The Design of Personal Privacy and Security Risk Scores for Minimizing Consumers' Cognitive Gaps in IoT Settings

Daeeun Choi
Virginia Tech
dechoi@vt.edu

Paul Benjamin Lowry
Virginia Tech
paul.lowry.phd@vt.edu

G. Alan Wang
Virginia Tech
alanwang@vt.edu

Abstract

The advent of Internet of Things (IoT) technology exponentially increases the collection of new information types in consumers' lives from various sensors. However, many consumers do not fully recognize the potential privacy and security risks (PSR) associated with IoT. Those who are aware rarely take action to protect their personal information because of a cognitive gap between PSR and its impact. To address this problem, we propose a design framework for evaluating and quantifying IoT PSRs related to IoT adoption. Grounded in the cognitive dissonance theory (CDT) and information processing theory (IPT), the proposed framework defines IoT PSR scores and proposes a visual representation for improving consumers' awareness of PSRs. Furthermore, we suggest a PSR control balance theory (PSR-CBT) to explicate the consumers' two internal power conflicts. The proposed PSR scores can reduce consumers' cognitive gaps, and thus, help them make informed purchase decisions toward IoT devices and services.

1. Introduction

The rapid evolution of the Internet and the explosion of Internet of Things (IoT) technology has made life very convenient for people, but at the same time, such technological advances posed new challenges to privacy and security protection. Beyond expanding traditional person-to-person communication, IoT extensively uses a vast array of sensors that are the objects of communication for person-to-things and things-to-things communications, as well as existing cellular communication and wireless technologies, such as Bluetooth (BT), Wi-Fi, and Zigbee [1]. Many consumers are attracted to its new features and convenience, either knowingly or unwittingly disclosing their personal information. Sometimes, they are not even aware of personal information leaks. CNN reported IoT privacy and security issues in 2019: "Not only is Alexa listening when you speak to an Echo smart speaker, an Amazon employee is potentially listening, too" [2].

As a result of IoT privacy and security problems, there is a great demand for mechanisms to protect IoT privacy and security. For the IoT security markets, Gartner predicts that, "worldwide IoT security spend will increase from $912M in 2016, soaring to $3.1B in 2021, attaining a 27.87% CAGR in the forecast period" [3].

IoT technology not only collects a massive amount of consumers' information, but it is also capable of understanding and predicting their behaviors. IoT devices are inherently small and cheap with limited privacy and security protection functions because strong protection systems in hardware and software cannot be embedded in a small and cheap device [4]. Thus, the privacy and security risks (PSR) of using IoT technology are much more significant than those of conventional electronic home devices. Consequently, IoT experts have warned consumers about the privacy and security vulnerabilities of IoT. Despite the vulnerability of IoT devices and services, it seems that in some cases, IoT PSRs do not appear to have an influence on the consumers' intention to purchase and use IoT. This is due to consumers' cognitive gaps and lack of awareness of privacy risks and security vulnerabilities related to IoT [5].

To reduce consumers' cognitive gaps and improve the awareness of PSRs, we propose a new mechanism for assessing IoT PSRs, namely personal PSR scores. We determine the PSR scores by collectively considering consumers' IoT information types, weight impact factors, and personal capabilities. Furthermore, we will propose a new design theory for personal PSR assessment that can be used to explain how consumers internally make a disclosure decision [6]. Because a design science research (DSR) concentrates on developing solutions to problems [7], a DSR approach is suitable for the development of our proposed PSR scores and theory. We adopt the information systems design theory (ISDT) because ISDT allows us to apply a set of requirements and designs for a solution. In addition,

URI: https://hdl.handle.net/10125/64366
978-0-9981331-3-3

we adopt the publication schema for DSR [8, 9, 10], which guides us to communicate with prior literature.

2. Literature Review

In this section, we review previous literature to demonstrate consumers' paradoxical behaviors between their attitudes toward PSRs and their actual IoT purchase and use behaviors. The objective is to analyze existing PSRs in the literature and identify new types of IoT PSRs that pose a threat to consumers. We then propose a new artifact as a solution to minimize the cognitive gap and increase consumers' awareness of PSRs.

The consumers' paradoxical behaviors in PSRs occur when the potential risks related to IoT often have little influence on consumers' purchase and use behaviors, until consumers experience serious and adverse consequences (e.g., identify theft). Consumers are limited as to how they manage their IoT PSRs, although they might think that they can control the risks [11]. According to a poll conducted in 2018, even though more than 70 percent of consumers believe that privacy for their data is extremely important and would not purchase products and services from an invasive company, few consumers take actual behaviors to protect their personal information [5]. This survey shows a cognitive gap between consumers' attitudes and actual behaviors toward PSRs. Many scholars have researched the cognitive gap as a privacy paradox and agreed that the awareness of PSRs is negatively associated with paradoxical behaviors toward PSRs. Barth and Jong [12] suggest that "creating privacy awareness in combination with tools that support users in their privacy decisions should help users to avoid paradoxical behavior." Kennedy-Lightsey and Martin [13] claim "perceived risk is key to individuals' disclosure decisions." Therefore, our study focuses on improving consumers' awareness of IoT PSRs, and ultimately minimizing consumers' cognitive gaps between their attitudes toward IoT PSRs and their purchase and use behaviors.

In order to assess privacy risks, prior literature classified consumer-disclosed information into six information types: (1) demographic information, (2) contact information, (3) vehicle information, (4) lifestyle, interests, and activities data, (5) financial and economic data, such as estimated income and home value, and (6) financial and credit data, such as credit score, loan, and credit card data [14]. However, the categorization fails to capture new types of data collected and transmitted by IoT devices, such as consumers' behavioral tendencies, real-time locations, and schedules.

Existing tools for raising privacy and security awareness are also insufficient for IoT devices. Belanger et al. [15] designed online parental consent for kid's electronic transactions (POCKET), which is a practical software solution to protect children from online privacy risks and threats. POCKET allows parents to choose a specific user privacy preferences file (UPPF) that includes the child's name and 27 specific preferences, including the child's first name, last name, email, address, zip code, parents' credit card numbers, and so forth [15]. Although UPPF contains detailed information about the child, it only focuses on basic demographic information.

Ananthula, et al. [16] suggested a method to measure privacy risks in an online social network. It calculates privacy quotient based on the sensitivity and visibility of the information shared by a user. Besides, they propose a privacy index (PIDX) used to measure the level of exposure of privacy. Some scholars have studied the degree to which users disclose their privacy as a score in multiple online social network environments, called the privacy disclosure score (PDS). With calculated PDS, they can analyze the user's potential information loss. Morando, et al. [17] have integrated a variety of privacy evaluation studies with empirical research results on personal data evaluation.

Although there are privacy risk evaluation studies, most previous privacy scoring models focus on the context of social media, rather than the context of IoT technology. Prior literature regarding privacy scoring models has not considered the vulnerabilities of IoT and the new information types that users normally do not encounter in social media. IoT broadly collects consumers' activity data, such as purchasing habits, emotions, real-time location data, and schedules, all of which put the users at PSRs from inappropriate manipulation and secondary use by vendors [18, 19, 20].

3. A Design Science Approach

This study adopts ISDT and the publication schema for a DSR study suggested by Gregor and Hevner [10]. The general overview of ISDT, including the kernel theories, meta-requirements (MR), meta-designs (MD), and testable hypotheses (TH), corresponds to the method section of the publication schema [10]. The MD in ISDT corresponds to the artifact description section of the publication schema. The evaluation section of the publication schema is used to test the research hypotheses of ISDT.

We choose the cognitive dissonance theory (CDT) as our major kernel theory. CDT considers a privacy paradox as a cognitive gap between attitudes

and actual behaviors. IS scholars have already learned that the increase of PSR awareness reduces consumers' paradoxical behaviors [5, 12, 13]. To improve PSR awareness, we adopt the information processing theory (IPT) that can explicate the relationship between information types and individuals' processing abilities toward the information. Furthermore, we propose the privacy and security risk control balance theory (PSR-CBT) based on the control balance theory (CBT) that can be used to explain consumers' internal power conflicts when disclosing their personal information.

Table 1 shows the components of the designed PSR assessment framework following ISDT. MRs are a set of goals for an artifact design [8]. This study proposes three MRs. First, we aim to develop a taxonomy of personal information types related to IoT PSRs using an inductive approach. Second, we design personal PSR scores, representing the level of perceived IoT PSRs, based on the two kernel theories, CDT and IPT. Last, we propose a new design theory based on CBT.

MDs are a set of design elements aiming to meet the MRs [8]. This study's MDs consist of five design elements: (1) a general process design for PSR assessments, (2) the process design of personal PSR scores, (3) the design of ten dimensions (personal information types, weight impact factors, and personal capabilities) for PSR scores, (4) a new model of PSR scores, and (5) a new design theory for PSR disclosures.

The last component of ISDT includes testable hypotheses related to the designed artifact [8]. To evaluate the performance of the proposed artifact, PSR scores, our study provides three evaluation approaches, including evaluation with visualizations, consumers' surveys, and experimental designs for PSR scores.

Table 1. Components of the designed PSR assessment framework

Kernel theories	• CDT • IPT
Meta-requirements	• Development of new dimensions of IoT information types based on inductive approach • Design of personal PSR scores based on the CDT and IPT • New theory based on the CBT and IPT
Meta-designs	• Process design of PSR assessments • Process design of personal PSR scores • Design of proposed ten dimensions for personal PSR scores • New model of personal PSR scores • New theory of the PSR-CBT
Testable hypotheses (Evaluation)	• Visualizations for ten dimensions of personal PSR scores • Evaluations with consumers' surveys • Evaluations with experimental designs

4. An IoT PSR Assessment Framework

In this DSR study, we adopt CDT and IPT as our kernel theories to support the proposed assessment framework for IoT PSRs. Before discussing the theories, we first present general challenges in privacy decision making and set up the boundary conditions for this study.

4.1. Boundary Conditions of PSR Assessment

Acquisti and Grossklags [21] suggested three challenges in privacy-related decision making. Consumers have (1) incomplete information to make PSR disclosures, (2) lack of ability to process their information, and (3) various cognitive biases. We will focus on the problem of having incomplete information and infeasible processes. In particular, for new IoT technology, few consumers understand the vulnerability of IoT and the possibility of data manipulation by vendors. If consumers had more knowledge of IoT privacy and security issues, they would probably be more conservative in purchasing and using IoT devices. The proposed PSR assessment framework will contribute to increasing consumers' awareness about the IoT devices they use, how significant the risks are, and how far they can control their information. Even if consumers had complete information, they would not be able to perfectly process their detailed information because this information is usually very complex [21]. The proposed PSR assessment framework will also contribute to improving consumers' ability to understand the details of IoT privacy and security issues by visualizing consumers' use of different data types and their privacy control capabilities [22]. Last, cognitive biases significantly influence consumers' decision making with PSRs, but we consider this factor to be beyond the scope of the current study and leave it for future research.

4.2. Cognitive Dissonance Theory (CDT)

We leverage CDT [23] to explicate the discrepancy between consumers' attitudes toward PSRs and the actual purchase and use behaviors of IoT products and services.

When people exhibit a conflict between their attitudes and their behaviors, this result is cognitive dissonance. This cognitive dissonance leads to a feeling of mental discomfort. One of the most popular demonstrations of CDT is the "smoking test": A person acquires knowledge about smoking from the media, friends, acquaintances, and physicians. The knowledge that smoking is bad is dissonant with the cognition that he or she keeps smoking [23].

The principle of CDT explains that people

want to avoid disharmony by changing their attitudes or behaviors with an inner drive. CDT suggests three ways to reduce dissonance. First, people can adjust their attitudes, beliefs, or behaviors to reduce their mental discomfort by removing the conflict. In the case of IoT, if consumers know that there is a serious PSR, they are more likely to change attitudes, beliefs, or behaviors around purchasing a product with high risks. However, many individuals have difficulty changing their behavioral responses, despite their well-learned knowledge [23].

Second, people want to eliminate the disharmony between attitudes and behaviors by acquiring new knowledge that outweighs the disharmonious beliefs [23]. With IoT, consumers are likely to expect that IoT companies should provide privacy and security protection by implementing such features into their products and services. They are also likely to expect that IoT providers carefully protect the privacy and security of consumers' data collected through IoT. However, in practice, there are many data breaches, and some companies, such as Amazon and Google, use consumers' personal information to manipulate their consumers and increase revenue [2, 18].

Third, people can diminish the importance of cognition, such as attitudes and beliefs for their cognitive consonance. People try to reduce cognitive dissonance by making an excuse for their behaviors, as mentioned in the example of smokers, who despite knowing the fact that smoking is bad for health [23]. For IoT products, consumers might convince themselves that, even if their personal information is leaked, it will not be that harmful because "they have nothing to hide." This, however, may lead to potentially serious consequences for everyday consumers, such as identity theft, harm to credit scores, and the leak of embarrassing photos or health conditions. The proposed PSR assessment framework can help consumers switch from a cognitive dissonance condition to a cognitive consonance condition by visualizing the information types shared with IoT, and how well they are able to protect their personal information. The improvement process of consumers' awareness of PSRs can be explained by IPT.

4.3. Information Processing Theory (IPT)

IPT originates from the cognitive process theory, which deals with humans' cognitive memories that consist of sensory memory, short-term memory, and long-term memory [24]. The information in sensory memory is usually unconscious and only lasts for up to three seconds. Short-term memory is also known as working memory. The information in sensory memory transfers to short-term memory and lasts for 15-20 seconds in short-term memory before transferring to long-term memory. The amount of an individual's cognitive load, the number of repeats, and individuals' selective processing capability collectively influence how information is processed in the short-term memory. Although long-term memory has much space, it relies on the quality of the organization of the memory, and thus, people cannot usually remember all the information in their long-term memory [25].

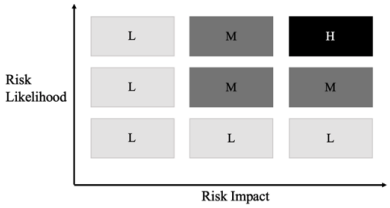
The proposed PSR scores can improve consumers' ability to process their information in working memory and long-term memory by increasing their awareness, as well as their personal capabilities to protect their personal information and organizing their distributed information regarding PSRs. Such improvement will occur because the PSR scores will help consumers visualize their use of data types, prior breach experiences, cultural impact, and the level of privacy literacy with a spider map and scores. Furthermore, the PSR scores will provide a three-level classification of PSRs and display where the consumers best fit [24].

4.4. MD1: The Process of PSR Assessments

The first MD is a general PSR assessment process. Before designing the PSR scores in detail, we need to have a general framework for evaluating personal PSRs with IoT. First, we start with an information collection process to establish the types of PSRs. Because the concept of IoT may be too broad, we focus on IoT technology which collects data from various wireless sensors such as Amazon Echo™ and Google Home™. Second, we identify possible privacy risks and security vulnerabilities based on the collected information. Third, we assess the identified PSRs. However, existing risk assessment developed for social networks might not be applicable to IoT. To determine the level of PSRs, we should find out the likelihood and impact of the identified PSRs [26]. Thus, we determine the likelihood and impact of potential risks. Based on the likelihood and impact, we categorize information types for PSRs. Last, we provide a personal privacy and security evaluation result, which is then used to

develop personal PSR scores.

This study follows MD1, which includes data collection, identification of PSRs and vulnerabilities, assessment of PSRs with the likelihood and impact (see Table 2). For steps 4, 5, and 6 of MD1, we suggest a matrix of personal PSR levels. The risk levels are strongly associated with the risk likelihood and impact [27]. When both factors are high, PSR is the highest. Figure 1 presents the matrix of different PSR levels, which influence the design of information types and weight impacts for MD2-MD4. To apply the last step of MD1 to PSR scores, we propose the process of PSR scores as MD2.



(L: Low; M: Medium; H: High)

Figure 1. The matrix of PSR levels

Table 2. The general process of PSR assessments

Step 1	Information collection in a specific area
Step 2	Identify possible privacy risks and security vulnerabilities
Step 3	Assess the identified PSRs
Step 4	Decide the likelihood of PSRs
Step 5	Decide the potential impact of PSRs
Step 6	Categorize the likelihood and impact of PSRs
Step 7	Provide a personal PSR result

4.5. MD2: The Process of PSR Scores

In this meta-design, we propose a process of generating personal PSR scores. First, we identify PSRs in IoT technology based on existing literature and experts' opinions. Given a new IoT technology, experts' opinions are particularly important because it is not easy to understand and assess the new technology for novices. Furthermore, we use survey data developed by professional survey firms [28, 29]. Second, we generate a taxonomy of IoT PSRs by classifying personal information types. In particular, IoT devices yield various information types that could be breached and used as a tool to manipulate consumers by the vendors [18]. Last, we quantify PSRs as scores and then display the scores in a visualization form [26].

Based on the overall PSR score design process presented in Figure 2, we will propose MD3 and MD4.

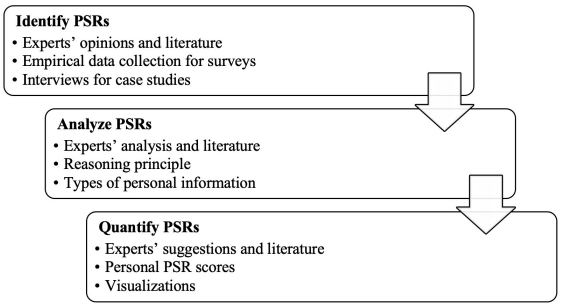


Figure 2. The process of PSR scores

4.6. MD3: The Design of New Dimensions

In this MD, we develop four new dimensions for IoT information types based on an inductive approach. As secondary data, we initially use the surveys conducted in 2018 and 2019 by RSA which is a professional survey company [28, 29]. The results of these surveys indicate that financial and banking information is the most significant threat for IoT consumers, followed by security information identity information, and personal activity information. In particular, consumers' activity information, such as purchasing history and location information, is introduced in new IoT technology environments since vendors can manipulate consumers' purchasing behaviors or personalized advertisements via consumers' activity data [18, 30, 31]. The consumer survey result is summarized in Figure 3. Interestingly, there are big cultural differences in personal information types [28, 29]. For example, US consumers are more sensitive to sharing location data than German and French consumers. US and French consumers are more generous than German consumers in disclosing their information. Early adopters want to purchase IoT devices and services to improve their ability to achieve their goals, for example the monitoring of diet using wearable IoT devices [28, 29].

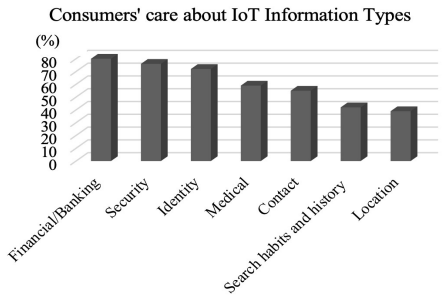


Figure 3. Consumers' care about information types

Figure 4 shows the results of MD3. We start with specific IoT information types such as credit card numbers, passwords, social security number (SSN), personal activities, and location data. Based on the different types of IoT data, we synthesize and create ten themes, such as financial, security, ID, family, contact, activity, location, and time information. These ten themes potentially reveal four new IoT PSR dimensions: monetary, security, identification, and manipulation risks. In practice, although we can directly use the ten themes to analyze a consumer's personal PSR score, we abstract these ten themes to four dimensions that can lead to a new theory in the privacy and security area.

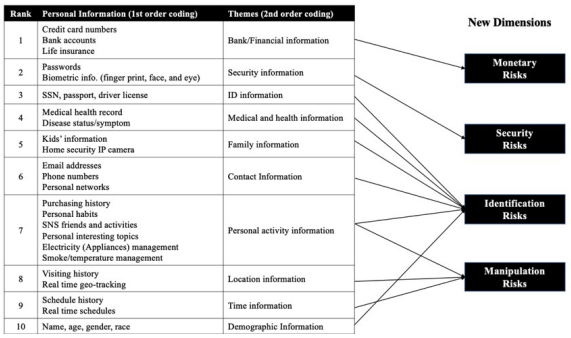


Figure 4. The IoT information type coding

Dixon and Gellman [14] classified consumers' information types for purchasing as demographic, contact, vehicles, lifestyle/interests/activities, financial and economic, and financial and credit data. However, the classification method does not directly apply to IoT because IoT collects more data types. Compared to Dixon and Gellman's classification, the proposed IoT information types adds security, ID, family, location, and time information. Figure 5 shows the proposed ten IoT information types.

Existing Consumer Information Types

	Personal Information Types
1	Demographic information
2	Contact information
3	Vehicles information
4	Lifestyle, interests and activities data (including medical)
5	Financial and economic
6	Financial and credit data

Proposed IoT Consumer Information Types

Rank	Personal Information Types
1	Financial and credit data
2	Security information
3	ID information
4	Medical and health information
5	Family information
6	Contact information
7	Personal activities information
8	Location information
9	Time information
10	Demographic information

Figure 5. The proposed IoT information types

4.7. MD4: The Model of PSR Scores

This MD defines the calculation of personal PSR scores that collectively consider four information types, three weight impact factors, and three personal capabilities. The proposed PSR scores show the level of balance between two powers: personal information disclosure power and personal information control power. The personal information disclosure power is calculated as the product of the four information types and the corresponding weight impact factors. The personal information control power is measured based on three personal capabilities. The weight impact factors positively moderate the relationship between the information risk type and the PSR scores. Volume, culture, and personal breach experiences are the elements of the weight impact factors. Volume is an important element used to determine the weight of the impact of information types on PSR since the impact of risks will fluctuate according to the number of IoT devices, the number of friends on social media accounts, the usage of Cloud services, and the scale of disclosure [32].

Cultural differences also influence the PSRs since culture determines the social norms and values. Soares and Shoham [33] cite the definition of culture from Sekaran in 1983 as "culturally patterned behaviors are thus distinct from the economic, political, legal, religious, linguistic, educational, technological and industrial environment in which people find themselves." Hofstede [34] defines culture as "the collective programming of the mind which distinguishes the members of one human group from another." Hofstede's four cultural dimensions, such as masculinity and femininity, uncertainty avoidance, power distance, and individualism and collectivism, are the outcomes from more than 100,000 IBM employees in 40 different countries [33, 34].

Prior studies found that previous experiences play a significant role as a moderator between optimistic biases and risk estimates at both a personal level and a social level [35]. According to IBM research, 28% of consumers have a data breach experience [36]. "Users who have never experienced a privacy breach are more trusting and link easily with reciprocating users. However, after experiencing a privacy breach, users become aware of the privacy risks on SNS and use the permeability rules to more cautiously share information" [37].

Personal capabilities negatively moderate the impact of information types on the PSR scores. To demonstrate the knowledge dimension in this study, we define knowledge as a technical understanding of the IoT and general computer-related techniques. Based on Byrd and Turner [38], we chose to use the term technical knowledge, which represents programming languages, IoT devices and services,

computer operating systems, expert systems or artificial intelligence (AI), network management and maintenance, developing Web or App-based applications, and big data warehousing or data mining skills.

Compared to the general knowledge of IoT technology, privacy literacy focuses on privacy and security. Prior scholars have suggested the concept of privacy literacy and defined it in various ways [39]. Nevertheless, leading scholars have emphasized the application of skills online as well as the knowledge of privacy: "Online privacy literacy may be defined as a combination of factual or declarative ("knowing that") and procedural ("knowing how") knowledge about online privacy" [40]. Thus, we define privacy literacy as the ability to collect personal information and apply practical skills online for personal data protection and privacy regulation.

Self-efficacy is also one of the essential constructs in privacy and security theories. Bandura [41] introduced self-efficacy before developing the social cognitive theory (SCT). According to the advent and development of computer network markets, computer self-efficacy (CSE) was suggested as a targeted form of self-efficacy. Mobile computing self-efficacy (MCSE) is a specific form of CSE for mobile environments. With the dramatic increase in the use of mobile computing devices, IS researchers have differentiated the self-efficacy of a mobile device from traditional self-efficacy and CSE, in order to analyze their models more accurately [42]. In this study, we follow the definition of self-efficacy, suggested by Johnston and Warkentin [43]: "the degree to which an individual believes in his or her ability to enact the recommended response."

We now describe how to calculate PSR scores mathematically, with four IoT information risk types, three weight impact factors, and three personal capabilities. The amount of each information risk type shared with an IoT device is multiplied by the level of significance, which is estimated using consumer survey results. Based on the survey results in Figure 3, monetary risk information disclosure will be the baseline risk because consumers worry the most about money-related information disclosure [28, 29]. We set its level of significance to be α. Security risk information disclosure is less concerned than money-related information. Its level of significance is β ($\beta < \alpha$). Similarly, the level of significance for identification risk information disclosure is set to δ ($\delta < \beta$) while that of manipulation risk information disclosure is set to γ ($\gamma < \delta$). The weights of the information types can be adjusted over time, based on the latest consumer surveys. For the calculation of the consumers' disclosing power, we multiply information types and weight impact factors because there is an individual difference, based on the consumer's network volume, culture, and previous experience. To calculate personal capabilities, we measure consumers' knowledge about IoT or new technology, self-efficacy, and privacy literacy via survey methods. Finally, we normalize the overall scores. Figure 6 shows the overall model expressed as a mathematical equation. Figure 7 shows the overall framework of the PSR scores. Figure 8 demonstrates the role of a moderator that moderates the impact of consumers' attitudes on their intention to behave.

$$\frac{a}{n}\iiint f(m,s,i,p)dx \cdot w(v,c,e)dy \cdot c(k,f,l)dz \rightarrow R_{score}$$

F_x: Information types

- f(m): Monetary risk information disclosure * α
- f(s): Security risk information disclosure * β
- f(i): Identification risk information disclosure * δ
- f(p): Manipulation risk information disclosure * γ

W_y: Weight impact factors

- w(v): Volume
- w(c): Culture
- w(e): Experience

C_z: Personal capabilities

- c(k): Knowledge
- c(f): Self-efficacy
- c(l): Privacy literacy

*n and a are constants to normalize the score

*α, β, δ, and γ are coefficients of information types

Figure 6. Mathematical equations of PSR scores

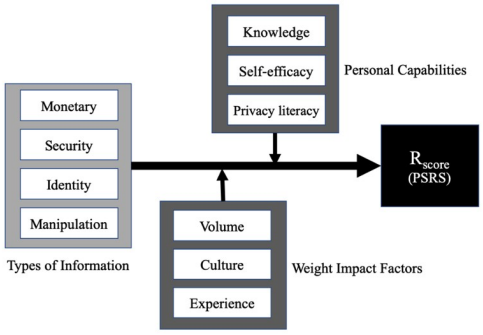


Figure 7. The conceptual framework of PSR scores

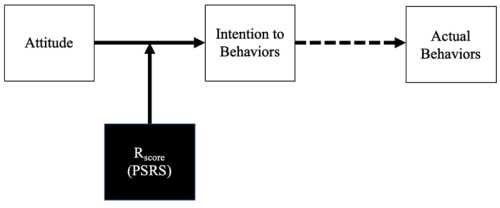


Figure 8. The model of PSR scores

4.8. MD5: A New Design Theory

As a final MD, we propose a new theory, PSR-

CBT, grounded in CBT and IPT [24]. The proposed PSR scores can contribute to not only supporting consumers to move their information from the short-term memory to the long-term memory by quantifying and visualizing the PSRs, but also by improving the identification of consumers' tendencies and abilities.

CBT discusses two powers [6]. When one power is stronger than the other, the stronger power can attack or hurt the weaker one. This study uses the two internal "powers" of personal information disclosure and personal information control. The disclosure power can be evaluated by information types and weight impact factors. The control power can be evaluated by personal capabilities. First, if the disclosure power is stronger than the control power, consumers are likely to disclose their personal information with little hesitation. Although consumers actively communicate with various sensors and online friends via IoT, they would be exposed to high risks. Second, if the disclosure power and the control power move to equilibrium, consumers will fall into a significant cognitive gap or a privacy paradox and hesitate to disclose their information. However, PSR scores can help increase the awareness of their disclosure habits and personal capabilities and reduce the cognitive gap. Third, if the control power is stronger than the disclosure power, consumers are not likely to disclose their information.

In this case, consumers will face limitations in various communications or online social relationships, and could isolate themselves, although their risks will be minimized. Using the equation in Figure 9, we can conclude which power is stronger. If the result is greater than 1, the disclosure power is higher than the control power, and if it is less than 1, the disclosure power is higher than the control power. Using the PSR scores, consumers will be aware of their current vulnerabilities, manage their personal PSRs, and minimize their privacy cognitive gaps.

$$a\ \frac{Information\ types\ \times\ Impact\ factors}{Personal\ capabilities^2} > 1$$

$$a\ \frac{Information\ types\ \times\ Impact\ factors}{Personal\ capabilities^2} \approx 1$$

$$a\ \frac{Information\ types\ \times\ Impact\ factors}{Personal\ capabilities^2} < 1$$

A. Information types * Impact factors > Personal capabilities ➔ Danger!!!
B. Information types * Impact factors ≈ Personal capabilities ➔ Warning!!
C. Information types * Impact factors < Personal capabilities ➔ Attention!

Figure 9. The discriminant of PSR scores

4.9. Visualization

Figure 10 is a simulated outcome with four new personal information types, three weight impact factors for the information types, and three personal capabilities to control PSRs. This spider map shows all the scores of the ten dimensions; consumers can easily recognize their weak parts and strong parts. This visualization will also display the result of the PSR control balance: a warning phrase and graphical signals.

5. DSR Evaluation

As an evaluation of our DSR approach, testable hypotheses of ISDT are used to evaluate whether MDs satisfy MRs [9]. In this study, we use an experimental design to test three hypotheses for the evaluation of our MDs.

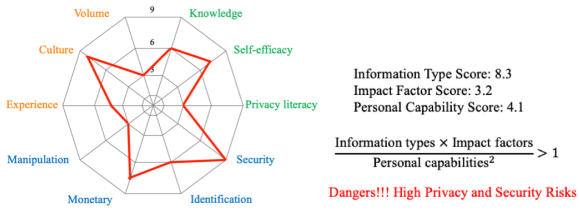


Figure 10. The spider map of the outcomes

We will measure the way in which the change of consumers' awareness toward PSRs is improved before and after having personal PSR scores. To measure if consumers' cognitive gaps are reduced, we will provide three statements. (1) I feel my awareness of PSRs improved after having my PSR scores. (2) I intend to be more careful when using the IoT after having my PSR scores. (3) I am willing to change my behavior towards the use of IoT devices after having my PSR scores.

The PSR scores are calculated by a consumer survey. Table 3 shows the scales of the ten dimensions for the consumer survey. All questionnaires and demographic questions are available upon request.

Table 3. The scales of the ten dimensions

	Personal Information Types				Weight Impact Factors			Personal Capabilities		
Score	Monetary	Security	Identification	Manipulation	Volume	Culture	Experience	Knowledge	Self-efficacy	Privacy literacy
9	Very High	Very High	Very High	Very High	Very High	Very High	Very High	Very High	Very High	Very High
7	High	High	High	High	High	High	High	High	High	High
5	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle
3	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
1	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low

Our testable hypotheses include the following:

TH1: The consumers who see the visualized PSR scores have better awareness of PSRs than those who do not.

TH2: The PSR scores have a negative influence on

consumers' cognitive gaps.

TH3: The PSR scores have a positive influence on consumers' behavioral changes.

6. Discussion

This study potentially contributes to minimizing consumers' cognitive gaps and improving consumers' awareness of PSRs by providing personal PSR scores and visualizing the PSR scores with a spider map and warning messages. We suggest new classifications and dimensions toward IoT information types, such as security, identification, family, location, and time information. These information types are likely manipulated by vendors as well as hackers in IoT settings, since IoT devices and services are naturally vulnerable toward PSRs. Last, this research proposes a new design theory for PSR disclosures called PSR-CBT that explicates consumers' internal assessments toward PSRs in IoT settings by evaluating disclosing power and control power. Furthermore, PSR-CBT can be generalized for other consumers' decision making when they have two internal conflicting powers. For example, when a person posts a sensitive picture on Facebook, there may be a conflict between disclosure power and control power in his or her mind.

However, this study has several limitations. First, although the PSR scores help consumers to increase their awareness of PSRs, the direct influence of the cognitive gap between the attitude and actual behavior is not easily measured since we should measure the change of the consumers' purchasing behaviors. Second, PSR scores can be subjective until we have sufficient PSR score data to compare individuals to populations. Third, the weight for information types and cultural differences can be changed, since the individuals' personalities and experiences can be altered.

As the next steps, first, we can validate and apply the proposed PSR-CBT to other fields to generalize the theory. Although PSR-CBT is applied to IoT settings in this study, PSR-CBT can be applied to other privacy and security issues when consumers make a decision. For example, when a person posts a sensitive picture on Facebook, there may be a conflict between disclosure power and control power in his or her mind. Second, we can identify the distinction between privacy and security in a future study because privacy and security may have different influence mechanisms on consumers' decisions. Third, future studies can carry out to identify consumers' trust issues toward IoT companies. Fourth, although we presented three reasons for privacy and security decision making, we did not consider cognitive biases in this study. We thus suggest further research on the relationship between cognitive biases and the privacy calculus model [31].

7. Conclusion

The advent of IoT leads to a change in the use of information types. Consumers face more serious PSRs because of the new information types that can be easily breached and manipulated by vendors. However, many consumers have limited information about IoT. Even consumers who have enough information about IoT rarely take action to protect personal information because of the cognitive gap.

This DSR study of personal PSR scores in the IoT settings contributes to minimizing the cognitive gap that explicates consumers' paradoxical behaviors and increasing the awareness of PSRs. We followed two DSR methodologies, including ISDT and publication schema for DSR to create the proposed artifact of PSR scores based on CDT and IPT.

The PSR scores consist of three major parts and ten dimensions in detail. IoT information risk types have four dimensions; monetary, security, identification, and manipulation risks. Weight impact factors, composed of volume, cultures, and prior experiences, play a role as a positive moderator between IoT information risk types and personal PSR scores. Personal capabilities, such as technical knowledge, privacy literacy, and self-efficacy for IoT PSRs, negatively moderate between IoT information risk types and personal PSR scores.

The proposed PSR-CBT contributes to consumers' understanding of their behaviors toward PSR disclosures by addressing the individuals' two internal powers. Future studies can develop the concept of PSR-CBT and the PSR scores as a general index that can be practically applied to consumers all around the world.

8. References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things: A vision, architectural elements, and future directions," FGCS, 29(7), pp. 1645–1660, 2013.

[2] J. Valinsky, "Amazon reportedly employs thousands of people to listen to your Alexa conversations," 2019.

[3] A. Rajagopal, "NIST releases IOT cyber security and privacy risks report," 2019.

[4] H. Lin and N. Bergmann, "IOT privacy and security challenges for smart home environments," Information, 7(3), pp. 1–15, 2016.
[5] M. Williams, Exploring the influence of privacy awareness on the privacy paradox on smartwatches. Thesis, Oxford, UK, 2018.
[6] P.B. Lowry, G.D. Moody, and S. Chatterjee, "Using it design to prevent cyberbullying," JMIS, 34(3), pp. 863–901, 2017.
[7] R.L. Baskerville, M. Kaul, and V.C. Storey, "Genres of inquiry in design-science research: Justification and evaluation of knowledge production," MISQ, 39(3), pp. 541–564, 2015.
[8] J.G. Walls, G.R. Widmeyer, and O.A.E. Sawy, "Assessing information system design theory in perspective: how useful was our 1992 initial rendition?" JITTA 6(2), pp. 43–58, 2004.
[9] A. Abbasi and H. Chen, "Cybergate: A design framework and system for text analysis of computer-mediated communication," MISQ, 31(4), pp. 811–837, 2008.
[10] S. Gregor and A.R. Hevner, "Positioning and presenting design science research for maximum impact," MISQ, 37(2), pp. 337–355, 2013.
[11] H. Cai, B. Xu, L. Jiang, and A. Vasilakos, "IOT-based big data storage systems in cloud computing: Perspectives and challenges," IEEE, 4(1), pp. 75–87, 2017.
[12] S. Barth and M. de Jong, "The privacy paradox - investigating discrepancies between expressed privacy concerns and actual online behavior," Telematics and Informatics, 34(7), pp. 1038–1058, 2017.
[13] C.D. Kennedy-Lightsey and M. Martin, "Communication privacy management theory: Exploring coordination and ownership between friends," Communication Quarterly, 60(5), pp. 665–680, 2012.
[14] P. Dixon and R. Gellman, "How secret consumer scores threaten your privacy and your future," 2014.
[15] F. Belanger, R.E. Crossler, J.S. Hiller, J.M. Park, and M.S. Hsiao, "Pocket: A tool for protecting children's privacy online," DSS, 54(2), pp. 1161–1173, 2013.
[16] S. Ananthula, O. Abuzaghleh, N.B. Alla, and S. Prabha, "Measuring privacy in online social networks," IJSPTM, 4(2), pp. 1–9, 2015.
[17] F. Morando, R. Iemma, and E. Raiteri, "Privacy evaluation: What empirical research on users' valuation of personal data tells us," IPR, 3(2), pp. 1–12, 2014.
[18] R. Calo, "Digital market manipulation," HeinOnline, 82(4), pp. 995–1051, 2014.
[19] H. Smith, S. Milberg, and S. Burke, "Information privacy: Measuring individuals' concerns about organizational practices," MISQ, 20(2), pp. 167–196, 1996.
[20] J. Kininmonth, T. Thompson, N. McGill, and A. Bunn, "Privacy concerns and acceptance of government surveillance in Australia," ACIS on December 3-5 in 2018, Sydney, Australia, 2018.
[21] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," IEEE, 3, pp. 26–33, 2005.
[22] K. Greenaway, Y. Chan, and R. Crossler, "Company information privacy orientation: A conceptual framework," ISJ, 25(6), pp. 579–606, 2015.
[23] L. Festinger, A theory of cognitive dissonance. CA: Stanford University Press, 1957.
[24] G.A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information," Psychological Review, 63(2), pp. 81–97, 1956.
[25] R.C. Atkinson and R. Shiffrin, "A proposed system and its control processes," PLM, 2, pp. 89–195, 1968.
[26] S. Kucukali, "Risk scorecard concept in wind energy projects: An integrated approach," Renewable and Sustainable Energy Reviews, 56, pp. 975–987, 2016.
[27] H. Li, W. G. No, and T. Wang, "Sec's cybersecurity disclosure guidance and disclosed cybersecurity risk factors," IJAIS, 30(C), pp. 40–55, 2018.
[28] RSA, "Privacy and security report," 2018.
[29] RSA, "RSA data privacy and security survey," 2019.
[30] C.E. Tucker, "Social networks, personalized advertising, and privacy controls," JMR, 51(5), pp. 546–562, 2014.
[31] Y.Q. Zhu and J.H. Chang, "The key role of relevance in personalized advertisement: Examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions," CHB, 65, pp. 442–447, 2016.
[32] D.H. Park and S. Kim, "The effects of consumer knowledge on message processing of electronic word-of-mouth via online consumer reviews," ECRA, 7(4), pp. 399–410, 2008.
[33] A. Soares and A. Shoham, "Hofstede's dimensions of culture in international marketing studies," Journal of Business Research, 60, pp. 277–284, 2007.
[34] G.H. Hofstede, Cultures and organizations: Software of the mind. NY: McGraw-Hill, 1991.
[35] H. Cho, J. Lee, and S. Chung, "Optimistic bias about online privacy risks," CHB, 26(5), pp. 987–995, 2010.
[36] P. Allor, "Key findings from the 2017 cost of data breach study: Global overview," 2017.
[37] B. Osatuyi, K. Passerini, A. Ravarini, and S.A. Grandhi, "'fool me once, shame on you...then, I learn.' an examination of information disclosure in social networking sites," CHB, 83, pp. 73–86, 2018.
[38] T.A. Byrd and D.E. Turner, "Measuring the flexibility of information technology infrastructure: Exploratory analysis of a construct," JMIS, 17(1), pp. 167–208, 2000.
[39] M. Bartsch and T. Dienlin, "Control your Facebook: An analysis of online privacy literacy," CHB, 56, pp. 147–154, 2016.
[40] S. Trepte, D. Teutsch, P. Masur, C. Eicher, M. Fischer, A. Hennhofer, and F. Lind, "Do people know about privacy and data protection strategies? Towards the online privacy literacy scale", pp. 333–365. 2015.
[41] A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," Psychological Review, 84(2), pp. 191–215, 1977.
[42] M.J. Keith, J.S. Babb, P.B. Lowry, C.P. Furner, and A. Abdullat, "The role of mobile-computing self-efficacy in consumer information disclosure," ISJ, 25(6), pp. 637–667, 2015.
[43] A.C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," MISQ, 34(3), pp. 549–566, 2010.