Lurking and Information Sharing on E-Commerce Sites

Babajide Osatuyi
The University of Texas Rio Grande Valley, USA

1. INTRODUCTION

Lurking on online groups is a topic that is of interest to Internet researchers and organizations. Lurking refers to the act of joining an online community with the intention to consume information available within the community and not necessarily contribute information to the community (Bishop, 2007; Dennen, 2008). It is reported that about 90% of users on user-generated content sites like social media are lurkers (Suster, 2010). Several perspectives have been provided to explain users’ tendency to lurk on online groups. With increased incorporation of social media capabilities on enterprise web platforms, organizations are particularly interested in how to engage lurkers on their web platforms. Moreover, studies show that users, lawmakers, and organizations are increasingly concerned about how their personal information is collected, stored, and shared on social media sites (Xu & Bélanger, 2013). However, no study has examined the relationship between privacy concerns and lurking. This study therefore contributes to the literature as it seeks to empirically investigate the role of lurking as it relates to privacy concerns on social media platforms. Given the large populations of lurkers on online communities, organizations are interested in how to gather useful information about them and to eventually convert them to customers (Suster, 2010). As such, this article also explores the relationship between lurking, users’ concern for information privacy, and their future intentions to provide their personal information during online transactions.

This study hypothesizes that given that social media sites require the voluntary provision of personal information in order to become a member and coupled with the aggressive collection, storage, and sharing of personal information on social media sites, it is plausible to expect users to be cautious on how they share information on those sites. This study uses social penetration theory as a theoretical framework to explore these hypotheses.

The rest of the article is organized as follows. Section 2 presents the research approach taken in this study followed by the presentation of the study variables used to develop the research hypotheses and model. Section 3 describes the methodology used to conduct the study and the data analysis and results are presented in Section 4. Section 5 discusses the findings from this study and their implications.

2. THEORETICAL BACKGROUND AND RESEARCH MODEL

The research approach taken in this study is in the exploratory region for two reasons: 1) information privacy research on social media is in its infancy, and 2) there is no known study that has established a relationship between lurking and concern form information privacy in the social media context. This region is described by Stebbins (2010) as the region of little known phenomena. Research in this region typically combines the report of descriptive statistics and generation of relationships between concepts.
Lurking and Information Sharing on E-Commerce Sites

Figure 1. The research model

2.1 Concern for Information Privacy (CFIP)

Several studies have explored concern for information privacy in the Information Systems (IS) field. Although a variety of models were developed to assess consumers’ concern for information privacy, the seminal study conducted by Smith et al., (1996) provided empirical support for the dimensionality of the CFIP measurement instrument. The instrument includes four dimensions for measuring CFIP as collection, unauthorized secondary use (internal and external), unauthorized access, and errors. Collection describes an individual’s perception of the amount of information being captured via organizational practices. Internal unauthorized secondary use describes the use of personal data collected by an organization for a legitimate reason (e.g., shipping information provided to an online merchant during checkout), but used for a secondary purpose without the consent of the user. External unauthorized use refers to the use of personal information captured from a legitimate transaction by a third party without the consent of either the user or the organization. Unauthorized access refers to concern that data about individuals are readily available to people authorized to view or work with this data. Errors describe the inaccurate storage or representation of the data collected by an organization.

In an attempt to improve the psychometric property of the CFIP measurement instrument, Stewart and Segars (2002) empirically validated it as a multi-dimensional construct. They also found that when mea-