Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2015 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2015

Why We Don't Block 3rd Party Trackers: An Attributional Theory Perspective

Frank Goethals
IESEG School of Management (LEM-CNRS)

Shamel Addas
IESEG School of Management (LEM-CNRS)

Why We Don't Block 3rd Party Trackers: An Attributional Theory Perspective

Research in Progress

Frank Goethals
IESEG School of Management (LEM-CNRS), France {f.goethals@ieseg.fr}

Shamel Addas
IESEG School of Management (LEM-CNRS), France {s.addas@ieseg.fr}

ABSTRACT

Research on online consumer privacy typically relies on the trust-risk framework to explain users' reactions to perceived privacy threats. However, little is known about such reactions in the context of third party tracking, where there is no explicitly defined agent to be trusted. In this research-in-progress, we propose an that in these situations users rely to the their attributional styles to shape their future actions. We present a model that predicts behavioral intentions based on traditional protection motivation theory and complements it with the construct of attributional style.

Keywords: attribution theory, attributional style, protection motivation theory, information privacy

INTRODUCTION

Information privacy, which refers to individuals' desire to control how their personal information is acquired and used (Culnan and Bies 2003), has become a prime concern in the digital age (Smith et al. 2011). A substantial amount of research has been dedicated to examining the impacts of privacy-related aspects on individuals' behavioral intentions and actual behaviors. Most information privacy impact studies have specified the boundaries of that phenomenon as involving the individual (first-party) who directly transacts with the vendor or service provider (second-party). Typically, the individual intentionally visits the site(s) of the vendor and discloses one's personal information to the vendor who collects and

compiles such information, and converts it to personalized product- or service offerings (Conger et al. 2013; Liang and Xue 2009). Within that two-party context, researchers have relied heavily on the trust-risk framework to explain information privacy impacts (Pavlou and Gefen 2005; Xu et al. 2005).

With the advent of Big Data, however, the traditional two-party context is extended to third party entities (e.g., aggregators; data analytics companies) that assume a key role by manipulating personal data collection and use (Najjar and Kettinger 2013). In particular, these third party entities are increasingly tracking users' behaviors across sites such as to build a profile of their interests, activities, and even their identities (Krishnamurthy and Wills 2009). For example, third-party advertisers such as Google's DoubleClick use third-party cookies to track users across thousands of websites on which they serve ads. Much of this third-party tracking occurs in a way that is covert to users (Conger et al. 2013; Culnan and Bies 2003). Still, there are free browser plugins available (such as Ghostery for Chrome and Lightbeam for Firefox) that enable people to see what websites are tracking them and to block those trackers. In preliminary discussions we conducted with users, we observed that when people become aware of the existence of 3rd party trackers and the tools that can be used to block them, most don't actually block the trackers. This is despite the fact that many express strong concerns about their online privacy. Thus, in line with research examining the privacy paradox, we ask the following question: what are the factors that influence individuals' privacy-related behavioral intentions regarding third-party behavioral tracking?

Contrary to previous research that focuses on trust/risk perceptions as primary predictors of behaviors/ behavioral intentions (Culnan and Armstrong 1999; Pavlou and Gefen 2005; Xu et al. 2005), we suggest that in an uncertain online environment in which transactions are not exclusive to explicit transacting parties, individuals resort to their

attributional styles in deciding on whether or not to take actions to protect their information online (i.e. block third party trackers).

We draw upon protection motivation theory (PMT) as a theoretical base. PMT is a social cognitive theory that has been widely used in research predicting coping behavior in the presence of threatening events (e.g., Herath and Rao 2009; Ng et al. 2009; Rogers 1975). The main premise of PMT is that the presence of threatening events (third party behavioral tracking in our case) impels individuals to engage in cognitive appraisals: threat appraisal and coping appraisal (see Figure 1). These two processes together arouse the individual's protection motivation (Maddux and Rogers 1983; Rogers 1975). Because the context of third party tracking presents unique challenges, we extend the basic PMT model by adding the concept of attributional styles.

The main contribution of this research is to explain users' behavioral intentions in the context of third party tracking. The paper extends research on information privacy in traditional two-party contexts. We show that in the presence of third party trackers individuals' behavioral intentions are driven mostly by their attributional styles rather than by trust/ risk perceptions. This contribution also has practical ramifications since it explains users' reactions to third party tracking and aggregation, which is a cornerstone of the Big Data phenomenon.

THEORETICAL DEVELOPMENT

Our basic theoretical assumption is that as users engage in online activity, they face uncertainty related to their information privacy, which they try to mitigate by using cognitive mechanisms (Pavlou et al. 2007). Two such uncertainty reduction mechanisms that have received wide attention are trust (Mayer et al. 1995) and causal attributions (Weiner 1986). In both Mayer et al.'s trust-risk framework and Weiner's attribution theory, individuals reduce

uncertainty by forming expectations about the outcome of events, with these expectations guiding their future actions. However, the two frameworks differ with respect to the entity on which these expectations are anchored. Trust-risk models presuppose the presence of an explicit agent (a second party, or a transaction system) whose characteristics, prior actions, or reputation form the basis of expectations about his or her choice of actions (Dasgupta 2000). By contrast, attribution theory anchors individuals' expectations about future outcomes on the causal search and explanation associated with similar past outcomes of events (Weiner 1986). In other words, the entity that shapes the expectations is not another actor's behavior, but rather the outcome of similar past events. In this research, we turn to attribution theory to understand why people (do not) protect themselves against 3rd party trackers.

The guiding principle of causal attributions is that people seek to understand the causes of events that are important for them (Weiner 1986). Causal attributions help individuals define their expectations about future outcomes and guide their actions to avoid the unexpected or aversive outcomes (Weiner 1986). Attributional style (AS) regarding related past events provides a framework for understanding future situations. Indeed, Martinko et al. (1996) argued that when individuals experience an entirely new IT implementation (an event for which no prior experience exists), "these attributions probably take their form from a generalized attributional schemata based on what the individual interprets to be related prior experiences" (p.315). Because of the novel and covert nature of third party tracking, individuals often cannot draw on explicit actual experiences to make causal attributions. Consequently, their AS regarding related situations can form the basis of their expectations and behavioral intentions.

An AS is a cognitive personality variable that reflects the habitual manner in which individuals explain or evaluate the causes of positive and negative events that happen to them (Seligman et al., 1984). It consists of three dimensions: internality versus externality, stability

versus instability, and globality versus specificity. The first dimension distinguishes whether the causes of events originate from within the individual or from external, situational factors. The second dimension differentiates between long lasting versus transient causes. The third dimension distinguishes between causes that occur across situations from those that ate more unique to the situation. Together, the three dimensions can differentiate between individuals whose ASs are more optimistic or pessimistic (Seligman et al. 1984). An individual with an optimistic style will attribute positive events to internal, stable, and global factors, and will attribute negative events to external, unstable, and specific factors. An individual with a pessimistic style will exhibit the reverse pattern. Still, these two patterns of styles represent ends of a continuum rather than two separate entities (Peterson and Seligman 1984). The AS can be measured using the Attributional Style Questionnaire (Peterson and Seligman 1984).

RESEARCH MODEL AND PROPOSED METHOD

The research model (see Figure *1*) shows that AS will influence behavioral intentions directly and indirectly through the threat and coping appraisals. Space limitations make it impossible to discuss here how the hypotheses are grounded in literature. Hypotheses 7-12 are based in the PMT; hypotheses 1-6 relate to the impact of one's AS on the PMT constructs and the final dependent variable. The model in Figure 1 will be tested using a large-scale survey.

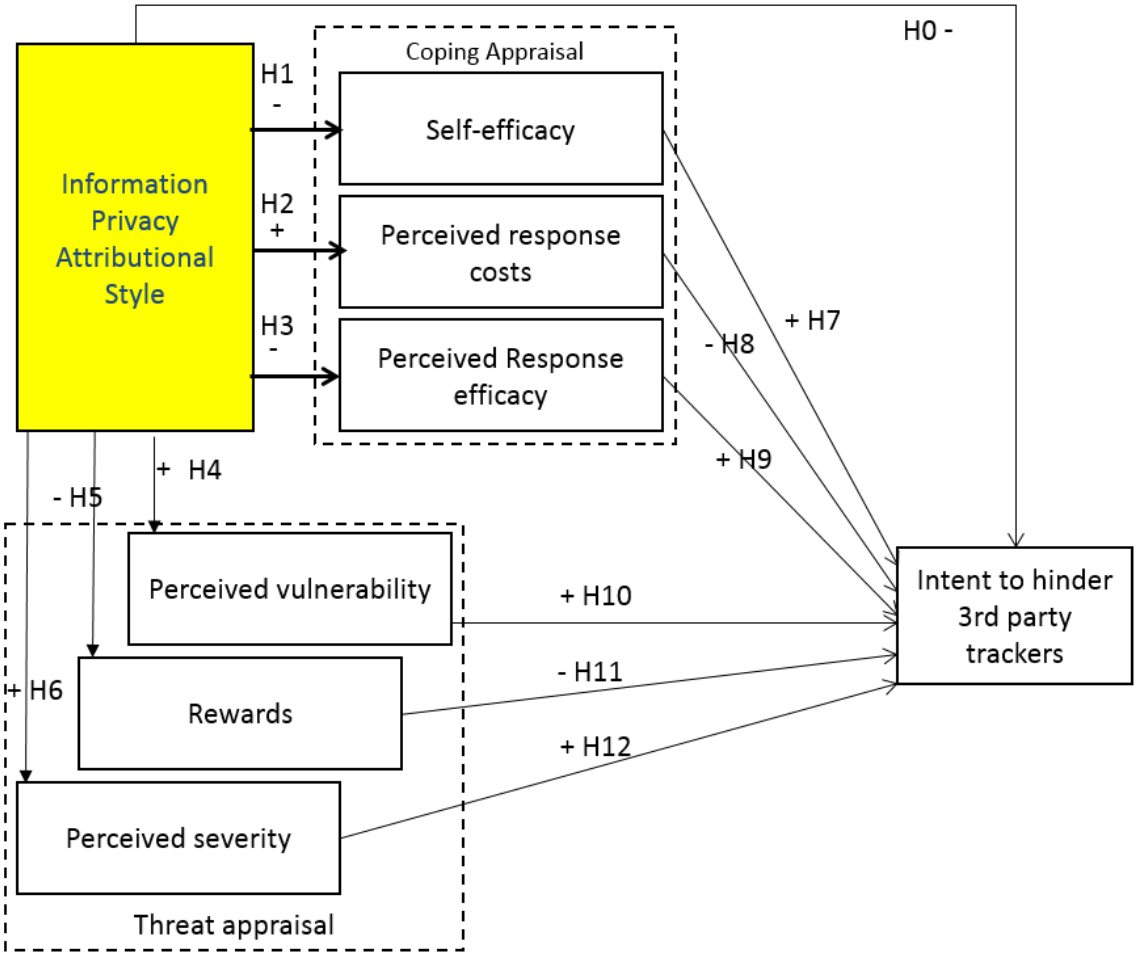

Figure 1: Research Model

Following recommendations to develop domain-specific AS constructs and measures (Curtona et al. 1984; Ashford & Fugate 2006), the AS shown in the model is specific to the domain of online information privacy. We will first develop and test an Information Privacy AS (IPAS) questionnaire, in line with previous ASQs. Simply stated, a person's IPAS shows whether a person is rather optimistic or pessimistic with respect to information privacy. If people are pessimistic about the control they have over their information (e.g., because they believe that companies can always get access to their data anyway), their intent to block 3rd party trackers is expected to be lower.

Survey respondents will first be asked questions concerning their AS. Only after that will they be shown a vignette that describes 3rd party tracking. They will subsequently be asked about their threat and coping appraisals with respect to 3rd party trackers. As

respondents will not know about 3rd party trackers before (this will be measured separately in the survey), their knowledge about 3rd party trackers could not have impacted their scores on the AS questions. This implies that the arrows for hypotheses 1 through 6 cannot go in the opposite direction in this research design.

Wherever possible, measures will be adapted from prior research. Threat appraisal measures (perceived vulnerability; perceived severity; rewards) will be adapted from Liang & Xue (2010) and Xu et al. (2009). Measures for coping appraisal (self-efficacy; response costs; response efficacy) will be adapted from Liang & Xue (2010). Behavioral intentions will be measured using a scale adapted from Dinev & Hart (2006). The survey instrument will be preliminarily validated using card-sorting analysis, pretesting, and pilot testing (Moore & Benbasat 1991).

CONCLUSION

This research-in-progress tackles an important and timely phenomenon. By expanding our understanding of privacy-related behavioral intentions in the context of third-party tracking, we add to the literature on online privacy, while shedding light on the privacy paradox. This research also provides a complementary perspective for explaining behavioral intentions. Rather than focusing on users' trust/risk perceptions, we posit that in the context of third party tracking, attributional style becomes a relevant predictor. This research-in-progress can have both theoretical and practical implications (e.g., using strategies to manipulate attribution style such as immunization or attributional training).

REFERENCES

Conger, S., Pratt, J. H., and Loch, K. D. 2013. "Personal Information Privacy and Emerging Technologies," *Information Systems Journal* (23:5), pp. 401-417.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323-342.

Dasgupta, P. 2000. "Trust as a Commodity," in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta (ed.). Department of Sociology, University of Oxford, pp. 49-72.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Krishnamurthy, B., and Wills, C. E. 2009. "On the Leakage of Personally Identifiable Information Via Online Social Networks," ACM, pp. 7-12.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71-90.

Maddux, J. E., and Rogers, R. W. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19:5), pp. 469-479.

Martinko, M. J. 1996. "An Attributional Explanation of Individual Resistance to the Introduction of Information Technologies in the Workplace," *Behaviour & Information Technology* (15:5), pp. 313-330.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *The Academy of Management Review* (20:3), pp. 709-734.

Najjar, M. S., and Kettinger, W. J. 2013. "Data Monetization: Lessons from a Retailer's Journey," *MIS Quarterly Executive* (12:4), pp. 213-225.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.

Pavlou, P. A., and Gefen, D. 2005. "Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role," *Information Systems Research* (16:4), pp. 372-399.

Pavlou, P. A., Huigang, L., and Yajiong, X. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105-136.

Peterson, C., and Seligman, M. E. 1984. "Causal Explanations as a Risk Factor for Depression: Theory and Evidence," *Psychological Review* (91:3), pp. 347-374.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), p. 93.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1016.

Weiner, B. 1986. "Attribution, Emotion, and Action," in *Handbook of Motivation and Cognition: Foundations of Social Behavior*, R.M. Sorrentino and E.T. Higgins (eds.). Guilford Press, pp. 281-314.

Xu, H., Teo, H.-H., and Tan, B. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk."