. 1, pp. 1–21, Jan. 2016.

[79] M. J. Culnan, ''Consumer awareness of name removal procedures: Implications for direct marketing,'' *J. Direct Marketing*, vol. 9, no. 2, pp. 10–19, 1995.

[80] J. Phelps, G. Nowak, and E. Ferrell, ''Privacy concerns and consumer willingness to provide personal information,'' *J. Public Policy Marketing*, vol. 19, no. 1, pp. 27–41, Apr. 2000.

[81] S. L. Jarvenpaa, N. Tractinsky, and M. Vitale, ''Consumer trust in an Internet store,'' *Inf. Technol. Manage.*, vol. 1, nos. 1–2, pp. 45–71, 2000.

[82] J. F. Hair, R. E. Anderson, R. L. Tatham, and W. C. Black, *Multivariate Data Analysis*, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1998.

[83] D. G. Kleinbaum, L. L. Kupper, and K. E. Müller, *Applied Regression Analysis and Other Multivariate Methods*, 4th ed. Boston, MA, USA: Duxbury Press, 2007.

[84] 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,'' *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879–903, 2003.

[85] N. Kock and G. Lynn, ''Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations,'' *J. Assoc. Inf. Syst.*, vol. 13, no. 7, pp. 546–580, Jul. 2012.

[86] R. P. Bagozzi, Y. Yi, and L. W. Phillips, ''Assessing construct validity in organizational research,'' *Administ. Sci. Quart.*, vol. 36, no. 3, pp. 421–458, 1991.

[87] P. B. Lowry and J. Gaskin, ''Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it,'' *IEEE Trans. Prof. Commun.*, vol. 57, no. 2, pp. 123–146, Jun. 2014.

[88] J. F. Hair, C. M. Ringle, and M. Sarstedt, ''PLS-SEM: Indeed a silver bullet,'' *J. Marketing Theory Pract.*, vol. 19, no. 2, pp. 139–151, 2011.

[89] M. Sarstedt, J. Henseler, and C. M. Ringle, ''Multi-group analysis in partial least squares (PLS) path modelling: Alternative methods and empirical results,'' *Adv. Int. Marketing*, vol. 22, no. 1, pp. 195–218, 2011.

[90] B. D. Keillor, G. T. M. Hult, R. C. Erffmeyer, and E. Babakus, ''NATID: The development and application of a national identity measure for use in international marketing,'' *J. Int. Marketing*, vol. 4, no. 2, pp. 57–73, Jun. 1996.

DEBAJYOTI PAL received the B.E. degree in electrical engineering from Nagpur University, India, in 2005, the M.Tech. degree in information technology from the Indian Institute of Engineering Science and Technology, Shibpur, Kolkata, India, in 2007, and the Ph.D. degree in information technology from the School of Information Technology, King Mongkut's University of Technology Thonburi, Bangkok, Thailand, in 2017. He is currently a Researcher with the King Mongkut's University of Technology Thonburi. His research interests include multimedia systems, quality evaluation of various multimedia services, the Internet of Things, human–computer interaction, and education technology.

SUREE FUNILKUL received the B.Sc. degree in mathematics from Mahidol University, Thailand, and the M.Sc. and Ph.D. degrees in information technology from the King Mongkut's University of Technology Thonburi, in 2008. Her research interests include information systems and database programming.

XIANGMIN ZHANG received the Ph.D. degree from the University of Toronto. He is currently an Associate Professor with the School of Information Sciences, Wayne State University, USA, where he teaches information technology related courses, including Human–Computer Interaction, information architecture, website development, and web-based information services. He also worked as a Faculty Member with Rutgers University, in mid-2000s. He has published extensively in prominent information science journals and peer-reviewed conference proceedings. He is a frequent presenter at international and national academic conferences. His research interests include information retrieval, data analytics, human–computer interaction (HCI), personalization, and user experience/interactions of information systems.