A Review of Measures of Disclosure Outcomes in the IS Privacy Literature

Emergent Research Forum Paper

Tawfiq Alashoor
Georgia State University
talashoor1@gsu.edu

Lisa Schurer Lambert
Georgia State University
lisalambert@gsu.edu

Samira Farivar
McMaster University
farivas@mcmaster.edu

Abstract

For twenty years, Information Systems (IS) researchers investigated privacy attitudes and disclosure outcomes, yet a full understanding of the privacy disclosure relationship has not been reached. In the current study, we argue that the lack of consensus regarding the privacy-disclosure relationship may stem, at least in part, from methodological shortcomings. We contend that variations in disclosure measurement practices may be responsible for ambiguous findings in the accumulated IS privacy research. We provide a preliminary review of the IS privacy literature from which we aim to build an initial foundation for recommendations regarding measures of disclosure outcomes. We identify four widely used measures of disclosure outcomes (i.e. intentional, breadth of, retrospective self-reports of, and actual disclosure) and discuss their methodological concerns. We conclude with a brief discussion on the methodology for the full review and recommendation for future research.

Keywords

Privacy concerns, disclosure, behavioral outcomes, measurements, IS privacy.

Introduction

For twenty years, Information Systems (IS) researchers have examined the impact of privacy concerns on behavioral outcomes, with the most visible outcome being users’ willingness to disclose and/or transact (for review see Bélanger and Crossler 2011; Li 2011; Smith et al. 2011). Clearly, disclosure outcomes constitute the most critical effect of privacy concerns, as privacy concerns have been widely attributed to minimal disclosure, refusal to disclose, and falsification of information (Smith et al., 2011). This body of research is useful to inform Information and Communication Technologies (ICTs) service providers, policy makers, and governments on how to alleviate privacy concerns, in an effort to remove practical and ethical impediments to progress in an era of “big data.”

Despite the accumulated research examining the effect of privacy concerns on disclosure outcomes, Bélanger and Crossler (2011), in a critical analysis of the IS privacy literature, revealed that future research is still needed to fully understand the privacy-disclosure relationship. Two issues appear critical, the privacy paradox and the apparent lack of consensus in findings on the privacy-disclosure relationship. First, prominent studies have shown paradoxical results in that users express high concerns about privacy which leads them to be wary about disclosing personal information but at the same time users behave contrary to their reported responses in real settings (Bélanger & Crossler 2011; Smith et al. 2011). Second, the strength of the relationship between privacy concerns and disclosure outcomes has varied widely. Accordingly, results from this research have been less informative than they might be.

In the current study, we argue that the lack of consensus regarding the privacy-disclosure relationship may stem, at least in part, from methodological shortcomings. Measures of disclosure outcomes vary
widely in the current IS privacy literature with diverse definitions and operationalizations. There is often little evidence of construct validity or evidence that these diverse measures of disclosure across studies actually correspond to each other. A lack of construct validity threatens substantive conclusions from a study and a lack of correspondence in measurement across studies means that their findings cannot be accumulated as generalizable knowledge (Edwards 2003; DeVellis 2003; Mackenzie et al. 2011). We contend that these variations in measurement practices may be responsible for ambiguous findings in the accumulated IS privacy research. Without establishing measures with adequate construct validity we cannot tell if the variations of the effect size of the privacy-disclosure relationship vary because of true variation in relationship, or are due to inconsistent or poor measurement practices (Cohen et al. 2003).

We concur with researchers who have attributed inconsistent findings to the privacy paradox phenomenon (Bélanger & Crossler 2011; Smith et al. 2011). But, we also argue that a thorough review of the psychometric properties of disclosure outcomes has potential to advance future IS privacy research beyond the privacy paradox. Accordingly, we will investigate the current state of disclosure outcomes in the IS privacy literature from which we aim to build an initial foundation for recommendations regarding measures of disclosure outcomes. While privacy attitudes and disclosure outcomes have been studied in other disciplines, we will utilize prominent studies from those disciplines for informing our recommendations. In a nutshell, the purpose of this study is to thoroughly assess measures of disclosure outcomes in the IS privacy literature while providing recommendations for future researchers.

**Disclosure Outcomes and Information Privacy Concerns**

The ubiquity of ICTs use resulted in a massive volume of personal information disclosed within and across different ICTs. Privacy researchers, in particular, have been highly interested in studying the drivers and barriers of disclosure outcomes that represent the most relevant outcome to practice. Disclosed information is invaluable to practitioners who may exploit disclosed information via advanced analytic tools to create strategic advantage, adapt business models, and target ads (Schmarzo 2013). Accordingly, the construct of disclosure outcomes is typically treated as an outcome variable affected by privacy concerns and other variables (e.g., perceived risk, perceived benefits, and trust) in most variance research models in the IS privacy literature (Smith et al. 2011). For instance, users who have high trust in and perceive high benefits and low risks of using a certain ICT are more willing to share personal information. It is important to note that, however, at the conceptual level, IS privacy studies used different terms to explicitly or implicitly refer to disclosure outcomes, e.g., behavioral outcomes, behavioral reactions, behavioral intentions, or self-disclosure each of which may be measured in multiple ways (c.f. Krasnova et al. 2010; Malhotra et al. 2004; Smith et al. 2011; Stewart and Segars 2002). In this study, we refer to any type of disclosure, explicit or implicit intentions or behaviors, as disclosure outcomes. Information privacy concerns refer to individuals’ general tendency to worry about how their personal information is collected, used, protected, and shared by companies (Li et al. 2011; Smith et al. 1996). Prominent studies have shown that privacy concerns, in multiple contexts, may lead to minimal disclosure, refusal to disclose, and falsification of disclosed information (Dinev and Hart 2006; Jiang et al. 2013; Li et al. 2011; Smith et al. 1996) yet other studies find that this effect is contingent on other factors (Chen 2013). We suggest that it is necessary to rule out measurement problems first before accepting findings.

**Preliminary Review of Groundbreaking IS Privacy-Disclosure Research**

Our initial review of prominent studies in IS privacy research suggests several methodological concerns with their measures. First, self-reports of intentions are problematic because they are inconsistently related to actual behaviors (Ajzen 1991). This has been widely recognized as one main source of the privacy paradox where individuals’ self-reports do not match their actual behaviors (Bélanger and Crossler 2011; Smith et al. 2011). Second, some items exhibit the fallacy of confounding the independent and dependent variables violating basic principles of scale design (DeVellis 2003). For example, one item, used in two prominent studies, includes both disclosure intentions (i.e. “refuse to give information”) and privacy-related cause (i.e. “because you think it is too personal”). Third, exposing participants to privacy concerns questions before asking them to report their willingness to disclose might have primed privacy concerns in the participants’ cognitive minds as they completed disclosure items (Harrison et al. 1996). Subjects induced to think about the privacy of their information were more likely to think prudently about
disclosure of personal information (Baek 2014). We suggest the ordering of the items may artificially inflate the privacy-disclosure relationship. Fourth, disclosure intentions questions were bounded by time, specifically three years. Construal-level theory suggests that distant future activities, compared with near future plans, are based on the desirability of the planned activity (e.g., protecting one’s privacy) rather than on time constraints (Trope and Liberman 2010). In other words, participants responses might differ depending on the time frame specified in the disclosure outcomes questions. Fifth, the evidence presented regarding the relationship between the items and the construct, i.e. construct validity, was incomplete. For instance, Smith et al. (1996) reported only the Cronbach’s alpha for disclosure outcomes, Stewart and Segars (2002) reported loadings for behavioral intentions but only in the context of the structural SEM model not for the CFA. These studies may have employed standards current for the time but there may be measurement error which can bias estimates of the privacy-disclosure relationship (Cohen et al. 2003).

**Preliminary Review of Past and Current IS Privacy Research**

Despite the tremendous impact of groundbreaking IS privacy studies, our preliminary review suggests there is abundant reason to be concerned about measurement issues in more recent research. We now proceed by discussing general observations of a number of studies published in premier and top-tier IS journals. Note that the objectives of the following studies were to examine the effect of privacy concerns on disclosure outcomes. Some studies also examined determinants of privacy concerns, but this is not of our interest in the current review. We observed four different measures of disclosure outcomes, each of which suffers from some limitations.

The first and most frequently used measure is intentional disclosure (e.g., Awad and Krishnan 2006; Bansal et al. 2016; Dinev and Hart 2006; Li et al. 2011; Li 2014; Sharma and Crossler 2014; Son and Kim 2008). Although intentions have long been used to assess the likelihood of related behavior, the relationship is far from perfect with other variables influencing the likelihood of intentions being converted to behavior (Ajzen 1991). An indication that this relationship between intentions and behavior should not be assumed is recognized in the privacy paradox. The second most used measure is the breadth of disclosure (Chen and Sharma 2015; Chen 2013; Krasnova et al. 2010, 2012; Yu et al. 2015). Breadth of disclosure refers to “the amount of disclosed information, which is a function of the frequency and duration of the disclosure” (Krasnova et al. 2010, p. 111). This type of measure may be influenced by a variety of cognitive biases (Bazerman and Moore 2013; Tversky and Kahneman 1974). Individuals may be highly susceptible to the availability bias, in that the vividness of information at the time of filling out the survey is likely to influence their intentions. For instance, a participant who has been very active in using Facebook only a few days before the survey is more likely to score high in the breadth of disclosure scale, even though this participant might have been an inactive user for several months. As a result, the availability bias would increase the measurement error in this scale which will ultimately bias the effect size of the privacy-disclosure relationship (Tversky and Kahneman 1974).

The third and fourth types of measures are variations of retrospective self-reports of past disclosure behavior (Jiang et al. 2013) and actual disclosure behavior (e.g. during the study itself) (Hui et al. 2007). Biases associated with retrospective self-report measures are well known and likely to apply to reports of disclosure (Ployhart and Vandenberg 2010). Respondents’ reports tend to present a more coherent narrative than what actually occurred because memories are constructed for future use rather than to maintain an objective record of events and behavior (Schacter et al. 1998). In contrast, measuring reports of actual disclosure behaviors might appear to be the most reliable approach but is not without bias. Respondents must not only be able to retrieve accurate information but these accounts may be biased by the distinctiveness of the information requested, its importance and emotional valence, and how much time they devote to recalling information (Tourangeau et al. 2000). Respondents’ reports of their own disclosure behaviors may be inaccurate given the prevalence of ICTs usage and that disclosure decisions may be made hastily as they focus on completing other tasks and objectives. Moreover, this measure is usually treated as a count variable but the unidimensionality and exchangeability of the disclosure scale should not be assumed (e.g., Hui et al. 2007). It is problematic to treat the disclosure scale as a count variable without testing for orthogonal sub-dimensions and the different weights each item contributes to the scale. This leads to oversimplification of the actual structure of the disclosure measure, because it has been shown that some items are more strongly related to privacy concerns than others (Knijnenburg et al. 2013). An additional concern with disclosure measures in all studies is that the extent to which studies
show content, construct, and criterion validity is less than ideal in this literature. For example, statistical evidence of construct validity varies considerably and is absent for some articles.

Methodology for Full Review, Discussion, and Conclusion

We will extract all studies that tested the relationship between a privacy-related and disclosure-related construct in all IS journals published between 1996 and 2016. We anticipate that coding categories will emerge, but currently expect that articles will be coded on the following multiple dimensions. Studies will be coded based on (1) the type of disclosure outcome: intentional, breadth of, retrospective, and actual disclosure; (2) correspondence between the theoretical definition of disclosure behavior and its operationalization, i.e. content validity; (3) statistical evidence pertaining to construct validity, e.g. Cronbach’s alpha, CFA results, and evidence reported regarding criterion validity; (4) the effect size of the privacy-disclosure relationship; and (5) the correspondence between the theoretical definition of disclosure outcomes with the theoretical reasoning and the study conclusions. This coding procedure will provide the basis for an assessment of the current state of the measures of disclosure outcomes. More importantly, we will provide a list of recommendations on ways to adhere to best practices regarding measurement development, use, and reporting.

In this research-in-progress, we emphasize a critical methodological issue in the IS privacy literature - that measures of disclosure outcomes may be problematic and hindering efforts to accumulate knowledge about the privacy-disclosure relationship. An implication of the issues discussed in our preliminary review may be that even a meta-analytic review of this literature might not be able to make a definite conclusion about the true effect of privacy concerns on disclosure outcomes because of error introduced by flawed measurement. Several researchers have already recommended future research to measure actual behaviors instead of intentions (Bélanger and Crossler 2011; Smith et al. 2011). Nevertheless, our preliminary review shows that recent studies still adopt intentions rather than actual disclosure. Prior to the full review that we plan to conduct, we recommend researchers using disclosure outcomes devote due attention to content, construct and criterion validity.

REFERENCES

A Review of Measures of Disclosure Outcomes


