Consumer Perceived Vulnerability, privacy calculus and information disclosure: an empirical investigation in retailer loyalty program

Abstract:

This paper investigates how perceived vulnerability moderates the effect of privacy calculus on consumerss' willingness to share information. Consumers' information disclosure behavior has been primarily studied from "privacy calculus" approach. For example, Kehr et al (2015) defined "*privacy calculus*" as "*a situational-specific trade-off of privacy related risk and benefit perceptions, bounded by dispositional tendencies and irrational behavior*" (Kehr, et al, 2015). According to Kehr et al (2015), in addition to the benefits and risks, dispositional factors and other situational factors, their gut feeling in these situations also affect consumers information sharing decision making. Indeed, the situational factors associated with psychological limitations and the general dispositional factors make it necessary to consider the constructs such as perceived vulnerability, perceived control and perceived trust into consideration when model the privacy calculus to understand how consumers make the tradeoffs for information disclosure. Therefore, our study contributes to the privacy calculus research literature by identifying the salient factors affecting consumer information disclosure decisions and in particular by providing insights into how consumer's perceived vulnerability could affect the salience and immediacy of privacy related constructs in their decision-making. Empirically, we use discrete choice analysis method. We provide participants with choices from bundles of attributes (constructs identified in the literature). The attributes that are shown are chosen by Sawtooth software in a way that allows all attributes to be compared to all others with the least amount of overlap. Using a monte-carlo style simulation, we can derive the relative importance of each of the attributes. This initial study will allow us to narrow down which elements are most important in a more complex choice analysis. We then use the videos to prime participants into a state of vulnerability. Finally, then we test the priming conditions to see if they make a difference in these choice methods. The theoretical significance of the research is to differentiate the effect of privacy concerns and perceived vulnerability, trust and control on consumer information disclosure. This has empirical implications for firms to find ways to enhance consumers' data sharing/disclosure behavior.

Introduction

We are in the era of Internet of Things (IoT) with big data [1]as one of its distinct features. Personal data[2] is one source of big data (George et al, 2010). We can foresee that in the near future, the demand, supply and exchange of personal data would

[1] Big data: volume, velocity and variety

[2] Personal data/information is defined as 'any information/data relating to an identified or identifiable natural person' Bonneau and Preibusch (2010).

increase drastically. Despite the benefits of big personal data (discussed extensively in the literature[3]), personal data could also potentially cause negative effects for firms and individuals[4]. The negative effects of personal data are primarily associated with privacy issues. Thus, privacy protection becomes the main concern for big data and its analytics in order to leverage benefits of personal data. Government has entered this space through legislation for privacy protection. Indeed, research has shown that consumer's concern for privacy is not absolute; consumers often make the trade-off between privacy concerns and economic benefits (Hann et al, 2002) (Godel et al, 2012, p.53). In some cases, we are relaxed about the scrutiny, i.e., we are willing to give up privacy in exchange for rather simple services. A privacy calculus has been employed to consider the decision for individuals on information disclosure. Consumer information disclosure has been investigated primarily using "privacy calculus" approach. The key issue here is that making these trade-offs for information disclosure decision requires consumers to have the skill/capability to understand the implications. However, when consumers are lack of the skills or not in the state to make these tradeoffs, they are deemed 'vulnerable'. Indeed, aside from state intervention, others argue that privacy is a red herring, and what needs to be addressed is vulnerability. Thus, vulnerability would be a key issue to be addressed in order to both protect consumers from the negative externalities of the personal data market and enable them to engage in appropriate benefits. The focus of this research is to provide insights into how consumer's perceived *vulnerability* could affect the salience and immediacy of privacy calculus in individual decision-making concerning personal data disclosure.

Privacy vs. privacy concerns

Based on the definitions of privacy[5], informational privacy has also been defined as (1) a right (2) claim and (3) control[6]. In the literature, it is suggested that privacy

---

[3] The positive externalities for firms include (1) improving decision making (Brown et al, 2011; Brynjolfsson et al, 2011); (2) delivering holistic product experience for consumers in manufacturing sector (Fleischmann et al, 1997; Guedria et al, 2009; Jun et al, 2007; El Kadiri, et al, 2016); and, (3) achieving real time targeting by recognizing customers' near-purchase-decision (Brown et al, 2011). For individuals, disclosing personal data would enable them to get (1) immediate monetary compensation (e.g. discounts) and information-based price discrimination; (2) intangible benefits (personalization and customization of information content); and, (3) better information by receiving targeted ads (Acquisti, 2010).

[4] For firms, these cost could include (1) being punished by the market by being perceived as invasive of consumers' privacy through mere collection of data but not adequately protecting consumer data (Ponemon, 2009); and, (2) incurring costs associated with data protection, over-investment in data security, and legislatively enforced data protection initiatives (Acquisti, 2010). For individuals, disclosing personal data could bring about cost and negative externalities include (1) privacy harms (subjective and objective) (Calo, 2011) and privacy costs (such as psychological discomfort; the embarrassment or social stigma and the effect of fear; (2) a state of uncertainty associated with privacy costs; (3) higher prices paid due to (adverse) price discrimination; and, (4) being manipulated towards services that consumers do not need because of segmentation and profiling by firms (Acquisti, 2010).

[5] Privacy as (1) **a claim, entitlement**, (2) or right ["the right to be left alone" (Warren & Brandeis, 1890; Solove, 2002; OM et al, 2007, p.157); (3) a **measure of control** an individual has over oneself ("a boundary control process in which the individual regulates with whom contact will occur and how much and what type of interaction it will be" (Pedersen, 1997)] and (4) a state or condition of limited access to a person ["Voluntary and temporal withdrawal of a person from the general society" including four sub-states: anonymity, solitude, reserve and intimacy (Westin, 1967); 'being apart from others' (Weinstein, 1971, p.626); "a state of limited access to a person" (Schoeman, 1984); "a boundary regulation process where people optimize their accessibility along a spectrum of "openness" and "closedness" depending on context" (Dourish, Leysia Palen and Paul);

[6] [**Right**: individual's right to determine how, when and to whom information about the self will be released to another person (Westin, 1967) or to an organization (Om, 2007, p.158); Individuals have the right to sell their personal data and capture some of the value in their data in the market)]; **claim** ("an individual's claim to control the terms under which personal information –

concerns could be a measurable proxy for privacy (Smith, et al, 2011). "Information privacy concerns refer to *an individual's subjective views of fairness within the context of information privacy* (Campbell 1997). "People often have different opinions about what is fair and what is not fair concerning a firm's collection and use of their personal information" (Smith et al, 1996, p.190).

Concern for information privacy is a tested, multidimensional construct (Smith et al. 1996; Stewart and Segars 2002; Awad and Krishnan, 2006). The first scale for the measurement for information privacy concern (CFIP: the concern for information privacy) was developed by Smith, Milberg and Burke (1996), which include such dimensions as collection, errors, unauthorized second use, improper access. According to Smith et al (2011), these dimensions have since been deemed as some of the most reliable scales for measuring individuals' concerns toward organizational privacy practices. This scale was further developed and validated in the context of Internet by Malhotra, Kim, and Agarwal (2004) and operationalized a multidimensional scale: IUIPC (Internet users' information privacy concerns) consisting of dimensions: control, awareness of privacy practice, errors, unauthorized secondary use, improper access and Global information privacy concern. This scale would be used to measure privacy in our research.

2. Privacy calculus

Privacy concern is not the only factor affecting information disclosure. Research on consumer information disclosure behaviour has primarily used a 'privacy calculus' approach. For example, Kehr et al (2015) defined privacy calculus as "*a situational-specific trade-off of privacy related risk and benefit perceptions, bounded by dispositional tendencies and irrational behaviour*" (Kehr, et al, 2015, xxx, page number?). According to Kehr et a (2015) consumer decision making behaviour concerning privacy is effected by the perception of the benefits (such as potential for financial rewards, personalization, self-enhancement and pleasure), the risks (such as implication private data disclosure to criminal parties), the dispositional factors (such as an individual's general doubts about information privacy or confidence about the general data requesting mechanisms; the perceived sensitivity of information disclosure) and other situational factors (such as individuals' (in)ability to process the information for these trade-offs or their "gut" feeling in data disclosure situations). Indeed, the situational factors associated with psychological limitations and the general dispositional factors make it necessary to consider the construct of perceived

information identifiable to the individual- is acquired, disclosed, and used" (Kang, p.1205); "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others" (Westin, 1967, p.7) (Hong and Landay, 2004, p. 177; Malhotra et al, 2004)] and **control** ("the ability to control the acquisition or release of information about oneself" (Froomkin, …p.1464); "the ability of the individual to personally control information about one's self" (Stone, et al, 1983)]

vulnerability into consideration when modelling the privacy calculus in order to achieve privacy protection in information disclosure.

3. Vulnerability: actual vs and perceived vulnerability

Vulnerability is a concept conceptualised and operationalized in marketing, psychology and crime studies. In Marketing, vulnerability has been referred to as *actual and perceived vulnerability* (Smith and Cooper-Martin, 1997). *Actual vulnerability occurs when vulnerability is, in fact, experienced and only can be understood by listening to and observing the experiences of the consumer. Perceived vulnerability occurs when others believe a person is vulnerable, but he or she may not agree or may not be (Baker, Gentry, and Rittenburg, 2005, p.2).*

Consumer actual vulnerability is defined as "*a state of powerlessness that arises from an imbalance in marketplace interactions or from the consumption of marketing messages and products*" (Baker, Gentry, and Rittenburg, 2005). Vulnerability is a transient experience, which could be experienced by anyone in some specific consumption contexts (*Broderick et al, 2011, p.9*). The actual vulnerability arises from the *interaction* of personal states, personal characteristics, and external conditions within a context where consumption goals may be hindered (Broderick et al, 2011). Consumer vulnerability occurs when barriers prohibit control and prevent freedom of choice (Baker et al. 2005; Broderick et al, 2011).

In marketing, research on vulnerability has primarily focused on perceived vulnerability. Perceived vulnerability is defined from third party's perspective. Vulnerable consumers were described as consumers "*who are more susceptible to economic, physical, or psychological harm in, or as a result of, economic transactions because of characteristics that limit their ability to maximize their utility and wellbeing* (Smith and Cooper-Martin, 1997, p.4). The characteristics of these (groups) vulnerable consumers are discusses from (1) their demographic characteristics (including "ethnicity, domicile, and low levels of education and income", Smith and Cooper-Martin, 1997, p.6) and the associated diminished capacities to understand the role of products and advertisements effects (Ringold, 1995); cognitive limitations (Walsh, and Mitchell (2005); and the resultant incapability of making informed decisions at the time of purchase (Morgan, Schuler, and Stoltman (1995). Commuri and Ekici (2008) suggest vulnerability construct with two dimension/components. Therefore, "consumer vulnerability may be hypothesized as a sum of two components: *a systemic class-based component and a transient state-based component*" (Commuri and Ekici, 184) (including both perceived and actual vulnerability).

In psychology and crime studies, perceived vulnerability is person-perceived-based. In psychology, perceived vulnerability has been defined as "as the subjective probability of becoming the victim of a disease. This equals one's perceived risk of

such an event" (Schwarzer,1994, p.162). In crime study, perceived vulnerability has been referred to as "*a belief that one is susceptible to future negative outcomes and unprotected from danger or misfortune. Accompanying this cognition is an affective component, consisting of feelings of anxiety, fear and apprehension"* (Perlof, 1983, p.43).

Therefore, it is possible to suggest that vulnerability could be (1) individual-based and (2) societal-system- based. Individual-based vulnerability consists of two dimensions: actual and perceived. These two dimensions are interconnected. When people experience actual vulnerability, they would also perceive them to be vulnerable for the future outcomes. But actual vulnerability might not be the necessary antecedents for vulnerability.

In our research context, we would focus on the effect of actual vulnerability (the transient experiences in a specific context) on consumer willingness to share their information. Methodologically, we could not observe participants' behaviour and talk about their experiences; we cannot provide the homogeneous contexts for participants to trigger their vulnerability. Therefore, we would use priming method in the experiment. Therefore, we would use Perlof (1983)'s definition and measurement for perceived vulnerability.

4. Control: actual vs perceived control

According to White (1959), control is regarded as a human driving force and defined as the need to show their competence, superiority and mastery over the environment (Hui and Bateson, 1991, p.174). According to Hajli and Lin (2016), control can be divided in to perceived control and actual control. Recently, Pagnini, Bercovitz, and Langer, (2016) defined perceived control as "*an individual's belief about his or her own capability of exerting influence on internal states and behaviors, as well as one's external environment* (Langer, 1977; Lefcourt, 1966; Pearlin & Schooler, 1978; Wallston, Wallston, Smith, & Dobbins, 1987)". Perceived control has also been defined as "perceived ability to alter events and achieve desired outcomes (Burger, 1989; Wallston, Wallston, Smith, & Dobbins, 1987)" ''a person's belief to significantly alter and predict a situation'' (Perry et al. 2001; Burger 1989) (Hajli and Lin, 2016, p.113). "Actual control is regularly used within theory and research to describe whether the nature of control over eventuality is truly within a person's control or not (Seligman 1975) and whether the person really (Bandura 1982) has the ability to wield control over diverse situations or events (Connell et al. 1985; Weisz et al. 1982)" (Haiji and Lin, 2016). Despite the conceptual distinctions, in operationalization, it is argued that "given the extent that perceived behavioral control is accurate, perceived control can serve as a proxy of actual control and can be used for the prediction of behavior (Ajzen 2002)" (Haiji and Lin, 2016, p.113).

Perceived control entails three types of interconnected beliefs: behavioural control (*the availability of a response which may directly influence or modify the objective*

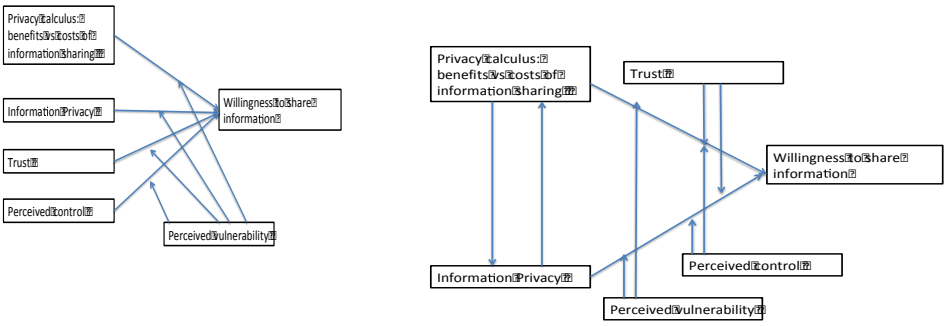
characteristics of a threatening event"); cognitive control (the way in which an event is interpreted, appraised, or incorporated into a cognitive "plan") and decisional control (the opportunity to choose among various courses of action) (Averill, 1973) p.287). Haiji and Lin (2016) described these three beliefs as: *behavioral control refers to one's aptitude to change neutrally the nature of a forthcoming event, whereas cognitive control refers to people's perception of whether they are able to understand and predict the nature of a forthcoming event. Decisional control generalizes expectations that one can gain a desirable outcome after dealing with an event (Lee 2012; Thompson et al. 1993; Skinner et al. 1988)"* (Haiji and Lin, 2016, p.113). Rothbaum (1982) argued the importance of the distinction between primary and secondary perceived control. "*Primary perceived control* describes the attempt to modify the environment to align with one's wishes (e.g., knowing that it is possible to re- schedule an appointment). *Secondary perceived control* refers to using mental strategies to change one's wishes so that they reflect the environment (e.g., deciding that an unreachable outcome is not that desirable, after all)" (Rothbaum, et al (1982, p.92). In our research we focus on perceived primary control.

5. Trust

In order to live a routine life, we need to place our trust in people, the services those people provide and act unreflectively. However, on occasions when our routine is broken, we have to evaluate risk and assigning trust in order to make decisions (Rutter, 2001). Trust has been extensively studied in various disciplines such as business, psychology and sociology and thus the trust objects range from business relationships, organisations, culture, e-commerce, and social life. For example, in the literature, trust has been defined as (1) expectations or confidence (Crosby et al, 1990), faith (Ramaswami et al, 1997) that the trusted party would have regular, honest, cooperative behavior) or behave in the interest of the customer (Anderson and Narus, 1990; Fukuyama (1995; Crosby et al, 1990); (2) a set of beliefs of/"Perceived" credibility (integrity) and benevolence, ability and predictability (Doney and Cannon, 1997; Gafen, Karahanna and Straub, 2003); (3) willingness to rely and depend (Doney et al (1998); Ganesan (1994); Gefen (2000;2002a); Gefen and Silver (1999); Gefen (2002b) derived from their beliefs and confidence; (4) willingness to be vulnerable (Jarvenpaa et al (1998) based on expectations of the trusted party's behavior (Jarvenpaa et al (1998; Mayer et al, 2005; Mayer and Davis, 1999; Mishra (1996). Empirically, trust could be measured by (1) trusting beliefs in terms of benevolence, competence, integrity and the resulting trusting intentions by measuring the willingness aspect (McKnight et al, 2002).

We propose that consumers' willingness to share their information will be the result of their trade-offs of the benefits and the costs associated with information sharing and their perceived importance of information privacy. The effect of perceived control, perceived vulnerability and trust on consumers' willingness to pay are

provisionally depicted in the above diagrams. These relationships would be tested through our experiments.



Research Question

Of primary interest to us is how individual-based, transient affective vulnerability states effect personal data disclosure decisions. We suspect that, regardless of a person's personal privacy beliefs, being made to feel more or less vulnerable will effect an individual's decisions about disclosing personal data. We question to what extent does a transient affective state of vulnerability influence decisions about personal data disclosure.

In addition, we explore the moderating effect of trust and control features of service offerings on personal data disclosure. We are interested in knowing how an offering's trust and control features might mitigate vulnerability-induced concerns. Similarly, we are interested in knowing how trust and control features are made more or less important in different affective states of vulnerability and across different individual privacy beliefs.

Methodology

To test our research questions, we will use an empirical quantitate method to measure the relative importance of the features of a service offering across different experimentally designed conditions of induced affective vulnerability. In a online survey, research participants will be asked to choose which features are most and least important in making a decision about disclosing personal data to a service provider. Some participants will be primed to be in a highly vulnerable affective state while others will not. We suspect that different features will be identified as more or less important in different states of vulnerability regardless of privacy beliefs.

This methodology is known as max-diff scaling and falls within the realms of conjoint-based choice analysis. The benefits of conjoint-based choice methodologies include allowing participants to more easily identify the dominating features of a decision in the face of a complex set of features. The methodology results in an estimation of utility factors for each individual feature. In our case, we plan to compare the utility of trust, control, and benefit features across two conditions: low and high vulnerability state.

Findings

The empirical research is undergoing. The preliminary findings would be presented in the conference.

References

References would be provided upon request.