Telematics and Informatics 49 (2020) 101377

Contents lists available at ScienceDirect

Telematics and Informatics

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

Home IoT resistance: Extended privacy and vulnerability perspective

Hwansoo Lee

Department of Convergence Security, Dankook University, 152 Jukjeon-ro, Suji-gu, Yongin-si, Gyeonggi-do 16890, Republic of Korea

ARTICLE INFO

Keywords:
Home IoT
Resistance behavior
Perceived vulnerability
Physical privacy concerns
Information privacy concerns

ABSTRACT

Home Internet of Things (IoT) services are expected to augment the efficiency and comfort of users' daily lives; however, this expectation is eclipsed by concerns regarding privacy and vulnerability. While these concerns critically impact the acceptance of IoT services for the home, they have been discussed primarily from a traditional point of view; academic discussions of privacy and vulnerability in the current environment are lacking. This study extends existing privacy and vulnerability theories to demonstrate the importance of physical privacy and user vulnerability protections in home IoT environments. To validate the proposed research model, an empirical analysis was conducted on 265 samples with a partial least squares structural equation modeling technique. The differences in vulnerability factors, along with privacy concerns and resistance to home IoT services, were also compared by gender, experience, and type of housing. Results show that user vulnerability has the strongest impact on home IoT privacy concerns and resistance to home IoT environments. Additionally, this study found that personal factors appear differently across vulnerabilities, privacy concerns, and home IoT resistance. This study extends the traditional concepts of privacy and vulnerability to the home IoT environment.

1. Introduction

The Internet of Things (IoT) was selected as one of the ten emerging technologies of the 4th Industrial Revolution at the Davos Forum in 2016. IoT refers to information and communication technology (ICT) that enables intelligent services through interaction between objects connected via wired and wireless networks (Park et al., 2018). IoT technologies have been applied to various industries, including medical services, smart offices, and smart cities (Atzori et al., 2010). Among the various IoT services, Home IoT is the most representative one. Home IoT refers to "a residence equipped with a high-tech network, linking sensors and domestic devices, appliances, and features that can be remotely monitored, accessed or controlled, and provide services that respond to the needs of its inhabitants" (Balta-Ozkan et al., 2013, p. 364). This service is expected to enrich users' lives, motivating rapid technological developments of related devices.

With the recent increase in advertisements, products, and news regarding home IoT, it is generally considered to be a novel service by consumers. However, the home IoT service is not new (Yang et al., 2018). It has repeatedly appeared yet continuously failed to spread in the market, despite various name changes including home automation, network home, and connected home (Aldrich, 2003). Previous studies have not discussed the reasons behind these continuous failures; instead, they have primarily focused on new technologies, including frameworks, architectures, and security (Jacobsson et al., 2016; Jose and Malekian, 2015). Although some studies have been conducted to understand the spread of home IoT services from a user's perspective, the majority of them are centered on socially disadvantaged users, including the elderly, medical patients, and those disabled under special

E-mail address: hanslee992@gmail.com.

https://doi.org/10.1016/j.tele.2020.101377
Received 30 May 2019; Received in revised form 21 December 2019; Accepted 25 February 2020
Available online 29 February 2020

circumstances (Portet et al., 2013; Rahimpour et al., 2008). These studies are limited in their understanding of general users' acceptance and the potential to popularize these services.

Home IoT has presented unexpected new challenges and risks (Kowatsch and Maass, 2012). A representative negative aspect of home IoT is the possibility of privacy infringement. One example is the Internet Protocol (IP) camera, a home IoT device that has rapidly spread across the world. While over 50,000 IP cameras have been sold via Amazon.com, a large number of them were vulnerable to hacking (Laughlin, 2019). In several countries such as Korea and China, hackers have exploited the vulnerability of IP cameras to spy on users. While traditional hacking was simply an informational privacy breach, the case of the IP camera shows that privacy breaches in the IoT environment can invade personal spaces and even physical privacy. Several studies have also indicated privacy challenges as one of the factors hindering the acceptance and spread of home IoT services (Lin and Bergmann, 2016; Weinberg et al., 2015; Zeng et al., 2017). According to Ciesielska and Li (2011), in the past, the failure of home IoT was attributed to a lack of understanding of the user's requirements, device and installation costs, system integration difficulties, etc., along with privacy issues. Kowatsch and Maass (2012) maintained that privacy risks and concerns, as well as trust in the institutions providing IoT services, influenced the acceptance and spread of IoT services. Arabo et al. (2012) demonstrated that privacy breaches could occur as a result of technical problems in home IoT, which could be a hindrance to the spread of smart home services.

Although privacy challenges critically impact the acceptance of home IoT services, sufficient studies have not been conducted on the detailed factors that influence user privacy concerns in a home IoT environment. Several studies have emphasized perceived vulnerability as an antecedent affecting privacy concerns (e.g., Bandyopadhyay, 2012; Salleh et al., 2013). Vulnerability is an exceedingly comprehensive concept, including information system assets that may pose security risks or weaknesses in the design, implementation, or operation of infrastructures (Cox, 2008). However, previous studies have discussed the relationship between vulnerability and privacy concerns by simplifying the concept of vulnerability in a one-dimensional manner. As a result, the understanding of vulnerability was restricted to its relevance to information systems alone. Additionally, the concept of vulnerability was not explicitly distinguished from perceived risks. Therefore, this study extends vulnerability theory to examine the effects of users' vulnerability on privacy concerns and resistance to home IoT services.

2. Related literature

2.1. Home IoT services

In recent times, home IoT has received attention as a representative IoT service as IoT has been actively applied to households. For the past 40 years, home IoT has been ambiguously described as a home automation system or an ubiquitous agent. It is more precisely defined as follows: 1) a residence that includes systems to improve the quality of life of residents through monitoring information such as a resident's health status (Demiris and Hensel, 2008), 2) a residence equipped with computing and information technology that anticipates and responds to the requirements of the residents (Aldrich, 2003), 3) a residence installed with sensors that are connected via networks to detect people or objects and to collect data (Balta-Ozkan et al., 2014b), and 4) a residence equipped with systems to promote independence and maintain the health status of the residents through monitoring (Chan et al., 2009). Thus, home IoT is a residence in which information communication technology is integrated with a residential environment to enhance the comfort of residents. The home IoT system improves the convenience and efficiency of general household tasks by centrally controlling various home electronic appliances through smartphones and tablets (Luor et al., 2015).

Previous studies on home IoT have been conducted primarily from the suppliers' perspective; they have focused on frameworks and network architecture or been developed from a security perspective. However, difficulties in spreading home IoT services initiated discussions aimed at understanding the causes of its failures to spread. Ciesielska and Li (2011) suggested that the primary causes of failures of the home IoT service were user perception, a lack of understanding of user requirements, data security and privacy challenges, a lack of effective marketing messages, lack of installation support, insufficient maintenance services and skills, devices and installation costs, old housing challenges, pessimistic views on supply markets, a lack of common standards, and difficulties in system integration. Balta-Ozkan et al. (2014b) also argued that additional difficulties include housing structure, security and safety issues, energy efficiency problems, and cost management challenges. In this manner, previous research has continuously shown that various challenges, which have been difficult to overcome, exist in the process of home IoT diffusion. However, these studies are limited in their understanding of home IoT services' ability to spread to the general public because of their overarching focus on technical aspects or specific users.

Currently, privacy issues regarding home IoT are actively being discussed. Kowatsch and Maass (2012) proved that the acceptance of home IoT services is affected by various factors ranging from privacy risks and personal interests to legislation, information security, and transparency of information use. Ziegeldorf et al. (2014) discussed various hazards to privacy that can occur in home IoT environments. The home IoT service can connect all the devices and data in the home and expose this information to the outside world, which can increase the threat of personal privacy violations. As this could involve sensitive personal information, such as medical or financial information, it may occasionally cause unexpected high-risk situations. For example, Internet Protocol (IP) camera hacking can expose life in the home, which can be a physical privacy threat beyond a simple information privacy infringement. Similarly, most Home IoT devices have security vulnerabilities, which can lead to personal information leakage and various types of privacy breaches. Traditional privacy breaches are primarily sensitive information leaks, and the damage caused is not necessarily catastrophic. However, as shown in Table 1, home IoT is a more dangerous environment, allowing a hacker to observe private spaces and physically control the devices in the home. However, in previous research, informational privacy infringement was primarily discussed. This has limited the extent of the theoretical discussion regarding privacy issues affecting the acceptance of home IoT services.

Table 1
Privacy threats of home IoT environment.

Devices	Threats	References
Smart TV	- Eavesdropping on users' daily conversations - Tracking users' watching habits and preferences	(Shane et al., 2017)
Smart Speaker	- Unauthorized data collection - Distributing sensitive information to third parties	(Hart, 2018)
Smart Plug	- Insecure communication protocols, lack of device authentication, and a weak password policy - Threat to patient's life when implementing medical devices using smart plugs	(Ling et al., 2017)
IP Camera	- Monitoring of all private information within the field of view of the device - Unauthorized distribution of recorded video through IP camera	(Vlajic and Zhou, 2018)
Smart Phone	- Tracking personal day-to-day information such as user location, time, and temperature - Unauthorized distribution of photos and videos stored on a user's device or cloud storage service	(Hatamian et al., 2019)
Smart Car	- Collection of driving time, distance, and location information - Collection of residence, work, and traffic information	(Weinberg et al., 2015)
Other Devices	- Monitoring of personal life and activity patterns - Remote control against the user's intention (lighting, door lock, gas valve, temperature control device, etc.)	(Park, 2019)

2.2. User resistance theory

According to Ram (1987), individuals possess a desire to maintain a psychological equilibrium. When facing changes, their psychological equilibrium is unbalanced, and they tend to resist changes rather than to accept them and re-adjust to them. Such resistance is triggered when consumers perceive an innovative change; essentially, user resistance is a natural reaction when consumers are threatened by changes.

New technologies affect user resistance by generating functional barriers (e.g., use, value, and risk factors) and psychological barriers (e.g., negative images and traditional cohesion) (Ram and Sheth, 1989). Resistance to technology innovation causes conflicts with existing beliefs in the acceptance of new technology (Kim and Kankanhalli, 2009). Resistance appears in the form of rejection, postponement, and opposition (Szmigin and Foxall, 1998). Such resistant behaviors arise because of the potential risks perceived in innovation. Sheth and Stellner (1979) analyzed consumers' resistance to innovation using two psychological structures: habits of practice and recognition of risks associated with innovation. As the risk increases, the perceived benefits to the user decrease, which increases resistance to innovation (Finucane et al., 2000; Sheth and Stellner, 1979).

User resistance is an important aspect of the new technology adoption process. At the core of resistance theory, a new technology must endure the process of resistance before it is adopted by the user (Kim et al., 2016). From this perspective, user resistance theory provides a basis to understand home IoT's failure to spread; it was essentially caused by an insufficient understanding of consumer needs, privacy and data protection issues, and high costs (Ciesielska and Li, 2011). Among the causes, privacy issues critically impacted home IoT acceptance (Accenture, 2014). Because the privacy risk was bigger than the users' expected benefit, this privacy challenge has had a negative impact on the acceptance and diffusion of home IoT. User resistance behavior due to privacy challenges occurs in various forms; the behavior may appear in a passive form, in which inaccurate information is disseminated and use is avoided, or it may appear in an aggressive form in which complaints are displayed or problems are announced (Son and Kim, 2008). Thus, understanding the level of user resistance due to privacy challenges is integral to home IoT companies' response to user resistance and the development of improved technologies.

2.3. Home IoT privacy concerns

The concept of privacy has evolved over time and been actively studied in various disciplines (Barth and De Jong, 2017; Lee et al., 2019). When 'privacy' was first conceptualized, scholars defined it as the free will of human body or action. Westin (1970) argued that privacy is the right to choose freely how much one can expose their body, attitude, and behavior to others in any environment. Gradually, the concept of privacy began to expand. Burgoon (1982) classified privacy into four types: physical, psychological, social, and informational. Physical privacy refers to the degree of physical accessibility to others, relating to personal space and area. Psychological privacy determines with whom and in what situations a person may share their thoughts or reveal their personal information. Social privacy involves an individual's abilities and autonomy in social contexts. Informational privacy is defined as the right to control one's personal information as well as when and how to share details regarding that information. As interest in personal information has increased, discussions surrounding informational privacy has become more active (Lee et al., 2015; Smith et al., 2011).

Informational privacy has been actively discussed in the field of information systems (IS) with regard to personal information infringement, outbreaks of which frequently occur in the information age (Chang et al., 2018). Online companies have violated individuals' privacy through their inappropriate personal information management practices, and the resulting informational privacy concerns cause various social side effects. IS research has focused on informational privacy concerns, which involve feelings or attitudes resulting from privacy violations. Informational privacy concerns refer to the "extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information" (Mohamed and Ahmad, 2012). Informational privacy concerns may negatively impact users' behavior, including the extent to which users accept new technologies

and internet services (Bélanger and Crossler, 2011; Tang and Lin, 2017). Such concerns, coupled with platforms that allow people to disclose distorted information, can deteriorate the order of online society (Choi and Sung, 2018; Youn and Shin, 2019). However, entry into the impending IoT era necessitates the evolution of the concept of privacy beyond that of the information age. Existing privacy research has discussed privacy solely in terms of information; however, in the IoT environment, discussions of privacy breach threats must extend beyond the simpler threats of the past. Currently, the concept of privacy is not evolving to accommodate relatively novel challenges specific to the IoT environment. The factors relating to privacy concerns today are also beyond the scope of conventional discussion, which limits the extension of privacy theory.

In a home IoT environment, physical privacy may also be significantly threatened, as information and communications technologies are integrated into everyday objects that reside very close to the body (Moreham, 2014). Physical privacy is violated by surveillance, recording of personal activities, and the distribution of such records to others (Joinson and Paine, 2007). Physical privacy also involves protection of the physical space itself from such threats as invasion, stalking, and spying on private property (Galluccio et al., 2011). In the past, direct physical infiltration was typically required for observation or surveillance. However, with the advancement of digital technology, surveillance is possible at an affordable cost without physical intrusion (DeVries, 2003). Home IoT devices can become the observers instead of physical individuals or intruders, and therefore, there is a high possibility that residents' physical privacy may be infringed by these devices. As home IoT is used in private spaces, personal and sensitive information can be collected and used. Therefore, home IoT users may have sincere privacy concerns for both their informational and physical privacy, as the risk of infringement of information and physical privacy may pose a serious threat to users. Accordingly, privacy challenges in the home IoT environment should be discussed from both informational and physical perspectives.

2.4. Perceived vulnerability in four perspectives

Home IoT services differ from existing IT services in several respects (Kowatsch and Maass, 2012). Home IoT services are closely related to users' lives, wherein all of their actions are stored as information or connected via the Internet, which can lead to various unexpected risks. For example, unauthorized access and misuse of personal information through home IoT hacking can cause infringement of informational privacy, physical damage, and financial crimes. Thus, although the home IoT environment affords increased connectivity, it does so at the potentially high cost of increased levels of risk. According to the risk theory by Cox, 2008, risk is calculated according to threats, vulnerabilities, and the resulting consequences. Generally, a threat refers to an external artificial attack, while a vulnerability refers to an inherent weakness of an object. Previous studies focused on vulnerability factors that affect privacy risks in a one-dimensional manner. However, this approach does not accommodate differing subjects of vulnerability and thus restricts academic discussion.

Khidzir et al. (2010) classified the vulnerability factors into thirty categories based on relevant literature. These categories can be further classified into four types: technology (system design flaws and weaknesses), provider (reliability and responsibility), law (insufficient enforcement of law), and user (ignorance and careless negligence) vulnerabilities. Table 2 shows an example of the four vulnerability factors in a home IoT environment.

The technology vulnerability refers to a weakness in the technology itself, originating from a lack of technological stability. Because home IoT devices basically use wireless networks that require low power, related communication technologies remain vulnerable in terms of security (Geneiatakis et al., 2017). Lightweight and low-power devices are required because home IoT services are used in private and confidential spaces. However, this feature makes it difficult to operate general security software. In addition, as home IoT technology is not yet very mature, there is a lack of discussion on possible frameworks for the integrated protection of various devices (Jacobsson et al., 2016).

Service providers should protect users' personal information according to their information management policies. However, providers simultaneously aim to utilize users' personal information to gain other benefits. Thus, the release of personal information to a provider can be a high-risk transaction because of their opportunistic behaviors (Malhotra et al., 2004). In addition, providers have to pay to actively keep users' personal information safe and protect their privacy, which contributes to them passively protecting

Table 2
Examples of four vulnerability factors.

Vulnerability	Examples	References
Technology	- Hacking and privacy invasion using security vulnerabilities of information communication technology (eg., Bluetooth, Wifi, Z-wave) - Weak security framework and solutions for the connected devices.	(Basen, 2019; Jacobsson et al., 2016)
Law	- Weak penalty or punishment avoidance due to insufficient laws - Lack of legal framework for home IoT equipment installation and technical standards	(Losavio et al., 2018; Weber, 2011)
Provider	- No user agreements or system updates to remove the vulnerability - Collection of users' personal information for other business or unauthorized use - Weak security measures and hardware parts owing to cost	(Jackson and Orebaugh, 2018; Liranzo and Hayajneh, 2017; Rutledge et al., 2016)
User	- Non-compliance with security policies (simple and unchanged passwords) - Poor use and management of home IoT devices due to age or inexperience	(de Boer et al., 2019; Portet et al., 2013; Zeng et al., 2017)

users' privacy. This is an inevitable risk that arises when personal information is handled by third parties. Thus, provider vulnerabilities result in the possibility of them avoiding the responsibility of managing users' personal information for their own benefit.

With the advent of the big data and IoT era, legal limitations are increasing as the concept of personal information becomes more complex (Ziegeldorf et al., 2014). Despite persistent consumer concern about data collection through information technology, the legal framework for privacy remains weak (Brookman, 2015). This problem is caused by the speed of legal changes not keeping pace with the progress of technology. Thus, it is not easy to sufficiently protect personal information and user privacy in a home IoT environment with existing personal information protection laws. When personal privacy is breached, the lack of regulation prevents appropriate penalties for the perpetrators. In some cases, postponing regulations to allow the development of new industries can play a role in creating legal weaknesses. Thus, legal vulnerability refers to the immature state of regulatory devices to protect the privacy of individuals.

User vulnerability refers to the weaknesses of home IoT users who possess a low level of competence or technical preparation related to home IoT services. Early home IoT services were developed primarily for use by the elderly or medical patients (Yang et al., 2017). In recent years, while the general public have become target users of home IoT service, women are found to be the main users, as most home IoT devices are related to housework (Yang et al., 2018). From a social engineering perspective, carelessness of users who do not manage passwords securely or ensure appropriate system updates are also a major source of user vulnerability (Kizza, 2009). Home IoT users need to know how to use their devices and manage them to keep the security of their systems and protect their privacy. However, users who are unfamiliar with IT devices become another vulnerability in the home IoT environment because it is difficult for them to take these precautions.

Previous studies have focused on the broad concept of privacy risk or have discussed privacy without clearly separating threats and vulnerabilities. As a result, the underlying and inherent issues of privacy concerns were limited. However, the vulnerability-based approach provides new perspectives for understanding users' privacy concerns. Because vulnerabilities are factors that can be controlled and improved, a more specific understanding of the cause of vulnerabilities can contribute to exploring measures to reduce privacy concerns. In the presentation of four vulnerabilities, an integrated framework is suggested to better understand the antecedents of home IoT privacy concerns.

3. Research model

This study examines the effects of the four subdivided types of vulnerabilities based on user resistance theories related to informational privacy concerns and resistance to home IoT services. According to a literature review and ensuing theoretical developments, this study presents a vulnerability-privacy concern-resistance (VPR) framework. This framework explains how a user's privacy concerns and vulnerability perception affect the resistance of new information technology services. Fig. 1 shows the research model of this study.

Because of a lack of security technology stabilization, technology vulnerabilities exist in home IoT services, making them an easy target for attacks regardless of time and location (Jose and Malekian, 2015). Using technological vulnerabilities, unauthorized people could gain unauthorized access to the system, potentially stealing personal information, violating privacy, or blackmailing users by obtaining control of the home IoT (Komninos et al., 2014). Leaked personal information may also be used for other crimes, such as intrusions, via identity theft or individual profiling. However, the detection and tracking of intrusions is difficult, as they are not recorded in system events (Jacobsson et al., 2016). The technology vulnerabilities in home IoT devices can cause privacy concerns by leading users to believe that sensitive information could be leaked.

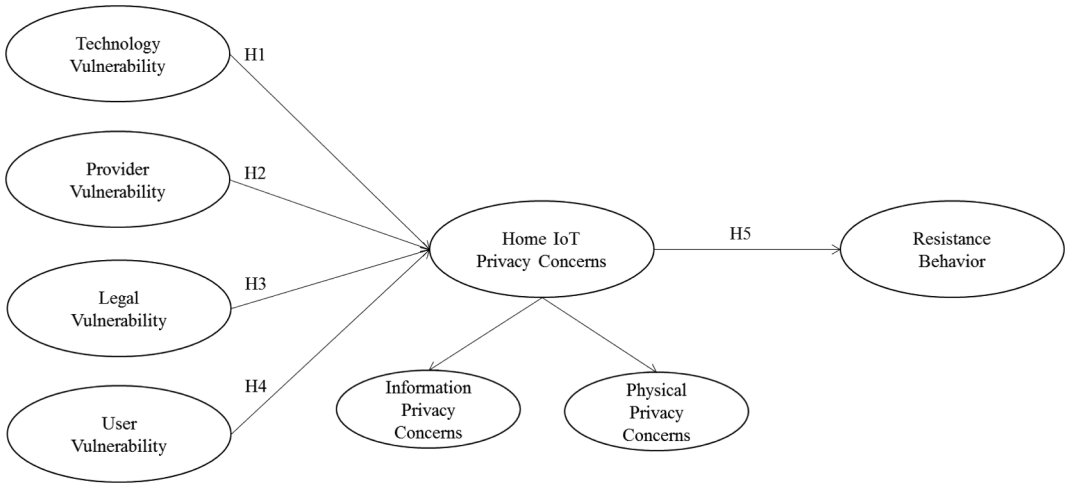

Fig. 1. Research Model.

Hypothesis 1: Technology vulnerability is positively associated with home IoT privacy concerns.

In a home IoT environment, it is difficult to completely protect privacy because it is difficult to limit the scope of users' personal information that requires protection (Ziegeldorf et al., 2014). Unclear legal standards could result in home IoT providers unintentionally violating laws or make it difficult for them to be penalized even when users' personal information is intentionally misused. Moreover, no international legislative guidelines exist regarding home IoT services; thus, privacy standards vary across countries, which can result in other vulnerabilities (Weber, 2015). Further, service providers may violate privacy laws when they believe that violating them is more beneficial than following them (Ziegeldorf et al., 2014). The existing compensation limit for damages following a privacy violation by a service provider may also increase legal vulnerabilities, which can in turn cause privacy concerns among home IoT users.

Hypothesis 2: Legal vulnerability is positively associated with home IoT privacy concerns.

Home IoT service providers are required to protect the sensitive information of home IoT users while simultaneously using the information to develop another revenue stream. This duality is an inherent vulnerability that corporations often cannot afford, thus encouraging various efforts to prevent related risks. Nonetheless, users sustain concerns regarding privacy breaches by service providers, such as the accumulation of sensitive personal data (Balta-Ozkan et al., 2014a), the non-purpose use of collected information (Tang et al., 2008), unauthorized access to data, and the possibility of misuse by corporate employees (Balta-Ozkan et al., 2014b). The near absence of publicity and marketing strategies to mitigate privacy concerns for users further increases privacy concerns (Ciesielska and Li, 2011).

Hypothesis 3: Provider vulnerability is positively associated with home IoT privacy concerns.

The technical stability of a home IoT service and the reliability of its devices are essential factors for certain user groups, such as elderly people and medical patients (Portet et al., 2013). Such groups are concerned that sensors or security devices may malfunction, or that a system failure may cause these devices to malfunction in an emergency situation. These concerns arise from user vulnerabilities such as physical constraints, a lack of understanding of the technology, and a lack of self-efficacy (de Boer et al., 2019). For example, elderly people have expressed concerns regarding situations in which sensors and security systems malfunction and home IoT appliances stop working, and have demonstrated excessive distrust and fear of computer systems (Czaja et al., 2006). Because of a lack of relevant skills, they are afraid of failing to be able to manage a task and are concerned about the increased risk perceived in being considerably dependent on technology (Balta-Ozkan et al., 2014a). Such user vulnerabilities may also increase concerns regarding potential privacy violations in a purportedly secure situation.

Hypothesis 4: User vulnerability is positively associated with home IoT privacy concerns.

Users resist innovation when risks are perceived with regard to the proposed changes (Bhattacherjee and Hikmet, 2007). Privacy concerns are one of the risk factors that result in resistance to innovation. Among the various risk factors involved in accepting new services, privacy risk is the most important factor (Featherman and Pavlou, 2003). Previous studies have confirmed that perceived privacy risk has negatively affected the acceptance of IoT services (Kowatsch and Maass, 2012) and consumer location-based services (Xu and Teo, 2004).

Hypothesis 5: Home IoT privacy concerns are positively associated with user resistance of home IoT.

4. Research methodology

Measurement items were developed based on previous literature. The items for research constructs are shown in Table 3. All items were measured using a seven-point Likert scale anchored on 'strongly disagree' and 'strongly agree.' Survey questionnaires including demographic questions were distributed via mobile survey companies in October 2016. Survey respondents were given a reward of approximately $1, and 300 responses were collected. Among the respondents, 35 respondents who were not familiar with home IoT were excluded from the analysis. The characteristics of the 265 respondents used in the analysis are shown in Table 4. The partial least squares structural equation modeling (PLS-SEM) technique was applied to verify the research hypotheses after testing the convergent and discriminant validity of all constructs. Smart PLS 3.0 and SPSS 20 were used as analysis tools.

5. Results

The PLS-SEM method was applied to test the outer and inner aspects of the proposed model. For internal consistency, Cronbach's alpha and composite reliability (CR) were tested. Cronbach's alpha and average variance extracted (AVE) results guarantee convergent validity. As seen in Table 5, Cronbach's alpha, rho_A, and CR exceeded the recommended cut-off value of 0.7 (Henseler et al., 2016). Convergent validity is defined as the degree to which measurement items are related to the construct. All factor loadings exceeded 0.7, and the AVE result for each construct exceeded 0.50, assuring the convergent validity of the constructs (Hair et al., 1998). Discriminant validity is demonstrated by confirmation that the square root of the AVE result for each construct is higher than

Table 3
Measurement items.

Construct	Item	Reference
Technology Vulnerability	Devices for home IoT services would be vulnerable to external invasion. Transmission information may be leaked when using home IoT services. My personal information would not be technically secure when using home IoT services.	(Banks et al., 2010; Lee, 2009)
Provider Vulnerability	Home IoT service providers are not doing their duty to protect my personal information. Home IoT service providers do not manage my personal information securely. Home IoT service providers have not established appropriate privacy policies.	(Dinev et al., 2006)
Legal Vulnerability	There are problems in the privacy laws of my country to use home IoT services safely. Even if privacy is violated while using home IoT services, our legal system cannot protect me. Even if home IoT service provider infringes on privacy, they do not receive sufficient legal sanctions.	(Dinev et al., 2013)
User Vulnerability	When using home IoT services, I may miss the necessary privacy safeguards. When using home IoT services, my personal information may be leaked because of my carelessness. I am unfamiliar with home IoT services, so I have no confidence to keep my privacy safe.	(Stanton et al., 2005)
Information Privacy Concerns	I am concerned about using home IoT services because my personal information could be misused. I am concerned about providing personal information home IoT services because of what others might do with it. I am concerned about providing personal information home IoT services because it could be used in a way I did not foresee.	(Xu et al., 2011)
Physical Privacy Concerns	When using home IoT services, I am concerned that someone may peep my private life. I am concerned that someone may break into my house by utilizing home IoT services. I am concerned that home IoT devices would be misused by others regardless of my will.	(Moreham, 2014)
Resistance Behavior	I think I will not use home IoT services. I will use more secure service than home IoT services. I will not recommend home IoT services to others.	(Zhang et al., 2016)

Table 4
Respondent characteristics.

Characteristic		Frequency (N = 265)	Ratio
Gender	Male	134	50.6%
	Female	131	49.4%
Age	20~	63	23.8%
	30~	68	25.6%
	40~	67	25.3%
	50~	67	25.3%
Home IoT Experience	Yes	175	66%
	No	90	34%
Residence Type	Apartment	172	65%
	House	93	35%

Table 5
Internal consistency and validity of constructs.

Construct	Mean (S.D.)	α	rho_A	C.R.	AVE	1	2	3	4	5	6
Technology Vulnerability	4.61(1.30)	0.79	0.79	0.88	0.71	**0.84**					
Provider Vulnerability	4.39(1.35)	0.86	0.86	0.91	0.78	0.54	**0.88**				
Legal Vulnerability	5.08(1.39)	0.84	0.84	0.90	0.76	0.51	0.62	**0.87**			
User Vulnerability	5.04(1.28)	0.74	0.74	0.85	0.65	0.53	0.60	0.68	**0.81**		
Home IoT Privacy Concerns	5.23(1.30)	0.92	0.92	0.94	0.72	0.54	0.46	0.52	0.59	**0.85**	
Resistance Behavior	4.32(1.28)	0.87	0.88	0.92	0.80	0.42	0.35	0.28	0.31	0.49	**0.89**

the corresponding inter-construct correlations (Fornell and Larcker, 1981). Another method to confirm the discriminant validity is the heterotrait-monotrait ratio (HTMT), wherein the HTMT cannot exceed 0.85 (Henseler et al., 2016). Table 5 shows that discriminant validity is confirmed.

As IoT privacy concerns are a second-order construct, the first-order factors (informational and physical privacy concerns) were also tested. No issues were found related to internal consistency and validity (Table 6). To check for common method bias (CMB), Harman's single-factor analysis was conducted, returning no issues with the test result. Current PLS-SEM studies request a different method in checking CMB. Kock and Lynn (2012) introduced the full collinearity test, wherein the variance inflation factor (VIF) from the full collinearity test should be less than 3.3. The highest VIF value of the research model is 2.181, confirming that CMB is not an

Table 6
Internal consistency and validity of first order constructs.

Construct	Mean(S.D.)	α	rho_A	C.R.	AVE
Informational Privacy Concerns	5.37(1.28)	0.89	0.89	0.93	0.82
Physical Privacy Concerns	5.18(1.30)	0.86	0.86	0.92	0.78

issue in this study.

Hypothesis testing results are presented in Fig. 2. A bootstrapping resampling (N = 1000) method was employed to calculate the corresponding t-values for each hypothesis. As summarized in Fig. 2, out of the five hypotheses, four were supported. Technology vulnerability, legal vulnerability, and user vulnerability were significant factors associated with home IoT privacy concerns, supporting H1, H3, and H4, and explaining 43.1% of the variance. (H1: $\beta = 0.278$, t-value = 3.497, $p < 0.001$; H3: $\beta = 0.165$, t-value = 1.665, $p < 0.05$; H4: $\beta = 0.348$, t-value = 4.129, $p < 0.001$; $R^2 = 0.431$). However, because the path from provider vulnerability to IoT privacy concerns was insignificant, H2 was rejected. The relationship between IoT privacy concerns and resistance behavior was significant (H5: $\beta = 0.486$, t-value = 10.08, $p < 0.001$; $R^2 = 0.236$).

In order to eliminate the influence of other factors on the dependent variables in the research model, the analysis was conducted by adding control variables (gender, age, and experience). None of the control variables had a significant effect on the resistance behavior. The path coefficients of the control variables were −0.045, −0.015, and 0.076 respectively. The goodness of fit (GoF) proposed by Tenenhaus et al. (2005) was checked for the overall fitness of the research model. The GoF value of this study is 0.50, which exceeds the cut-off value for large effects.

Comparative analyses were also conducted based on gender, home IoT experience, and residence types (Table 7). The results provide several insights. In the case of male users, the impact of legal vulnerability on home IoT privacy concerns was relatively strong. However, user vulnerability was the only significant antecedent of home IoT privacy concerns for female users. People with home IoT experience were sensitive to technical vulnerabilities, while those without experience had significantly different privacy concerns, mainly regarding the vulnerabilities of service providers. In terms of the effects of technical vulnerabilities, a significant difference was observed based on housing types.

6. Discussion

6.1. Findings

The empirical results of this study provide several research implications. First, the influence of users' privacy concerns on resistance was statistically confirmed in the home IoT environment. Multiple researchers have emphasized the importance of privacy protection in the home IoT environment (Arabo et al., 2012; Kowatsch and Maass, 2012; Lin and Bergmann, 2016); however, there are few empirical studies on the effects of privacy concerns on resistance behavior. Yang et al. (2017) showed that privacy risk has a negative impact on the acceptance of home IoT services, but this study was limited in that it considered only the informational privacy viewpoint and applied the same concept to both privacy and security. However, the results of the present study more precisely outline the effects of privacy concerns, from an integrated perspective, on home IoT resistance.

Second, current and potential users are realistically concerned about physical privacy invasion in the home IoT environment. According to the descriptive statistics (Table 6), the level of perceived physical privacy concerns is similar to informational privacy

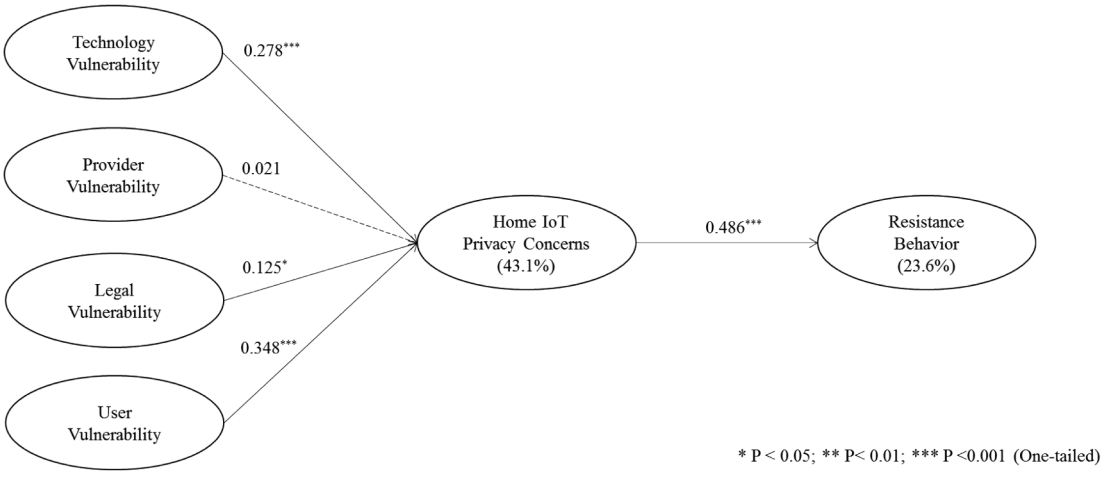

Fig. 2. PLS-SEM Results.

Table 7
Comparative analysis.

	Gender		Experience		Residence Type	
	Male (n = 134)	Female (n = 131)	Yes (n = 175)	No (n = 90)	Apartment (n = 172)	House (n = 93)
H1	0.29***	0.20*	0.36***	0.07	0.34***	0.13
H2	0.04	−0.02	−0.06	0.24*	0.04	−0.05
H3	0.27**	0.03	0.12	0.16	0.13	0.18
H4	0.27***	0.47***	0.30***	0.42***	0.37***	0.32**
H5	0.49***	0.48***	0.53***	0.38***	0.51***	0.44***

concerns. Accordingly, individuals are aware that the risks of the home IoT environment involve not only personal information leakage, but may also affect the body. Because home IoT is a type of cyber physical system (CPS), the importance of physical security has been emphasized (Ali and Awad, 2018; Geneiatakis et al., 2017). Physical security challenges can eventually lead to physical privacy breaches. There is growing concern around physical privacy because recent information leakage incidents have surpassed personal information usurpation and involved fatalities.

Third, user vulnerability is an integral antecedent affecting home IoT privacy concerns. Kim et al. (2017) argued that in home IoT services, the challenges in user operation must be addressed. Recent hacking incidents (e.g., IP camera hacking) have shown that users may experience severe privacy breaches if their device knowledge is insufficient. User vulnerability may also affect privacy concerns when the damage caused by it in a home IoT environment leads to physical damage beyond that of the existing cyber environment.

Fourth, the impact of sub-factors of vulnerability in home IoT privacy concerns varies based on user characteristics. In particular, the varying effects of perceived legal and user vulnerabilities according to varying genders suggest multiple implications. The results show that male users perceive legal vulnerabilities to be a more significant factor in the protection of their privacy. Males tends to be more aggressive, more critical, and less trusting of the government than women (Muller and Jukam, 1983). Similarly, the male user is less likely to believe that government-created privacy laws will protect their privacy. The difference in user vulnerability's impact between male and female users may be explained by technological anxiety and familiarity of the female users. According to previous studies, females have a higher level of anxiety and feel less comfort surrounding new technologies than males (Huffman et al., 2013). Because of this tendency, females are aware of their own vulnerability and feel concerns regarding privacy violation.

Lastly, it was found that the home IoT environment is perceived to function differently according to vulnerabilities and privacy concerns. For individuals who have experience with home IoT, the difference in function might be observed as a result of the perception that the current home IoT technology is not yet stable. In the case of individuals inexperienced with home IoT, the perception that privacy violations may occur results from fears regarding service providers rather than technology instabilities. Accordingly, service providers and technology developers should identify methods to reduce this gap in user perceptions of home IoT insufficiencies.

6.2. Contributions

The first theoretical contribution of this study is the presentation of the extended privacy concept for the home IoT environment to include physical privacy. Previous studies have limited discussions of various privacy infringements in the current information environment to discussions of primarily informational privacy infringements. By constructing sub-factors of privacy concerns, privacy concerns in the home IoT environment can be measured more accurately.

Secondly, this study has specified and segmented the concept of vulnerability based on traditional risk theory. Previous studies include mixed risks, threats, and vulnerabilities or have defined them in a manner that contradicts traditional risk theory. This has obscured conceptual differences by measuring vulnerability as a single dimension. Thus, the present work contributes a clearer approach to risk theory and helps to reduce these uncertainties.

Third, this study develops a VPR framework to explain user resistance behavior toward new information technology services. Previous studies attempted to explain resistance behaviors based on broad and ambiguous risk factors, which limits clear identifications of the cause of the risk. As most previous works concentrate on an informational perspective, there has been a lack of fundamental research surrounding privacy issues with regard to user behavior. However, this study presents a new theoretical framework to overcome these limitations.

Lastly, this study confirmed that users' personal and environmental characteristics play a significant role in the proliferation of home IoT. As a cyber-physical system, home IoT is a service that controls physical devices in a virtual environment. The object of control is the space around human activity and the devices in it. In addition, the adoption and resistance of home IoT can also be affected by factors related to the user or environment, as it is not yet a common service. The results of this study show that the consideration of personal and environmental characteristics in acceptance or resistance of home IoT services need to be discussed for the generalization of future research.

This study also provides several practical applications. First, the fundamental obstacles to home IoT diffusion are elucidated. According to the results, both informational and physical privacy concerns affect consumer's acceptance of the home IoT service. In the home IoT environment, privacy breaches are not only a matter of information leakage, but also one of personal life. If an

unauthorized, external, anonymous entity gains control of a home IoT, incidents that threaten a resident's physical safety may occur. Therefore, home IoT providers should provide trustworthy solutions to protect users' physical safety.

As a second practical contribution, it is shown that companies should better understand the characteristics and behavior of common users. In the rapidly changing information technology environment, users themselves are aware of vulnerabilities resulting from their failure to adjust to the rapid pace of technological change. This suggests that companies should be more concerned with improving users' familiarity with new technologies.

Third, the different effects of vulnerabilities on privacy concerns according to users' characteristics show the strategic approaches that should be taken to popularize home IoT services. By providing differentiated home IoT services that consider a user's gender, experience, and residential environment, negative factors recognized by users in advance can be minimized. These practical findings could ultimately help lower consumers' resistance to home IoT, thereby contributing to its growth.

Finally, according to the results of this study, users may perceive the government's regulations and laws regarding informational privacy to be limited, which has a negative impact on the acceptance of home IoT services. The positive effect of legal vulnerabilities on home IoT privacy concerns indicate that users lack confidence in related information protection laws, the strongest safeguards to protect their privacy. This shows that policymakers or lawmakers must improve traditional regulations and laws or create a reliable foundation for protecting users' privacy.

6.3. Limitations and further study

Although this study has extended the theory of vulnerability, it is limited in that it excludes discussions and analyses of external threats. In the future, research that integrates both the internal factor of vulnerability and the external factor of threats could more meaningfully ascertain the resistance attitudes of users. Here, while the privacy concern model incorporating the concept of physical privacy is presented based on the existing privacy theory, discussions that consider social and psychological privacy are still required. Because the current challenge of privacy surrounds the violation of various types of information, a research model that comprehensively considers privacy sub-dimensions would contribute to a more thorough understanding of complex privacy problems.

6.4. Conclusion

In this study, the effects of both informational and physical privacy concerns on user resistance to home IoT are statistically examined. Among the four established categories of vulnerabilities relating to privacy concerns, user vulnerability was determined as the most significant antecedent to home IoT resistance. Among vulnerability subfactors, differences in legal and user vulnerabilities varied with user characteristics, while prior experience with home IoT most significantly impacted users' perception of the home IoT environment's functionality. These findings can inform the methods with which companies and service providers present the home IoT environment to consumers, ultimately contributing to the potential further spread of home IoT. While this work primarily considers the environment's internal dangers of various vulnerabilities, further work should incorporate the external dangers of threats to the system. This would develop a more realistic model to intricately examine the tendency of home IoT services to spread despite various limitations.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Accenture, 2014. The Internet of Things: The Future of Consumer Adoption, from https://www.accenture.com/t20150624T211456_w_/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf.
Aldrich, F.K., 2003. Smart homes: past, present and future. In: Inside the Smart Home (pp. 17-39): Springer.
Ali, B., Awad, A., 2018. Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors 18 (3), 817.
Arabo, A., Brown, I., El-Moussa, F., 2012. Privacy in the age of mobility and smart devices in smart homes. Paper presented at the 2012 International Conference on Privacy, Security, Risk and Trust (PASSAT).
Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: a survey. Comput. Netw. 54 (15), 2787–2805.
Bélanger, F., Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. Mis. Quart. 35 (4), 1017–1042.
Balta-Ozkan, N., Amerighi, O., Boteler, B., 2014a. A comparison of consumer perceptions towards smart homes in the UK, Germany and Italy: reflections for policy and future research. Technol. Anal. Strateg. 26 (10), 1176–1195.
Balta-Ozkan, N., Boteler, B., Amerighi, O., 2014b. European smart home market development: Public views on technical and economic aspects across the United Kingdom, Germany and Italy. Energ. Res. Soc. Sci. 3, 65–77.
Balta-Ozkan, N., Davidson, R., Bicket, M., Whitmarsh, L., 2013. Social barriers to the adoption of smart homes. Energ. Policy 63, 363–374.
Bandyopadhyay, S., 2012. Consumers' online privacy concerns: causes and effects. Inn. Market. 8 (3), 32–39.
Banks, M.S., Onita, C.G., Meservy, T.O., 2010. Risky Behavior in Online Social Media: Protection Motivation and Social Influence. Paper presented at the AMCIS.
Barth, S., De Jong, M.D., 2017. The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. Telematics Inform. 34 (7), 1038–1058.
Basen, J., 2019. Goodbye Smart Hubs, Hello Hackers, from https://restechtoday.com/rip-smart-hubs/.
Bhattacherjee, A., Hikmet, N., 2007. Physicians' resistance toward healthcare information technology: a theoretical model and empirical test. Eur. J. Inform. Syst. 16 (6), 725–737.
Brookman, J., 2015. Protecting privacy in an era of weakening regulation. Harv. L. Pol'y Rev. 9, 355–374.
Burgoon, J.K., 1982. Privacy and communication. Ann. Int. Com. Ass. 6 (1), 206–249.

Chan, M., Campo, E., Estève, D., Fourniols, J.-Y., 2009. Smart homes—current features and future perspectives. Maturitas 64 (2), 90–97.
Chang, Y., Wong, S.F., Libaque-Saenz, C.F., Lee, H., 2018. The role of privacy policy on consumers' perceived privacy. The role of privacy policy on consumers' perceived privacy. 35 (3), 445–459.
Choi, T.R., Sung, Y., 2018. Instagram versus Snapchat: self-expression and privacy concern on social media. Telematics Inform. 35 (8), 2289–2298.
Ciesielska, M., Li, F., 2011. The connected home: from market barriers to business model solutions. Paper presented at the Conference on e-Business, e-Services and e-Society.
Cox Jr, L.A.T., 2008. Some limitations of "Risk= Threat× Vulnerability× Consequence" for risk analysis of terrorist attacks. Risk Anal. 28 (6), 1749–1761.
Czaja, S.J., Charness, N., Fisk, A.D., Hertzog, C., Nair, S.N., Rogers, W.A., et al., 2006. Factors predicting the use of technology: findings from the center for research and education on aging and technology enhancement (CREATE). Psychol. Aging. 21 (2), 333–352.
de Boer, P.S., van Deursen, A.J., van Rompay, T.J., 2019. Accepting the Internet-of-Things in our homes: the role of user skills. Telematics Inform.. 36, 147–156.
Demiris, G., Hensel, B.K., 2008. Technologies for an aging society: a systematic review of "smart home" applications. Yearb. Med. Inform. 17 (1), 33–40.
DeVries, W.T., 2003. Protecting privacy in the digital age: Berkeley Tech. LJ.
Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., Colautti, C., 2006. Privacy calculus model in e-commerce–a study of Italy and the United States. Eur. J. Inform. Syst. 15 (4), 389–402.
Dinev, T., Xu, H., Smith, J.H., Hart, P., 2013. Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. Eur. J. Inform. Syst. 22 (3), 295–316.
Featherman, M.S., Pavlou, P.A., 2003. Predicting e-services adoption: a perceived risk facets perspective. Int. J. Hum.-Comput. St. 59 (4), 451–474.
Finucane, M.L., Alhakami, A., Slovic, P., Johnson, S.M., 2000. The affect heuristic in judgments of risks and benefits. J. Behav. Decis. Making 13 (1), 1–17.
Fornell, C., Larcker, D.F., 1981. Structural equation models with unobservable variables and measurement error: algebra and statistics: SAGE Publications Sage CA: Los Angeles, CA.
Galluccio, L., Leonardi, A., Morabito, G., Palazzo, S., 2011. Context privacy in the internet of things. In: Trustworthy Internet (pp. 61-73): Springer.
Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., Baldini, G., 2017. Security and privacy issues for an IoT based smart home. Paper presented at the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).
Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Tatham, R. L., 1998. Multivariate data analysis (Vol. 5): Prentice hall Upper Saddle River, NJ.
Hart, L., 2018. Smart speakers raise privacy and security concerns. Smart speakers raise privacy and security concerns. 225 (6), 70-70.
Hatamian, M., Momen, N., Fritsch, L., Rannenberg, K., 2019. A Multilateral Privacy Impact Analysis Method for Android Apps. Paper presented at the Annual Privacy Forum.
Henseler, J., Hubona, G., Ray, P.A., 2016. Using PLS path modeling in new technology research: updated guidelines. Ind. Manage. Data Syst. 116 (1), 2–20.
Huffman, A.H., Whetten, J., Huffman, W.H., 2013. Using technology in higher education: the influence of gender roles on technology self-efficacy. Comput. Hum. Behav. 29 (4), 1779–1786.
Jackson, C., Orebaugh, A., 2018. A study of security and privacy issues associated with the Amazon Echo. A study of security and privacy issues associated with the Amazon Echo. 1 (1), 91-100.
Jacobsson, A., Boldt, M., Carlsson, B., 2016. A risk analysis of a smart home automation system. Future Gener. Comp. Sy. 56, 719–733.
Joinson, A.N., Paine, C.B., 2007. Self-disclosure, privacy and the Internet. In Oxford handbook of Internet psychology (pp. 237-252).
Jose, A.C., Malekian, R., 2015. Smart home automation security. SmartCR. 5 (4), 269–285.
Khidzir, N.Z., Mohamed, A., Arshad, N.H., 2010. Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. Paper presented at the Information Retrieval & Knowledge Management,(CAMP), 2010 International Conference on.
Kim, H.-W., Kankanhalli, A., 2009. Investigating user resistance to information systems implementation: a status quo bias perspective. Mis Quart. 33 (3), 567–582.
Kim, J., Kim, S., Nam, C., 2016. User resistance to acceptance of In-Vehicle Infotainment (IVI) systems. Telecommun. Policy 40 (9), 919–930.
Kim, Y., Park, Y., Choi, J., 2017. A study on the adoption of IoT smart home service: using Value-based Adoption Model. Total Qual. Manag. Bus. 28 (9–10), 1149–1165.
Kizza, J.M., 2009. Guide to Computer Network Security. Springer.
Kock, N., Lynn, G., 2012. Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. J. Assoc. Inf. Syst. 13 (7).
Komninos, N., Philippou, E., Pitsillides, A., 2014. Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun. Surv. Tut. 16 (4), 1933–1954.
Kowatsch, T., Maass, W., 2012. Critical privacy factors of internet of things services: an empirical investigation with domain experts. In: Knowledge and Technologies in Innovative Information Systems. Springer, pp. 200–211.
Laughlin, A., 2019. The cheap security cameras inviting hackers into your home, from https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home/.
Lee, H., Lim, D., Kim, H., Zo, H., Ciganek, A.P., 2015. Compensation paradox: the influence of monetary rewards on user behaviour. Compensation paradox: the influence of monetary rewards on user behaviour. 34 (1), 45-56.
Lee, H., Wong, S.F., Oh, J., Chang, Y., 2019. Information privacy concerns and demographic characteristics: data from a Korean media panel survey. Gov. Inform. Q. 36 (2), 294–303.
Lee, M.-C., 2009. Factors influencing the adoption of internet banking: an integration of TAM and TPB with perceived risk and perceived benefit. Electron. Commer. R A. 8 (3), 130–141.
Lin, H., Bergmann, N., 2016. IoT privacy and security challenges for smart home environments. Inform. 7 (3), 44.
Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., Fu, X., 2017. Security vulnerabilities of internet of things: A case study of the smart plug system. 4 (6), 1899–1909.
Liranzo, J., Hayajneh, T., 2017. Security and privacy issues affecting cloud-based IP camera. Paper presented at the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON).
Losavio, M. M., Chow, K., Koltay, A., James, J., 2018. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. 1 (3), e23.
Luor, T.T., Lu, H.-P., Yu, H., Lu, Y., 2015. Exploring the critical quality attributes and models of smart homes. Maturitas 82 (4), 377–386.
Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. 15 (4), 336-355.
Mohamed, N., Ahmad, I.H., 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: evidence from Malaysia. Comput. Hum. Behav. 28 (6), 2366–2375.
Moreham, N., 2014. Beyond information: physical privacy in english law. Camb. Law J. 73 (2), 350–377.
Muller, E.N., Jukam, T.O., 1983. Discontent and aggressive political participation. Brit. J. Polit. Sci. 13 (2), 159–179.
Park, C., Kim, Y., Jeong, M., 2018. Influencing factors on risk perception of IoT-based home energy management services. Telematics Inform. 35 (8), 2355–2365.
Park, S.E., 2019. Technological Convergence: Regulatory, Digital Privacy, and Data Security Issues. Congressional Research Service.
Portet, F., Vacher, M., Golanski, C., Roux, C., Meillon, B., 2013. Design and evaluation of a smart home voice interface for the elderly: acceptability and objection aspects. Design and evaluation of a smart home voice interface for the elderly: acceptability and objection aspects. 17 (1), 127–144.
Rahimpour, M., Lovell, N.H., Celler, B.G., McCormick, J., 2008. Patients' perceptions of a home telecare system. Int. J. Med. Inform. 77 (7), 486–498.
Ram, S., 1987. A model of innovation resistance. Adv. Consum. Res. 14, 208–212.
Ram, S., Sheth, J.N., 1989. Consumer resistance to innovations: the marketing problem and its solutions. J. Consum. Mark. 6 (2), 5–14.
Rutledge, R.L., Massey, A.K., Antón, A.I., 2016. Privacy impacts of IoT devices: a SmartTV case study. Paper presented at the 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW).
Salleh, N., Hussein, R., Mohamed, N., Aditiawarman, U., 2013. An Empirical Study of the Factors Influencing Information Disclosure Behaviour in Social Networking Sites. Paper presented at the 2013 International Conference on Advanced Computer Science Applications and Technologies (ACSAT).

Shane, S., Rosenberg, M., Lehren, A.W., 2017. WikiLeaks releases trove of alleged CIA hacking documents. N.Y. Times.
Sheth, J. N., Stellner, W. H., 1979. Psychology of innovation resistance: The less developed concept (LDC) in diffusion research: College of Commerce and Business Administration, University of Illinois at Urbana-Champaign Urbana-Champaign, IL.
Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: an interdisciplinary review. Mis. Quart. 35 (4), 989–1016.
Son, J.-Y., Kim, S.S., 2008. Internet users' information privacy-protective responses: a taxonomy and a nomological model. Mis. Quart. 32 (3), 503–529.
Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J., 2005. Analysis of end user security behaviors. Comput. Secur. 24 (2), 124–133.
Szmigin, I., Foxall, G., 1998. Three forms of innovation resistance: the case of retail payment methods. Technovation 18 (6–7), 459–468.
Tang, J.-H., Lin, Y.-J., 2017. Websites, data types and information privacy concerns: a contingency model. Telematics Inform. 34 (7), 1274–1284.
Tang, Z., Hu, Y., Smith, M.D., 2008. Gaining trust through online privacy protection: self-regulation, mandatory standards, or caveat emptor. J. Manage. Inform. Syst. 24 (4), 153–173.
Tenenhaus, M., Vinzi, V.E., Chatelin, Y.-M., Lauro, C., 2005. PLS path modeling. Comput. Stat. Data An. 48 (1), 159–205.
Vlajic, N., Zhou, D., 2018. IoT as a land of opportunity for DDoS hackers. IoT as a land of opportunity for DDoS hackers. 51 (7), 26-34.
Weber, R.H., 2011. Accountability in the Internet of Things. Accountability in the Internet of Things. 27 (2), 133–138.
Weber, R.H., 2015. Internet of things: privacy issues revisited. Comput. Law Secur. Rev. 31 (5), 618–627.
Weinberg, B.D., Milne, G.R., Andonova, Y.G., Hajjat, F.M., 2015. Internet of Things: Convenience vs. privacy and secrecy. Internet of Things: Convenience vs. privacy and secrecy. 58 (6), 615-624.
Westin, A., 1970. Privacy and Freedom. Atheneum, New York.
Xu, H., Dinev, T., Smith, J., Hart, P., 2011. Information privacy concerns: linking individual perceptions with institutional privacy assurances. J. Assoc. Inf. Syst. 12 (12), 798–824.
Xu, H., Teo, H.-H., 2004. Alleviating consumers' privacy concerns in location-based services: a psychological control perspective. Paper presented at the ICIS 2004 proceedings.
Yang, H., Lee, H., Zo, H., 2017. User acceptance of smart home services: an extension of the theory of planned behavior. Ind. Manage. Data Syst. 117 (1), 68–89.
Yang, H., Lee, W., Lee, H., 2018. IoT smart home adoption: the importance of proper level automation. J. Sensors. Article ID 6464036.
Youn, S., Shin, W., 2019. Teens' responses to Facebook newsfeed advertising: the effects of cognitive appraisal and social influence on privacy concerns and coping strategies. Telematics Inform. 38, 30–45.
Zeng, E., Mare, S., Roesner, F., 2017. End user security and privacy concerns with smart homes. Paper presented at the Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017).
Zhang, S., Zhao, L., Lu, Y., Yang, J., 2016. Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social network services. Inform. Manage. 53 (7), 904–914.
Ziegeldorf, J.H., Morchon, O.G., Wehrle, K., 2014. Privacy in the Internet of Things: threats and challenges. Secur. Commun. Netw. 7 (12), 2728–2742.

Hwansoo Lee is an assistant professor in the Department of Convergence Security at Dankook University, South Korea. He received his PhD degree in Business & Technology Management from Korea Advanced Institute of Science and Technology (KAIST), South Korea. His research focuses on information security & privacy, electronic commerce, and enterprise information systems. His papers have appealed in journals such as *Government Information Quarterly, Information & Management, Information Systems and e-Business Management, Behaviour & Information Technology, Industrial Management and Data Systems, Journal of Global Information Management, and Telematics & Informatics*. He also received the Best Paper awards at various international and domestic conferences. Further, he has well-qualified experiences related to information systems as a developer and a system analyst. He is currently serving as an editorial review board member of Industrial Management and Data Systems.