A Hybrid Model of Rationality and Non-Rationality for Information Privacy Decision Making

Bongsik Shin
Management Information Systems
Fowler College of Business
San Diego State University
Email: bshin@sdsu.edu

Gimun Kim
Management Information Systems
School of Business,
Chungnam National University, Korea
Email: gmkim12@cnu.ac.kr

Abstract

The growing access to private information has been amplifying concerns of privacy compromise. Although concerned about privacy, people still give up their personal information to online services too easily, thus called 'privacy paradox.' Privacy Calculus Theory (PCT) has been dominant to explain the contradictory behaviors. It, however, has been subject to criticism as it relies on unrealistic rationality assumptions of decision making and there have been growing calls to embrace nonrational theories and their elements. We introduce a hybrid model that explains privacy paradox through three antecedents—cognitive bias, affect and need—drawn from the nonrational viewpoints of behavioral economics, psychology, and biology. The proposed model is significant in privacy research as it proposes a new theory intended to harmoniously complement (rather than contradict) the PCT in explaining the "privacy paradox" of online service users.

1. Introduction

An enormous amount of personal information is gathered by online service firms to support their business needs (e.g., service customization, target marketing) [1]. As such, online service users frequently face situations to decide whether to release their personal information. Among the situations are to join a new membership, receive personalized services, participate in an event, and accept friend requests on a social network platform [2]. The growing access to personal information inevitably amplifies concerns of privacy compromise. According to [3], many people feel that they already have lost the ownership and control of their own personal information. There is a swelling fear that information privacy is getting out of hand.

Despite that individuals are gravely concerned about their privacy in jeopardy, they still easily give up their personal information to online businesses. The privacy paradox has been noted by studies (e.g., [4]). Among many studies attempted to explain the contradictory behaviors, the privacy calculus theory (PCT) has been widely accepted [4][5]. It is a type of *rational theory* because individuals are expected to perform rational decision-making (or rational risk-benefit assessment).

Meanwhile, there has been a stream of scholarly publications that pointed out the problems of PCT in explaining *information privacy decision making* (hereafter *IPDM*) as it relies on the unrealistic assumptions (i.e., agents with omniscience or unbounded rationality) [4][6]. The studies argue that postulating *nonrationality* (or bounded rationality) in the risk-benefit assessment better reflects the real circumstance of IPDM. The *nonrationality* means that humans are not omniscient (i.e., not rational) and thus make various mistakes or errors in their decision-making process. As such, there have been growing calls for expanding research efforts, embracing nonrational factors that interfere with the IPDM processes [7][8]. In fact, the work of [7] empirically proves that both rational and nonrational forces are in play simultaneously when it comes to privacy-related decision-making. Despite, there has been little research efforts to reconcile their interplays to better explicate decision dynamics as researchers chose to anchor their research on the rational or nonrational ground [7].

As one of theoretical efforts to reconcile the two valid perspectives, we introduce a hybrid model that compensates the limitations of Privacy Calculus Theory by identifying and including primary nonrational factors in swaying the risk-benefit perceptions. In the model, first, the decision to disclose private information is reached through the risk-benefit

assessment as predicated in rational decision making; and second, the self- assessment process, however, is moderated much by nonrational forces. To explicate how the nonrational decision-making occurs, our model identified three nonrational forces (i.e., cognitive bias, affect, and need) drawn from the behavioral economics, psychology, and biology domains. Subsequently, we offer propositions that define the dynamics between the nonrational factors and the risk-benefit assessment. ***The theoretical contributions of this work are:*** first, the proposition of a hybrid model that harmonizes both rationality and nonrationality in IPDM; and second, the identification of primary nonrational dimensions (i.e., cognitive bias, affect, and need) and specific factors pertaining to each dimension and their incorporation into propositions to further future research.

2. Rational vs Nonrational Theories

There is a significant volume of research on decision making and related theories are largely divided into rational and nonrational theories, the terms stated by [9] and [10]. The two schools of thought take fundamentally different positions on the rationality of decision makers. According to [9], rationality is a set of skills or aptitudes (e.g. computational power, knowledge, time, resources including information) we use to discover a course of actions necessary to achieve a goal.

Rational theories postulate the existence of “unbounded” rationality (i.e., a prototype of homo economicus) of an agent in the skill or aptitude set. In other words, these theories are grounded on the implicit assumption that the agent has unlimited computational power, knowledge, time, and resources [12]. The unbounded rationality assumption typically underlies economic theories (e.g., expected utility theory, subjective expected utility theory) as they are derived from homo economicus, a cornerstone of all neoclassical economic models [13]. With the underlying “omniscience”, rational theories rely on an ideal that people reach optimal decisions—that is, final decisions to maximize the expected utility—through the rational and unbiased decision-making process [12]. For instance, according to subjective expected utility (SEU) theory, agents choose between alternatives by determining their possible consequences, estimating their probability and utility, multiplying the probability by the utility, and summing the result. Once the computation has been performed, the agent selects an alternative with the highest expected utility (i.e., optimal decision).

Nonrational theories refer to a heterogeneous class of decision-making theories intended to

overcome the unrealistic assumption of an agent’s unbounded rationality [10]. Though heterogeneous, the nonrational theories share the common base of an agent’s bounded rationality. First introduced by [11], an agent’s ability for rational decision making is considerably bounded by her cognitive limitations and environmental constraints such as available time, information, and resources. Subsequently, psychologists and behavioral economists introduced bounded rationality theories grounded on the agent’s cognitive limitations [14]. According to the theories, cognitive limitations (or cognitive biases, cognitive illusions) impede an agent’s rational decision-making processes, engendering a wide variety of reasoning errors (e.g., [15]). The positioning of nonrational perspectives is considered more realistic [10].

3. PCT & Rational Decision Making

3.1. PCT

PCT was introduced to explicate the privacy paradox, and has become a dominant theory that the majority of information privacy publications relied on. Figure 1 summarizes the relationship between the core variables of PCT [16][17].

Figure 1. Privacy calculus theory (PCT)

Information disclosure means the revealing of private information to a service provider [18]. An individual’s *privacy concern* is a general attitude toward losing the control of her personal information [19]. As can be seen, a person’s privacy concern is more native and thus is not cultivated by the engagement with a particular transactional environment (e.g., website) [1]. The variables of *perceived risks* and *perceived benefits* represent the beliefs that information disclosure is going to result in certain losses or gains [1][16]. Unlike *privacy concerns*, *perceived risks* and *perceived benefits* are situational factors tied to a particular context or environment [1].

Grounded on rational and economic theories, PCT views privacy as something equivalent to a commodity subject to business transactions [20]. According to PCT, individuals agree to disclose their personal information and accept subsequent risks in exchange

for tangible/intangible benefits [21]. PCT assumes that, in facing situations to decide the information disclosure, individuals have or are given complete information necessary to make sound judgments and comprehend their consequences (i.e., benefits and risks). Also, as a rational theory, it is presumed that an individual is fully competent to precisely compute anticipated risks and benefits facing a decision situation [22]. The overall risk is obtained when each risk factor's significance is multiplied by its probability of occurrence, and, subsequently, all risk scores are aggregated. The same approach is used to derive the overall benefit. This complex computational decision-making process is frequently called *risk-benefit assessment*. An individual, then, compares the overall scores of expected risks and benefits, and determines a utility score.

3.2 Limitations

The criticism of PCT comes primarily from those who study behavioral economics (e.g., [23]). They point out that the PCT's normative assumptions including the availability of complete information, rationality in risk-benefit assessment, and assessment objectivity do not reflect the reality. First, PCT assumes that an individual can have complete information on risks and benefits of information disclosure when a situation arises. This is, however, not convincing as it is very difficult for a person to know all the risks and benefits (see Table 1) of information disclosure in a particular decision-making situation [24].

Second, PCT assumes that individuals are completely rational in privacy decision making. That is, it assumes that they are competent in processing a large volume of information on risks and benefits [25]. The reality is that, when there is an information overload situation, people are simply overwhelmed. Naturally, many researchers who believe in such cognitive (e.g., computational ability) limitations were drawn to bounded rationality in information privacy research [4][26].

Third, PCT assumes that an individual reaches a consistent decision whenever she faces the *same* or *similar* situation of information disclosure because the decision is driven by the rational and correct calculation [27]. In other words, PCT postulates that the offeror's computational outcome (i.e., expected utility) of the expected risk-benefit tradeoff is largely invariable. In reality, however, she/he displays different reactions to the same or similar situations [27].

Benefits	Financial compensation (e.g., membership point, free gift, credit point, samples, discount, gift card, voucher), customization service, service augmentation, and tailored offer [1][2][24].
Risks	Psychological damage, private information abuse, financial loss, time and effort to remove resulting spam emails, unsolicited telemarketing, sacrifice in credit score, and others [2][24].

Table 1. Benefits and risks of private information disclosure

4. Nonrational Information Privacy Decision Making (IPDM)

Many psychologists and behavioral economists suggested that the human-being has two independent memory systems, which enable two different modes of thinking—rational and nonrational [9] [10]. From the duality perspective, then, PCT implicitly embraces rational or high-effort process as the computation of risk-benefit tradeoffs demands conscious, analytical, and systematic assessment of potential risks and benefits [6][29]. As already stated, however, an online user is unable to have complete information in facing a situation to decide information disclosure. Also, her cognitive limitations (including cognitive biases) make it practically impossible to do the complex risk-benefit computation. Besides, as she is mostly subject to decision making on the fly, such thorough and analytical assessment of risks and benefits is hardly possible [6]. Due to the personal and situational limitations, postulating IPDM as a rational process (as argued by PCT) is not tenable. Rather, it is more realistic to expect that the decision results from the compromised mental efforts [30][31] of a quicker and simpler judgment process [32]. Also, expecting a person to undertake precise risk-benefit assessments is not cogent [29]. Rather, it would be more convincing to postulate compromised, subjective, and thus erroneous decisions as the process of risk-benefit assessment is more likely biased by the constraints. That is, the risks and benefits of a privacy decision are inevitably overestimated or underestimated [6].

We believe that the nonrationality of IPDM stems from the limitations of both the human (e.g., bounded rationality) and the decision-making circumstance (e.g., limited time, information, and resources). The circumstantial restrictions, however, equally apply to

all individuals facing privacy decisions and thus may not hold a key in comprehending the dynamics of risk-benefit assessment. In our theoretical model, therefore, the circumstantial constraints become underlying assumptions rather than being included as antecedents of IPDM. That is, our research model focuses on the limitations of humans. There are significant variations in the degree people are cognitively biased and affected by emotions and needs. The variations should naturally lead to differences in the risk-benefit evaluation of private information sharing.

4.1 Proposition of a Hybrid Model

Built on the previous discussions, we propose a high-level model (see Figure 2) that depicts an individual's IPDM when she faces a situation of privacy concession. Derived from a comprehensive review of information privacy literatures related to the theoretical viewpoints, our model is composed of three antecedents of *cognitive bias*, *need*, and *affect*, which infuse nonrationality into the risk-benefit assessment. This is in addition to the influence of rational, normative factors. As a result, perceived benefits and risks can be either over- or underestimated, and consequently this may engender biased IPDM.

Whereas several current studies adopted the attitude variable—*Intention to disclose private information*—as the outcome of privacy decisions, we embrace the behavior variable of *private information disclosure*. This is because, although intention has long been used as a proxy of behaviors, such proxy relationship does not hold well in the context of information privacy [4]. For example, [33] discovered that individuals share much more private information than they originally intended. [7] empirical work also highlights the differences between hypothetical and actual IPDM.

Our research model significantly differs from existing privacy studies in two major fronts. First, according to the comprehensive literature reviews by [6][16][19] and [34], *privacy concern* was the only variable that mediates the effects of many antecedents on *perceived risks*. Also, according to the review studies, as is the case of PCT in Figure 1, no antecedents of *perceived benefits* have been identified and empirically tested. Whereas, our model proposes antecedents (i.e., need, cognitive bias, affect) that are expected to influence both perceived benefits and perceived risks. Second, existing studies undertaken from the nonrationality perspective have rarely considered benefit- and/or risk variables as part of the decision-making process. As a result, there has been a lack of systematic theoretical explanations on how the nonrational forces could “distort” IPDM [6]. Our work fills the large void that current research fails to

address. ***Based on the theoretical position, we offer propositions subsequently focusing on the effects of nonrational forces in swaying or moderating privacy risk-benefit perceptions.***

Figure 2. Proposed hybrid model of IPDM & propositions

4.2 Effects of Cognitive Bias

Current studies primarily examine the direct association between cognitive biases and privacy behaviors. Thus, the influence that cognitive biases have on the assessment of perceived risks and benefits has not been given enough theoretical considerations [6]. As stated, our study postulates bounded rationality of individuals and incomplete information during IPDM. In such situation, they are restricted in their ability to systematically estimate the risk-benefit tradeoff and, also, the inadequate and/or inaccurate information becomes their decision base [24]. Additionally, their cognitive prejudices make the objective valuation more difficult [25]. Cognitive biases generally result in lower cognitive efforts during IPDM [29], because they steer a person to use simple mental processes [36]. This way, a person's cognitive biases impede her from undertaking rational examination of risks and benefits based on logical reasoning [37]. Not surprisingly, this will result in an inaccurate and erroneous appraisal of the situation [38].

Meanwhile, cognitive biases may not have equal bearing on IPDM. Some may play a bigger role in inflating benefits and suppressing risks, while others may have an opposite effect suppressing benefits and inflating risks. Among the biases discussed, *optimism*, *overconfidence*, *immediate gratification*, and

hyperbolic discounting tend to be more associated with the former (i.e., inflate benefits and suppress risks); whereas, *framing* and *loss aversion* are more tied to the latter (i.e., suppress benefits and inflate risks).

Optimism is a tendency to believe that one's chance of experiencing negative incidents is lower than others [39]. An online user with optimistic personality may underestimate the risks of divulging private information as she tends to discount the chance and impact of negative incidences [40] [41]. Whereas, with a higher anticipation that good things will happen, she may overrate the benefits of private information disclosure [40]. *Overconfidence* represents a person's excessive conviction of her own skills and knowledge [42]. A person with a higher confidence in her own capacity tends to believe that she can control the consequences of private information disclosure [43]. Thus, she may underestimate risks and overestimate benefits. *Immediate gratification* means that people tend to give more weight on 'current' benefits than 'future' risks [44]. As a similar notion, *hyperbolic discounting* is a person's disposition to ignore expected costs or benefits in the future [45]. A person with a higher inclination for immediate gratifications and hyperbolic discounting prefers more immediate results [44]. Facing information privacy decisions, therefore, those seeking immediate satisfactions are expected to inflate benefit perceptions (e.g., convenience in online order placement) and to underrate risk perceptions.

Framing and *loss aversion* are introduced by Prospect Theory [15]. *Framing* means that, when an individual makes decisions, she may frame her behavioral outcomes differently from the earlier status quo. Facing the decision situation, therefore, a person with a positive frame on information disclosure could end up with a risk-benefit assessment much different from a person with a negative frame. In other words, while the "gain" frame may amplify benefits and underestimate risks of private information sharing, the "loss" frame may work opposite. *Loss aversion* means that an individual displays a higher disposition (about twice) to avoid losses than to opt for gains. These days, private information gathered through various channels is abused for commercial gains. People are increasingly awakened by the implicated risks, which may be felt stronger among those of high loss aversion. Thus, facing a privacy decision, those with a loss-aversion tendency may be more mindful of potential risks and even amplify them. On the other hand, as they weigh more on the risk side, they may play down benefits of private information sharing.

Proposition 1: In the private information disclosure decision, cognitive biases of optimism, overconfidence, immediate gratification, hyperbolic discounting, and 'gain' frame lead a person to (P1a) underestimate risks and (P1b) overestimate benefits.

Proposition 2: In the private information disclosure decision, cognitive biases of 'loss' frame and loss aversion lead a person to (P2a) overestimate risks and (P2b) underestimate benefits.

4.3 Effects of Affect

Affect reflects an individual's subjective sentiments or feelings [46]. An individual's positive or negative affect has a bearing on her cognitive conditions [47]. A person with a stronger positive affect pays more attention to information congruent with it, and naturally thinks and behaves more positively. Likewise, an individual with a stronger negative affect is more mindful of information compatible with it and displays more negative thoughts and behaviors. Psychologists call such tendency as 'congruent effects' [19]. Due to the congruent effect, an individual may selectively factor in the information compatible with her positive or negative affect and excludes other information even if it is relevant to decision making. That is, affect curtails the amount of information useful for decision making, and subsequently the reduced mental effort leads to faster decisions. Further, relying on the information skewed by the positive or negative affect more likely results in biased privacy decisions.

As a type of affect, the *emotion* causes the congruent effect as it constrains a person from individuating available information for informed decisions. For example, a person who experiences strong negative emotions (e.g., anger, fear) tend to consider only information that agrees with her emotions and reaches quick decisions [48]. This partial decision making due to the congruent effect is similarly experienced by a group of positive emotions (e.g., elation, physical arousal) [49]. For example, [50] reported that personal enjoyment of a website grows her trust in the site and its privacy protection. According to [51], whereas positive emotions of a consumer toward a product or service tend to reduce her sense of its risks, negative emotions reinforced her risk perceptions.

Likewise, psychology research demonstrates that a person's *mood*, independent of situational stimuli, can have the congruent effect on her thoughts and judgment. [52] explain the mood-congruity in terms

of the information processing method. According to them, those with strong positive moods (e.g., happiness) tend to make quicker decisions without having concerted assessment efforts due to their belief that things will progress well. On the other hand, those with strong negative moods (e.g., sadness) tend to make rather prudent decisions as their situational assessment is more conservative and thus exert more efforts to find solutions.

As discussed, a person under excessive emotional influences tends to make decisions congruent with her emotional conditions and thus oftentimes flawed ones. An individual facing a privacy decision may be in a positive or negative mood [35], and also she may experience positive and/or negative emotions from the decision situation [19]. The mood and emotional conditions make it difficult to objectively evaluate involved risks and benefits due to the congruent effect [6]. Based on the expected congruency between an individual's emotions/moods and her assessment of risks/benefits of private information sharing, we propose that:

Proposition 3: In the private information disclosure decision, an individual of strong negative emotions/moods overestimates its risks (P3a) but underestimates its benefits (P3b).

Proposition 4: In the private information disclosure decision, an individual of strong positive emotions/moods underestimates its risks (P4a) but overestimates its benefits (P4b).

4.4 Effects of Need

Risk-Sensitivity Theory suggests that a person's need impinges upon the risk-bearing decision making. As an example offered by them, a person running late should decide whether to run to catch a bus. Running itself is an act bearing both risks and benefits. If she arrives at the bus station early enough to catch a bus, she saves waiting time and can get to work in time. If she misses the bus despite running, she only wastes energy or may end up hurting herself due to an accident. In this scenario, her decision depends entirely on the level of her need. If the need is strong enough, she is expected to put more weights on benefits than risks.

The influence of needs is easily applicable to other situations. For illustration, let's consider a sports game. The losing team finds itself in a decision situation regarding whether to put more emphasis on offense than defense. If the team reinforces the offense line replacing defense players, its chance to score goals and even winning the game increases; but, at the

same time, it is taking the risk of allowing more goals due to the weakened defense. At this juncture, the losing team's decision rests logically on its need for a win. If this game is the last chance to advance, the team will definitely make a decision to do everything to drive offense. If there is still a chance to advance despite this loss, the team may choose to strengthen its defense not to allow additional goals.

The examples demonstrate that the risk-benefit assessment and decisions in real life are much simplified and swayed by personal needs. Likewise, a person with a strong leaning toward either privacy protection or privacy disclosure is expected to be skewed in the risk-benefit assessment for the gratification (or justification) of such personal inclination [25]. That is, if she values protected privacy (i.e., low privacy disclosure need), she may overestimate risks and at the same time underestimate benefits of private information sharing to be congruent with her need. The same line of reasoning applies to a person who welcomes private information sharing as it justifies more benefits than risks congruent with her need. Meanwhile, an online user's needs for privacy protection and disclosure may change in accordance with the satisfaction level of previous decisions [53]. In other words, a person may perceive more benefits than risks in divulging personal information at a particular point in time, but that perception may wane over time.

Proposition 5: In the private information disclosure decision, a person with high (or low) privacy protection needs will overestimate (or underestimate) the potential risks of private information disclosure.

Proposition 6: In the private information disclosure decision, a person with high (or low) privacy protection needs will underestimate (or overestimate) the potential benefits of private information disclosure.

Proposition 7: In the private information disclosure decision, a person with high (or low) privacy disclosure needs will underestimate (or overestimate) the potential risks of private information disclosure.

Proposition 8: In the private information disclosure decision, a person with high (or low) privacy disclosure needs will overestimate (or underestimate) the potential benefits of private information disclosure.

5. Discussions

Our research proposed a theoretical model intended to facilitate research on the grounds of both rationality and nonrationality in information privacy decision making (IPDM). The hybrid model has several theoretical and practical implications and benefits.

First, the model can contribute to the expansion of research that postulates nonrationality in IPDM. There is a clear need for comprehensive theoretical models that can drive information privacy research through the lens of nonrationality [4]. [6] proposed a model based on the famous “Antecedents — Privacy Concerns — Outcomes (APCO)” macro model [16]. It is a high-level abstraction in which the variables including *cognitive bias* and *affect* have a bearing on the level of privacy concern, trust and perceived risk, and their inter-relationships. Unlike the APCO type models, we derive significant antecedents (e.g., cognitive bias, affect, and need) that influence the risk-benefit assessment of privacy decisions based on the theories introduced by different academic disciplines. We, then, offer concrete mechanisms of why and how the nonrational antecedents affect the personal evaluation of risks and benefits. This way, our model is more empirically verifiable than the enhanced APCO model.

Second, ours is a general-purpose model and thus broadly applicable to study information privacy decisions in diverse online service settings (e.g., online shopping, social networks, online gaming). The broad applicability is due to that the model contains high-order antecedent constructs from which many low-order variables can be defined for empirical examinations in a variety of study contexts. For instance, excessive optimism and over self-confidence are select variables of cognitive bias; resource acquisition, socialization and happiness reflect the need for privacy disclosure; and anxiety, fear, and sense of perplexity are variables of negative emotion. The decision context (e.g., online shopping, social network) of private information sharing differs in many ways (e.g., type and sensitivity of private information shared). Naturally, the statistical significance of antecedent variables may be more context-dependent and also the same antecedent variable could have differing impacts depending on the context of information sharing. In order to pursue information privacy research through the lens of nonrationality, therefore, researchers may come up with specific study variables pertaining to each antecedent and relevant to a particular research context.

The influence of these variables may vary over time. Generally, cognitive bias variables may not

change much in their level as they are innate to an individual. That is, the “timing” factor (e.g., last month, last week, today) may not be an important consideration for their operationalization and assessment. However, “timing” may have a significant bearing on the variables related to need and affect. We believe that the measurement of variables whose values are subject to change over time becomes more accurate when the respondents’ recollection efforts are minimized.

Third, our model postulates the unpredictable outcome of the risk-benefit assessment as it is subject to the conditions of antecedents. This, in fact, is the core mechanism that explains the influence of a person’s nonrationality on her privacy decisions. Without the assumption of “unpredictability”, it is difficult to find a plausible explanation of a person’s privacy decisions. According to PCT, a person is expected to reach consistent decisions within the similar (or same) context of online services, and thus to display coincident behaviors [27]. In reality, however, she often goes for higher risk options [25] or the ones contradictory to previous choices despite their circumstantial similitude [6]. The behavioral unpredictability, therefore, well justifies the addition of personal traits into the research model. Despite, existing research that embraces nonrationality elements didn’t look at it from the perspective of risk-benefit assessment. That is, the current nonrationality-based studies largely failed to define the risk-benefit evaluation aspect and to explicate how the evaluation mediates the relationship between the nonrationality antecedents and privacy-related behaviors. Factoring in the dynamic and variable nature of the personal risk-benefit assessment into the research model helps researchers clearly observe the privacy paradox. For instance, our hybrid model can explain a person’s biased risk-benefit assessment (e.g., underestimate risks, overestimate benefits) through its congruence with her mental/emotional conditions [29]. Embracing the fluid nature of the risk-benefit assessment as the central theoretical tenet is expected to significantly boost the explanatory power of an individual’s privacy decisions.

Fourth, in our model, the nonrational antecedents influence both risk- and benefit perceptions. Our model differs from other macro-level models appeared in literature review publications such as [6][16]. The macro models all suggest that the risk perception is only affected by privacy concerns as in Figure 1, but the benefit perception has no influential antecedents. This may be due to that the assumption of rational decision making underlies most studies. When rationality in decision making is postulated, there is a logical link between *privacy concern* and *risk factors*;

but, relating *privacy concern* to *benefit factors* becomes problematic. If, however, research builds on the additional nonrationality premise, we can expect that high privacy concerns will attribute to the underestimation of perceived benefits. Our model, therefore, offers balanced views in information privacy research by logically explaining the influence of the antecedents on both perceived risk and benefit factors. In addition, whereas the antecedent of perceived risks is primarily limited to *privacy concern* in current studies, our model offers additional factors (e.g., cognitive bias, affect, need) that are expected to affect both perceived risks and benefits.

Fifth, our model has practical implications by offering additional theoretical perspectives to the debates of privacy regulation. As the indiscriminate gathering of private information by online services is seriously risking service users' fundamental rights, there has been heated debates between the government and the industry about the necessity of privacy-related regulations. Service firms argue that the government's involvement is unnecessary as the personal practice of self-control is sufficient [41]. On the other hand, the government insists its active engagement through regulatory measures as there are mounting concerns of private information abuse (e.g., [41] [54]). From the perspective of nonrational privacy decisions, the service firm's argument of online users' self-control capability (exercising rational judgments) remotely reflects the reality. If people are unable to adequately assess risks and benefits, they may not want the complete ownership of information privacy decisions. Meanwhile, the government's argument for regulations has been lacking a theoretical ammunition to back it up and our model can fill the void if its integrity is empirically validated.

6. Conclusion

We proposed a general-purpose research model of private information disclosure postulating significant nonrationality in the decision-making process. Although Privacy Calculus Theory (PCT) that highlights people's rationality in decision making has been dominant, it has been exposed to wide criticism as it relies on untenable assumptions. Naturally, there has been growing calls for research to embrace 'nonrationality' of privacy decisions by online service users. Due to the relative lack of research grounded on the 'nonrationality' premise, theoretical models that can guide empirical as well as theoretical research have been lacking. This work intends to serve the need by explicating privacy decisions through the lens of three nonrational antecedents (i.e., need, cognitive bias, affect). Identified through comprehensive

reviews of current works from several disciplines, the antecedents are expected to alter the benefit- and risk perceptions of information sharing, and subsequently sway privacy decisions. On the other hand, the variables of non-rationality introduced here are, by no means, an exhaustive list and thus more efforts are warranted to identify other significant ones. Also, we caution that the nonrational dimensions and factors are not the only sources of irrationality. For example, the irrationality in the form of disconnect between the perceived risks/benefits and the actual disclosure decisions being made has been discussed. Our hybrid model significantly differs from the existing ones that posit either rationality or nonrationality of privacy decisions. Our model offers a concrete mechanism that the antecedents cause sub-optimal decisions and consequently behaviors of 'privacy paradox'.

7. References

- [1] Wilson, D., and Valacich, J. 2012. "Unpacking the privacy paradox: irrational decision making within the privacy calculus," *Proceedings of the 33rd International Conference on Information Systems (ICIS 2012)*, Orlando, USA.
- [2] Zhu, H., Ou, C. X., van den Heuvel, W. J. A. M., and Liu, H. 2017. "Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision making," *Information & Management*, 54(4), pp. 427-437.
- [3] PEW RESEARCH, 2016. The state of privacy in America: what we learned, <http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacyin-america/>.
- [4] Kokolakis, S. 2017. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, 64, pp. 122-134.
- [5] Morosan, C., and DeFranco, A. 2015. "Disclosing personal information via hotel apps: A privacy calculus perspective," *International Journal of Hospitality Management*, 47, pp. 120-130.
- [6] Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box," *Information Systems Research*, 26(4), pp. 639-655.
- [7] Adjerd, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, 42(2), pp. 465-488.
- [8] Goes, P. B. 2013. "Information systems research and behavioral economics," *MIS Quarterly*, 37, iii-viii.
- [9] Simon, H. A. 1993. "Decision making: Rational, nonrational, and irrational," *Educational Administration Quarterly*, 29(), pp. 392-411.
- [10] Gigerenzer, G. 2001. "Decision making: Nonrational theories," in *International encyclopedia of the social and behavioral sciences*, N. J. Smelser and P. B. Baltes

- (Eds.), Vol. 5, Oxford, UK: Elsevier, pp. 3304–3309,
- [11] Simon, H. A. 1945. *Administrative behavior: A study of decision making processes in administrative organization*, New York: The Free Press.
 - [12] Basel, J. S., and Brühl, R. 2013. "Rationality and dual process models of reasoning in managerial cognition and decision making," *European Management Journal*, 31(6), pp. 745-754.
 - [13] Morgan, M. S. 2006. "Economic man as a model man: Ideal types, idealization and caricatures," *Journal of the History of Economic Thought*, 28(1), pp. 1-27.
 - [14] Todd, P. M., and Gigerenzer, G. 2003. "Bounding Rationality to the World," *Journal of Economic Psychology*, 24(2), 143–165.
 - [15] Kahneman, D., and Tversky, A. 1981. "The framing of decisions and the psychology of choice," *Science*, 211(4881), pp. 453-458.
 - [16] Smith, H.J., Dinev, T., and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly*, 35(4), pp. 989-1015.
 - [17] Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information disclosure on mobile devices: reexamining privacy calculus with actual user behavior," *International Journal of Human-Computer Studies*, 71(12), pp. 1163-1173.
 - [18] Kehr, F., Wentzel, D., and Mayer, P. 2013. "Rethinking the privacy calculus: On the role of dispositional factors and affect," *Proceedings of the 34th International Conference on Information Systems (ICIS 2013)*, Milan, Italy.
 - [19] Li, H., Sarathy, R., and Xu, H. 2011. "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors," *Decision Support Systems*, 51(3), pp. 434-445.
 - [20] Bennet, C. J. 1995. *The political economy of privacy: a review of the literature*, Hackensack, NJ: Center for Social and Legal Research.
 - [21] Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. "Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts," *European Journal of Information Systems*, 22(3), pp. 295-316.
 - [22] Anderson, C. L., and Agarwal, R. 2011. "The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information," *Information Systems Research*, 22(3), pp. 469-490.
 - [23] Tsai, J. Y., Egelman, S., Cranor, L. and Acquisti, A. 2011. "The effect of online privacy information on purchasing behavior: An experimental study," *Information Systems Research*, 22(2), pp. 254–268.
 - [24] Acquisti, A. 2010. "The economics of personal data and the economics of privacy," Carnegie Mellon University Research Showcase, Working Paper, pp. 1-50.
 - [25] Mishra, S. 2014. "Decision making under risk: integrating perspectives from biology, economics, and psychology," *Personality and Social Psychology Review*, 18(3), pp. 280-307.
 - [26] Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science*, 347(6221), pp. 509-514.
 - [27] Acquisti, A. and Grossklags, J. 2005. "Privacy and rationality in individual decision making," *IEEE Security and Privacy*, 3(1), pp. 24-30.
 - [28] Acquisti, A., and Grossklags, J. 2004 "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior," in *The Economics of Information Security*, L. J. Camp and S. Lewis, eds., Kluwer, pp. 165–178.
 - [29] Barth, S., and de Jong, M. D. T. 2017. "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," *Telematics and Informatics*, 34(7), pp. 1038-1058.
 - [30] Gigerenzer, G., and Selten, R. 2002. *Bounded rationality: The adaptive toolbox*, MIT Press.
 - [31] Gigerenzer, G., and Gaissmaier, W. 2011. "Heuristic decision making," *Annual Review of Psychology*, 62, pp. 451-482.
 - [32] Simon, H. A. 1956. "Rational choice and the structure of the environment," *Psychological Review*, 63(2), pp. 129-138.
 - [33] Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, 41(1), pp. 100-126.
 - [34] Bélanger, F., and Crossler, R. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly*, 35(4), pp. 1017-1041.
 - [35] Kehr, F., Wentzel, D., Kowatsch T., and Fleisch E. 2015b. "Rethinking privacy decisions: Pre-existing attitudes, pre-existing emotional states, and a situational privacy calculus," *Proceedings of the 23th European Conference on Information Systems (ECIS)*, Münster, Germany.
 - [36] Polites, G. L., and Karahanna, E. 2013. "The embeddedness of information systems habits in organizational and individual level routines: Development and disruption," *MIS Quarterly*, 37(1), pp. 221–246.
 - [37] Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015a. "Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Information Systems Journal*, 25(6), pp. 607-635.
 - [38] Aivazpour, Z., Valecha, R., and Rao, H. R. 2017. "Unpacking privacy paradox: a dual process theory approach," *Twenty-third Americas Conference on Information Systems*, Boston.
 - [39] Helweg-Larsen, M., and Shepperd, J. A. 2001. "Do moderators of the optimistic bias affect personal or target risk estimates? A review of literature," *Personality and Social Psychology Review*, 5(1), pp. 74–95.
 - [40] Cho, H., Lee, J. S., and Chung, S. 2010. "Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience," *Computers in Human Behavior*, 26(5), pp. 987-995.
 - [41] Baek, Y. M., Kim, E. M., and Bae, Y. 2014. "My privacy is okay, but theirs is endangered: Why comparative

- optimism matters in online privacy concerns,”
- [42] Jensen, C., Potts, C., and Jensen, C. 2005. “Privacy practices of Internet users: self-reports versus observed behavior,” *International Journal of Human-Computer Studies*, 63(1), pp. 203–227.
 - [43] Brandimarte, L., Acquisti, A., and Loewenstein, G. 2013. “Misplaced confidences privacy and the control paradox,” *Social Psychological Personality Science*, 4(3), pp. 340–347.
 - [44] Acquisti, A. 2004. “Privacy in electronic commerce and the economics of immediate gratification,” in *Proceedings of the 5th ACM Electronic Commerce Conference*, New York, USA, pp. 21–29.
 - [45] O’Donoghue, T., and Rabin, M. 2001. “Choice and procrastination,” *Quarterly Journal of Economics*, 116(1), pp. 121–160.
 - [46] Cohen, J. B., Pham, M. T., and Andrade, E. B. 2008. “The nature and role of affect in consumer behavior,” in *Handbook of Consumer Psychology*, C. P. Haugtvedt, P. Herr, and F. Kardes (eds.), Mahwah, NJ: Lawrence Erlbaum, pp. 297–348.
 - [47] Damasio, A. R. 1994. *Descartes’ error: emotion, reason, and the human brain*, Putnam, New York.
 - [48] Bodenhausen G. V., Mussweiler, T., Gabriel, S., and Computers in Human Behavior, 31, pp. 48–56.
 - Moreno, K. N. 2001. *Affective influences on stereotyping and intergroup relations*, Erlbaum, Mahwah, NJ.
 - [49] Ariely D, and Loewenstein, G. 2006. “The heat of the moment: The effect of sexual arousal on sexual decision making,” *Journal of Behavioral Decision Making*, 19(2), pp. 87–98.
 - [50] Wakefield, R. 2013. “The influence of user affect in online information disclosure,” *Journal of Strategic Information Systems*, 22(2), pp. 157–174.
 - [51] Chaudhuri, A. 2002. “A study of emotion and reason in products and services,” *Journal of Consumer Behavior*, 1(3), pp. 267–279.
 - [52] Schwarz, N., and Clore, G. L. 2007. *Feelings and phenomenal experiences*, Guilford, New York.
 - [53] Mishra, S., and Fiddick, L. 2012. “Beyond gains and losses: the effect of need on risky choice in framed decisions,” *Journal of Personality and Social Psychology*, 102(6), pp. 1136–1147.
 - [54] TRUSTe, 2016. U.S. consumer privacy index 2016, <https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/>.