Privacy fatigue in the internet of things(IoT) environment*

Junhyoung Oh, Ukjin Lee, and Kyungho Lee†
Korea University
Seoul, Republic of Korea
{ohjun02, ukjinlee, kevinlee}@korea.ac.kr

Abstract

The purpose of this study is to analyze the phenomenon of privacy fatigue in an Internet-of-Things environment. As the paradigm shifts from towards IoT, users' perception of personal information is also changing. Users' perception of personal information and people's actions to protect personal information have a great impact on security. Because the theory of protection motivation is a representative theory to explain the change of users' protection behavior against the threat, we conducted a structured in-depth interview based on the motivation theory. As a result of the interview, various results came out which were not found in previous studies such as that the level of security knowledge of IoT users, the usage environment and purpose of IoT devices affect privacy fatigue. These results will be of benefit to IoT device designers and privacy researchers and can be the basis for a variety of follow-up studies.

Keywords: Privacy Fatigue, Internet of Things, Smart Home, Human-Computer Interaction.

1 Introduction

Personal information of users that managed by companies is today often digitized and stored in information systems and the amount is increasing exponentially. Billions of people are connected via the Internet, and personal information is being moved and processed on various devices and systems. However, most people do not fully understand how their personal information is used and who can access it [11]. Consumers tend to simply not accept privacy policies when they use devices or services [14]. Recently, users have to agree on providing personal information, which is one of the main reasons for their overwhelming choice [16]. Users are also sensitive to responding to their personal information and to controlling their access to personal information [13]. However, they tend to adopt easy methods and choose basic options to easily use their personal information.

As the frequency of data outbreaks increases, the occurrence of data outbreaks has a substantial impact on the consumer's long-term choice [9]. People lose control of their personal information due to repeated leakage of personal information. Thinking that they can not control their personal information, they will no longer try to control their personal information [6]. For these reasons, privacy fatigue occurs. Privacy fatigue is a phenomenon that it becomes difficult to manage personal information, individual loses control, and it is meaningless due to repeated data leakage, so that it does not care about personal information at all.

Privacy fatigue is a hypothesis that there has been much debate about in academia, but there is little practical research. Recently, however, Choi et al. [1] conducted a survey of 324 participants, revealing that privacy fatigue exists and the importance of privacy fatigue is emerging. As the Internet of Things (IoT)

IT CoNvergence PRActice (INPRA), volume: 6, number: 4 (December 2018), pp. 21-34

*The first two authors, Ukjin Lee and Junhyoung Oh, contributed equally to this paper.

†Corresponding author: Anam-ro 145, Anam-dong 5 Seongbuk-gu, Seoul, 136-713, Republic of Korea, Tel: +82-10-5002-5099, E-mail: kevinlee@korea.ac.kr, Website: www.rimala.net

spreads, IoT devices are in the people's life. IoT devices collect and use much more personal information than general IT devices to provide customized services to users. The characteristics of such IoT devices are expected to have a different impact on consumers than existing IT devices. For example, in the IoT environment, sharing of personal information is frequent due to an increase in collaboration per service, and it is difficult to obtain the prior consent of the information subject due to the autonomous collection of IoT devices [4]. Therefore, users do not try to exercise their rights to personal information in the IoT environment carefully.

There is no research that analyzed privacy fatigue phenomenon in IoT environment. However, considering the increasing importance of the IoT market and the increasing importance of privacy fatigue, the study of privacy fatigue in the IoT environment has great significance. In this study, through qualitative research, we investigate the privacy fatigue phenomenon in the IoT environment collectively from the cause to the current application. To this end, we analyze each element of the Protection Motivation Model and investigate the effect on users' behavior.

2 Background and Related Work

2.1 Privacy Fatigue

Privacy Fatigue is a term that is still under discussion, and there are only a few studies about it. For this reason, it is difficult to make a clear definition, but it can be said that users feel tired of protecting their personal information for various reasons and give up their protection behavior.

Keith et al. [8] supported the privacy fatigue theory by examining the effect of the complexity of privacy control based on the theory of feature fatigue on the users' personal information leakage behavior. Choi et al. [1] suggested that emotional exhaustion and cynicism are the basis of privacy fatigue through experimental studies.

2.2 Protection Motivation Theory

The Protection Motivation Theory was developed by Rogers [12] to explain the health-related belief in the health domain and analyzes the behavior that is changed by the Fear Appeal based on Expectancy-value theory and Cognitive processing theory. People have a motivation to protect themselves from danger, which is shaped by psychological factors and changes behavior [7]. Protection Motivation Theory, which began in the field of health sciences, is increasingly being applied to research on privacy and personal information.

Woon et al. [17] analyzed the dangers of home wireless network users through the Protection Motivation Theory, and studied the effects on the implementation of network security functions and the results. Based on the Protection Motivation Theory, Crossler [3] found that self-efficacy and response efficacy have a positive impact on backups, and perceived security vulnerabilities and perceived security threats have a negative impact on backups. Marett et al. [10] has analyzed the fear of privacy in social networking websites and their changing behavior through the Protection Motivation Theory. Tsai et al. [15] used the Protection Motivation Theory to investigate the security threats they experience when using the Internet and to identify new motivators such as prior experiences, subjective norms, habit strength, perceived security support, and personal responsibility. Crossler et al. [2] used the Protection Motivation Theory to analyze the security practices of home computer users and suggest new ways to apply them by collecting new security practices. Hanus et al. [5] have discovered that perceived severity, response efficacy, self-efficacy, and response cost are key factors in exploring the impact of security awareness on desktop security behavior using Protection Motivation Theory.

Protection motives are generated from Threat Appraisal and Coping Appraisal. Threat Appraisal is an

individual assessment of a threatening event, consisting of Perceived Vulnerability and Perceived Severity. Perceived Vulnerability is an individual's assessment of the likelihood of a threat occurring. In this study, it refers to the degree to which information related to one's own perception is highly perceived through illegal access, secondary use, or improper collection on the IoT network. Perceived Severity is the severity of the threat. In this study, it refers to the severity of the negative consequence of privacy infringement in the IoT network is considered.
Coping Appraisal is composed of Self-Efficacy, Perceived Response Effectiveness, and Response Cost as the ability to prevent and cope with threats. Self-Efficacy is the individual's belief in the ability to cope with threats, and this study implies an individual's belief that he or she possesses the skills and abilities to perform a given task. Perceived Response Effectiveness is the efficiency of coping strategies. In this study, the subjective beliefs of individuals who believe that threats can be significantly reduced through protective actions to prevent privacy infringement on the IoT network. Response Cost is the cost of performing the protection action. In this study, the cost and psychological disturbance factors related to the personal information protection behavior on the IoT network are considered.

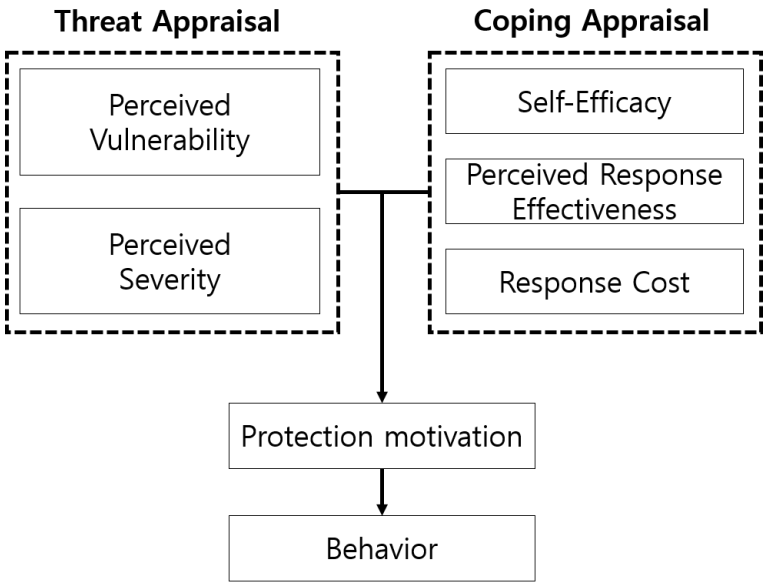


Figure 1: Protection Motivation Model

3 Methodology

This section describes the preliminary work for the interview, including the recruitment of participants and the pre-established interview protocol.

3.1 Preliminaries

The drafting of the interview protocol was made by referring to the qualitative research using the threat model for the security concern of users in the smart home [18]. However, privacy fatigue is a phenomenon that gives up privacy protection for various reasons such as loss of control and burn-out. Therefore, the protection motivation theory is more suitable than the threat model. Although we drafted the interview protocol, the actual interviews have various variables, so we changed the order of the interview protocols according to the situation or practiced adding new questions.

Participants were recruited through the university community site. Participants in the university community site were able to read the recruitment postings even if they were not university students. Information was gathered primarily on the type of IoT device used, the duration of use, and demographic information (age, major, and gender). IoT devices in the smart home and health care sectors are the most commonly used, so we recruited participants using devices in those domain. Based on the results, ten people were finally recruited.

3.2 Interview Procedure

All of the interviews were conducted offline, and all participants received a 5 dollar gift certificate for the interview. Recording was conducted for the purpose of scripting, and the collected personal information was used for research purposes only. These facts were previously notified to all participants and signed by the consent form which they prepared. After signing, interviews were conducted on average for 30 minutes per participant. The interview was conducted by two researchers. One researcher asked questions based on the interview protocol and encouraged participants to get answers. Other researchers recorded interview, wrote scripts, and asked additional questions that were not considered in the interview protocol.
First, we let the participants score on how they feel about the technology themselves, and then listen to the reason. The participants then painted a mental model of how they use personal information on their IoT devices and which flows through them. After hearing about the mental model, we asked various questions about the basic IoT device. If we make reference to personal information, privacy salience is generated and it can raise awareness of their security consciousness. So, we did not mention about personal information or things about security and privacy. When responding to the question, if the participant first responded to personal information, we encourage them to speak about privacy fatigue without direct questions. After obtaining all possible answers within the scope of not generating a privacy salience, we told them that the purpose of the experiment is to study the user's position on privacy infringement in the IoT environment. Then we asked about the factors of protection motivation theory, Perceived Vulnerability, Perceived Severity, Self-Efficacy, Perceived Response Effectiveness, and Response Cost, respectively. The questions about each element were used to give a variety of results by telling both before and after use experiences.

4 Results

4.1 Participants

General technology
The average for all participants' general skills was 5.7 out of 10, showing a moderate level of involvement in general skills. P1, P2, P3, P8 and P9 are included in the group with higher involvement of general technology than the average. They responded that they are familiar with technology because of their expertise in technology and relatively easy access to information. P4, P5, P6, P7, P10 are included in the group with lower involvement of general technology. They responded that they were not familiar with the technology because they did not know how to operate the device, had difficulty installing the application directly, or did not use the application functions skillfully.

Computer security
The average score self-reported by participants was 3.75 out of 10, showing relatively low involvement in computer security. The group with higher involvement in computer security than average include P1,

P2, P3, and P7. They responded that they are familiar with computer security because they have the expertise to evaluate the security level of the computer or practice the recommended security strategy.On the other hand, the group with lower involvement in computer security include P2, P4, P6, P8, P9, and P10. They responded that they are not familiar with computer security because they asked for help from their acquaintances if they have problems with computer security, or because they had been hacked in the unprotected state in the past.

IoT technology

The average score of all participants for IoT technology was 5.15 out of 10, showing a moderate level of involvement in IoT technology. Groups with higher involvement in IoT technology include P1, P2, and P3. They know the latest trends in IoT technology, have used IoT applications, and are more actively using IoT devices than people around them. On the other hand, the groups with lower involvement in IoT technology include P4, P5, P6, P7, P8, P9 and P10. Most of them responded that we do not know how IoT devices are operated and implemented.

Table 1: Summary of participants

ID	Gender	Age	IoT Device	Usage (month)	Primary User (/10)	Involvement(/10)			Privacy Concern (/10)	
						General Tech	Security	IoT Tech	IT	IoT
P1	M	28	LG Home Camera	12	2	9	7	7.5	6	6
P2	M	32	Aapple Watch	36	9	8	8	9	7	5
P3	F	20	Amazon Echo Dot	48	9	6	4	7	8	3
			Xiaomi Mi Band	24	4					
P4	F	25	Xiaomi Mi Band	2	5	4	3.5	5	7	3
P5	F	23	Kakao Mini	7	10	5	1	3	6	1
P6	F	23	Kakao Mini	3	10	4	1	4	3	4
P7	F	22	SKT NUGU	3	2	5	4	4	8	5
P8	F	38	SKT NUGU	6	6	7	3	1	9	4
P9	F	25	Xiaomi Mi Band	1	2	7	3	4	6	1
			Fitbit Charge	2	9					
P10	M	24	Kakao Mini	3	9.5	3	3	4	5.5	4

4.2 General IoT Devices Use

By exploring the general purpose of use or the type of device used, we can explore what security or privacy issues are. In addition, we can explore potential gaps in different protection motivation models per users and understand how they differ from Privacy Fatigue according to the level of technology or security knowledge. First, we identified various use cases for each type of devices. Many participants

were using Intelligent Personal Assistant as an IoT device and mentioned that they use weather checking, music listening, alarm and timer functions. In addition, the second most popular IoT device was the smart band, and users mentioned that they usually check the clock, step count, heart rate, and analyze the activity and physical condition such as calorie analysis.

Table 2: Participants' general use of IoT device

	Type of Devices	count	Examples	use cases
Smart Homes	Intelligent personal Assistant	6	Kakao Mini, SKT NUGU, Amazon Echo Dot	weather(6), music(6), alarm/timer(6), TV control(2), online searching(2) sports result(1), chat(1), phone call(1)
	Camera	1	LG Home Camera	Pet surveillance(1)
Smart HealthCare	Smart band	5	Xiaomi Mi Band, Apple Watch, Fitbit Charge	time(5), step count(4), heart rate(2), calorie analysis(2), sleep state analysis(1), life pattern analysis(1)

4.3 Mental Models

It is not easy for them to figure out how much people understand IoT network. Mental model can be used to grasp this in a sophisticated way. We asked for a mental model to deeply understand the knowledge that participants have about the IoT network in terms of personal information, including the flow of personal information and the process of use. The participants' mental models were interpreted by two researchers and divided into high dimensional mental models and low dimensional mental models. There are two broad criteria for high and low dimensional mental models. The first is whether or not the personal information can be escaped to the network or the enterprise. The second is whether the feedback to the personal information will affect the user.

The high dimensional mental model corresponds to P1, P3, P5, P6, P9, P10. They understood that their personal information was moved to the mobile phone or other device via the IoT device and then moved back to the server. They also knew that the movement of personal information caused feedback to upgrade the performance of IoT devices. P3 knew what kind of information flowed into each of the Amazon echo dots and Mi-bands that she was using, and understood how it would affect users.

For low dimensional mental models, P2, P4, P7, P8 are applicable. Most of them did not know that personal information could be moved to a server or other company, and some participants did not even know that personal information was mobile. One of them, P2, had a good understanding of the interaction between the device and the user, but did not know clearly how to move personal information to the server.

4.4 Protection Motivation Model and Privacy Fatigue

4.4.1 Perceived Vulnerability

Most participants shared issues related to the convenience or limitations of IoT technology, rather than mentioning privacy concerns when asked questions that did not explicitly address security. However, when asked again about security-related topics, there were more participants perceived to be highly perceived than those who perceived IoT network vulnerabilities as low. In particular, most participants

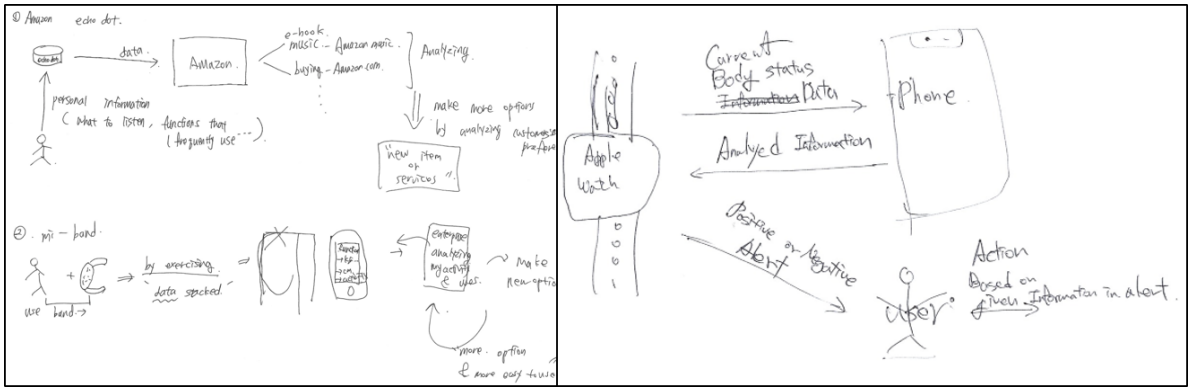


Figure 2: Mental models of participants. The figure on the left is a picture of P3 and is a representative example of a high dimensional mental model. The figure on the right is a picture of P2 and is a representative example of the low dimensional mental model.

highly rated the vulnerability of the IoT network in terms of frequent contact with news related to privacy violation incidents, low confidence in the security of IoT devices and services, and commercial use of users' personal information.

I think that the possibility of personal information leakage is very high. In fact, there are cases where personal information is leaked at banks. (P10)

I was a little hesitant to try a smart refrigerator, and if the company gets my taste or purchase information and recommends it, I think it will flow to my company that I do not want to expose. Because it will be used as marketing, I think it will provide me with advertising and spam. (P7)

On the other hand, some participants felt IoT network vulnerability to be low due to their trust in IoT service companies, and their lack of sophisticated mental models. Particularly, there were participants who did not care about protecting personal information because they thought their personal information was useless. These vulnerability factors that perceived by the participants did not occur in the existing IT environment. Therefore, it can be interpreted that it is possible to explain the cause of privacy fatigue in the IoT environment and how to solve it.

I think my personal information is useless. Even if my personal information could be valuable later on, I do not care because I do not think it's worth it at the moment. (P10)

4.4.2 Perceived Severity

Overall, participants perceived the high severity of the negative consequences of IoT personal information leakage. At the same time, however, they have become dull about the ongoing leak of personal information. Some respondents indicated that real-time stalking and privacy tracking is possible if IoT privacy breaches occur. In addition, other participants noted that massive privacy could be violated through multiple IoT devices / services interlocked. Some participants pointed out that the use of the IoT ecosystem in their everyday lives could lead to an increase in the amount of information the user would be exposed to because of the ambiguity of the perception of safety and risk during use. Taken together, most participants rated the severity of IoT privacy outbreaks higher than the existing IT environment.

Table 3: Participants' perceived vulnerability

		Factors	Mentioned
Perceived Vulnerability	High	Information from News	3
		Low credibility on IoT device / service security	3
		Company's commercial use of personal information	2
		User's high carelessness due to safety frustration	1
		Advanced hacking technology	1
		Low trust for the company	1
	Low	High trust for the company	2
		Novice mental model for IoT network	2
		Low importance of personal information used	2
		High credibility of IoT device / service security	1
		No Information from News	1

I do not use complex functions because my data is gathered somewhere and can be used for stalking. I think it is very serious because if someone thinks about it, they can know my life pattern and then I feel like I'm in front of CCTV for almost 24 hours. (P5)

I think ... The more IoT is used with multiple devices or the Internet, the greater the severity. For example, if I use it in conjunction with IoT and e-mail, I think it is dangerous to collect the search logs basically from the portal site, what I search, what kind of cafe, where to search for restaurants, etc. (P4)

On the other hand, some participants underestimated the severity of IoT privacy violations in terms of low utilization and importance of personal information provided for receiving IoT service, and actively donating personal information for better service quality. Users are encouraged to share and use their personal information in order to use better services, so privacy fatigue has the potential to appear different from the existing ones.

I do not think my personal information is of high value. I do not know where to use it even if a hacker takes my personal information (P5)

I do not feel that the accumulation of my personal information in the database is an information leak, but rather that it makes the software more convenient. It would be nice if my personal information could be used in a better way rather than being abused. (P8)

4.4.3 Self-Efficacy

More than half of the respondents perceived themselves as not fully possessing the skills and abilities necessary for IoT privacy practices. Some participants responded that they had sufficient personal skills and abilities to protect their personal information. Specifically, in order to prevent information infringement, they can stop or use services that are concerned about data infringement during the use of IoT, read personal information terms and conditions, and learn cases of IoT data infringement . In addition, some participants indicated that it would be beneficial for users with low involvement in security to manually present security guidelines. On the other hand, some participants perceived themselves to have insufficient personal skills and abilities to protect their personal information. The reason for this is that the security expertise required to protect personal information in the IoT environment is low, and that it is absolutely dependent on the reputation of the security of a particular company.

Table 4: Participants' perceived severity

		Factors	Mentioned
Perceived Severity	High	Real-time stalking and privacy tracking	3
		Interworking of multiple devices	2
		Low alertness of users in IoT environment	1
		Unpredictable scope of personal information leakage	1
		Global spread of exposed personal information	1
	Low	Low importance of personal information used	5
		Voluntary donation rather than passive infringement	4
		Low utilization and value for personal information	3
		Reliability due to a large number of IoT service users	2
		Personal information that has already been exposed	1

First of all, I think I should pay attention to my choice when agreeing to personal information. If I am concerned about my personal information, I may be able to protect my personal information by stopping or not using the function or service. (P6)

If I hear of other damages, I'll find out. (P7)

It is important to make sure that users are aware of the possible outflow scenarios when using IoT devices, and each product developer would like to disclose in a transparent level of security of these products. (P2)

If I know something technologically, I will be thinking about how to prevent data infringement. But I can't do anything because you do not know because people who are trying to get information are at the hacker level and I am not. So I gave up. (P8)

I pick up a company's products that I trust when choosing IoT devices or services. I believe Apple is using its own cloud to make it safe and uses only Apple products (P2)

Table 5: Participants' self-efficacy

		Factors	Mentioned
Self-Efficacy	High	Suspension of suspicious services	2
		Attention to privacy terms and conditions	1
		Learn about IoT private data breach cases	1
		Periodic data deletion and device reset	1
		Security management through email alarm when IoT device is connected	1
	Low	Minimal interworking and simple functions only	1
		Management through periodic vaccines	1
		Low level of knowledge about security	7
		Over-reliance on the company's security systems	2

4.4.4 Perceived Response Effectiveness

Among the participants, those who believed that they could significantly reduce the possibility of infringement by themselves, and those who showed an ambiguous attitude showed a comparatively comparable proportions. No highly perceived participants were found for perceived response effectiveness levels. In this regard, it can be interpreted that, even if a user actively copes with protecting personal information, it is more difficult to actually reduce the possibility of infringing personal information. Participants who were perceived as low on response effectiveness indicated that no self - coping could be effective in preventing information infringement. For that reason, they have already exposed vast amounts of personal information through the use of IoT, are unable to counter the hacker's hacking skills, and are exposed to the inevitably required personal information in order to receive services. Users shared personal anecdotes and shared a sense of helplessness in that they were forced to use the IoT device / service with the possibility of threat and information infringement on their own.

It seems likely that personal information will be leaked. Anyone with technology is likely to pull out. I think this is an area that I do not know well and I can not avoid it even if I stop it. (P7)

I already have a lot of personal information on the IoT network, so I do not care about protecting my privacy right now. (P8)

I think there is nothing better than cracking the information on my own from a user standpoint. (P9)

Table 6: Participants' perceived response effectiveness

		Factors	mentioned
Perceived Response Effectiveness	Low	Lots of personal information already exposed	3
		High-level hacking technology	2
		Inevitable leakage of personal information to use IoT	2
		Repeated failure experience with privacy or security	1

4.4.5 Response cost

Most participants perceived the magnitude of the psychological and physical factors that interfered with self-practice to protect personal information on the IoT network in the IoT environment, and other participants were ambivalent about the cost of response. The reaction cost was not perceived to be low. The protection of personal information may limit the services that users may receive because of Privacy Terms and Conditions with compulsorily requiring consent. And, consumers are less alert when dealing with IoT devices, which are always used in everyday environments. Therefore, they said that they have difficulty in practicing to protect personal information. In other words, in order to protect personal information, the service should not be provided, the boundaries of privacy invasion should not be overdue, and the expectation cost of reading a vast number of terms and conditions was greatly perceived.

If I do not agree to use personal information, I am not be able to use the IoT service even if I have already purchased IoT device. And if I do not want to agree, I have to agree to go to the next step. (P8)

Terms and Conditions are not on a single page. so I should click through to see it, or scroll to the box. The text is too small, and the amount of content is too large. Also, the readability and accessibility is low. (P5)

I do not act to protect personal information. Because it is more efficient to stay still than to invest in it. I think that the cost of investing is, for example, worrying about what to say or not saying such things. If I have to do that, I will not have IoT device in the first place. (P10)

Table 7: Participants' response cost

		Factors	Mentioned
Response Cost	High	Obligation to Consent to Privacy Terms of Use	3
		Low Accessibility of Personal Information Terms and Conditions, requiring a lot of cognitive/ temporal resources	1
		Low alertness of users in IoT environment	1
		Low level of knowledge about security	1

5 Discussion

Low security knowledge level of IoT users is likely to increase privacy fatigue.
Participant groups showed a high degree of familiarity and involvement in general technology aspects and IoT technology aspects, but low familiarity with computer security aspects because they had little or no interest in security related knowledge. Interviews with IoT users showed that most participants were overestimating or underestimating threat assessments and coping assessments, ultimately trying not to think or act to protect personal information. In this regard, one of the potential causes of distorted threat / coping assessment was the user's low familiarity with security. That is, IoT users perceive severity, vulnerability, efficacy, effectiveness, and response cost as distorted because they are not familiar with security or privacy protection methods. This can be interpreted as causing privacy fatigue by making it difficult for users to perform appropriate protective action strategies and measures such as passively relying on a recognized company or giving up privacy protection. Therefore, as a way to mitigate privacy fatigue with respect to IoT security, it is possible to provide user-friendly guidelines for users to access security. In addition, in marketing stage of IoT devices and services, not only functional and technical aspects but also sufficient information about the security evaluation result of related devices or related systems can be provided, so that users can feel familiar about security in their daily life.

It is possible to feel privacy fatigue differently depending on the usage environment and purpose of IoT device.
Most of the smart home devices that use artificial intelligent speakers are functioned as controller. They use convenience as a substitute for their troublesome tasks. On the other hand, most people using smart bands uses IoT devices to analyze accumulated biomedical data as a function to confirm their real-time data. Unlike existing IT environment, IoT usage environment is attached to user 's house or user' s body and user 's data continues to be used. As a result, users have environmental characteristics that make it difficult to evaluate threats or cope with the use of services, such as doubts about the provision of personal information, awareness, or very low vigilance to accurately judge safety and risk. Smart health care users are continuously using their services in return for providing their personal information, so they have been exposed to "personal information disclosure" and do not care. Smart health care services can be ineffective in securing personal information because it not only creates low alertness but also requires constant collection of personal data. In other words, smart health care device users may become insensitive to continued exposure of personal information, which can lead to a greater tendency to privacy

fatigue.

Privacy fatigue can be increased because it is difficult to see the seriousness if personal information is leaked on the IoT network.
People who are highly perceived and those who are perceived as less serious have not experienced the degree of severity of what physical / psychological damage they will suffer in the event of a dangerous event. Most expressed their own data abandonment of privacy, mentioning that they were already exposed a lot. Some participants predicted that the severity of personal information leakage would be the same as spamming. The IoT environment, which is newly settled in the consumer's daily environment, will be different from the existing IT environment. It is impossible to experience the seriousness of the future IoT infringement because they have never heard about IoT security. IoT users who already believe that a lot of personal information is being leaked use IoT service in return for paying personal information. Their continued failure to protect privacy can increase privacy fatigue.

Lowering the user's perceived vulnerability to IoT can help increase the acceptance of IoT devices and services.
IoT users mentioned the magnitude of the vulnerability of IoT security at an ambiguous level and found that they did not have a standard to judge accurately. As mentioned earlier, it is interpreted as a part of the story because they show low involvement in security. The participant group also overestimated or underestimated the threat assessment due to the ambiguous criteria for vulnerability. Analyzes of responses to factors that consider buying IoT devices or stopping the use of the service suggest that most participants would like to use it because of the aesthetics, convenience, and media novelty of IoT devices. However, the use was stopped because of functional inconvenience and technical incompleteness. That is, the user considers functional convenience as the most important factor in accepting and using the IoT technology and service, while considering the security as secondary. However, since most participants perceived a higher vulnerability to IoT devices than IT devices, marketing the enhanced security of IoT devices and services would make acceptance intention.

6 Conclusion

As the spread of IoT devices increases, the amount of personal information used increases drastically and the perception of personal information changes. It is expected that the privacy fatigue will be differentiated according to the change of the perception, but there is no research on this. Therefore, in this study, 10 participants were interviewed in depth to analyze privacy fatigue in IoT environment. In order to conduct a systematic interview, the interview protocol was constructed based on the protection motivation theory. As a result of interviews, many new perspectives on privacy fatigue were found. Low level of security knowledge of IoT users is likely to increase the level of privacy fatigue and feel differently depending on the environment and purpose of IoT devices. It was also revealed that the intention of accepting IoT devices and services will be different depending on the vulnerability of users to IoT network. Also, it is difficult to feel the seriousness of personal information on IoT network. From various perspectives, we can see that privacy fatigue in IoT environment is very different from the existing IT environment from cause to result. These results can affect the strategy of online suppliers and can benefit IoT devices and service providers. In addition, there is a need for policy makers to understand privacy fatigue in the IoT environment to establish a more realistic privacy policy.

Acknowledgments

This research was supported by the MSIT(Ministry of Science, ICT), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2018-2015-0-00403) supervised by the IITP(Institute for Information &communications Technology Promotion).

References

[1] H. Choi, J. Park, and Y. Jung. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81:42–51, April 2018.

[2] R. Crossler and F. Bélanger. An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (usp) instrument. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 45(4):51–71, November 2014.

[3] R. E. Crossler. Protection motivation theory: Understanding determinants to backing up personal data. In *Proc. of the 43rd Hawaii International Conference on System Sciences (HICSS'10), Honolulu, Hawaii, USA*, pages 1–10. IEEE, January 2010.

[4] C. Gutwin. Roundup of internet of things forecasts. `https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#1c35f9151480` [Online; accessed on August 15, 2018], 2017.

[5] B. Hanus and Y. A. Wu. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1):2–16, 2016.

[6] J. F. Hopstaken, D. Linden, A. B. Bakker, and M. A. Kompier. A multifaceted investigation of the link between mental fatigue and task disengagement. *Psychophysiology*, 52(3):305–315, July 2015.

[7] P. Ifinedo. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1):83–95, February 2012.

[8] M. Keith, C. Maynes, P. Lowry, and J. Babb. Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In *Proc. of the 2014 International Conference on Information Systems (ICIS'14), Auckland, New Zealand*, December 2014.

[9] J. Kwon and M. E. Johnson. The market effect of healthcare security: Do patients care about data breaches? In *Proc. of the 14th Annual Workshop on the Economics of Information Security(WEIS'15), Delft, The Netherlands*, June 2015.

[10] K. Marett, A. L. McNab, and R. B. Harris. Social networking websites and posting personal information: An evaluation of protection motivation theory. *AIS Transactions on Human-Computer Interaction*, 3(3):170–188, September 2011.

[11] Y. J. Park. Digital literacy and privacy behavior online. *Communication Research*, 40(2):215–236, August 2013.

[12] S. Prentice-Dunn and R. W. Rogers. Protection motivation theory and preventive health: Beyond the health belief model. *Health education research*, 1(3):153–161, January 1986.

[13] L. Rainie, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish. Anonymity, privacy, and security online. *Pew Research Center*, 5, September 2013.

[14] B. W. Schermer, B. Custers, and S. van der Hof. The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, 16(2):171–182, June 2014.

[15] H.-y. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59:138–150, June 2016.

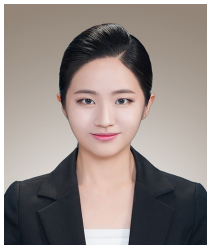
[16] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman. Information accountability. *Communications of the ACM*, 51(6):82–87, June 2008.

[17] I. Woon, G.-W. Tan, and R. Low. A protection motivation theory approach to home wireless security. In *Proc. of the 2005 International Conference on Information Systems (ICIS'05), Las Vegas, Nevada, USA*, page 31. AIS, December 2005.

[18] E. Zeng, S. Mare, and F. Roesner. End user security & privacy concerns with smart homes. In *Proc. of the 13th Symposium on Usable Privacy and Security (SOUPS'17), Santa Clara, California, USA*, pages 65–80. USENIX, July 2017.

Author Biography

Junhyoung Ohreceived the B.S. degree in electrical engineering from Korea University, Seoul, Korea. He is currently pursuing the Ph.D. degree with the graduate school of information security at Korea University. His research interests include Usable Security, Psychological Security and Privacy.



Ukjin Lee received the B.S. degree in industrial psychology from Hoseo University, Cheonan, Korea. She is currently pursuing the M.S. degree with the Department of Psychology at Korea University, Korea. Her research interests include User Behavior, Biometrics Usability evaluating the human factors, and Usable Security.

Kyungho Lee received his Ph.D. degree from Korea University. He is now a professor in the graduate school of information management and security at Korea University, and has been leading the risk management laboratory in Korea University since 2012. He was a former CISO at Naver Corporation, and he was the former CEO of SecuBase Corporation.