User Privacy Concerns for E-Commerce

Kim-Phuong L. Vu
California State University – Long Beach, USA

Robert W. Proctor
Purdue University, USA

INTRODUCTION

The goal of this encyclopedia entry is to review research relating to privacy for E-commerce, discuss issues of consequence, and provide recommendations for future research. We begin with studies surveying user privacy concerns and present research showing that users' behaviors often do not match their stated privacy concerns or preferences. Next, we present reports showing the efficacy of privacy seals and discuss studies illustrating the benefits of using software tools that alert users when Web sites violate their privacy preferences. We also point out usability issues associated with these privacy checking tools. Subsequently, we discuss issues relating to metrics for capturing user privacy preferences and comparing results across studies. We end the entry with recommendations for areas of future research.

BACKGROUND

According to the 2012 US Census data, E-commerce made up 5.2% of the total retail sales that year, amounting to $227 billion (US Census Bureau, 2012). It has been estimated that the sales will grow to a trillion dollars worldwide in 2015 (Bigcommerce, 2014). Unlike traditional, in-store purchases, where transactions can be made anonymously through cash payments, E-commerce transactions require users to enter personal information in addition to the payment. The personal information collected may include billing/shipping address, phone numbers, E-mail addresses, and credit card numbers. A concern for many online consumers is how this information will be used by the organization to which it is submitted, not only for the processing of the transactions but for other marketing and data sharing purposes. Recent security breaches of the E-commerce sites of large companies, for example, Target in 2013 and E-Bay in 2014, have increased the concern among users about the security of personally identifiable information as well. Several retailers have reported compromises of consumers' credit and debit information through unauthorized access. Moreover, the recent surge in mobile computing has allowed users the convenience of engaging in E-commerce in both private and public locations, but at the additional cost of potential privacy violations. Thus, for an organization to be successful in E-commerce, its Web site must promote privacy and security. In the next section, we review the research conducted on user trust and privacy concerns with E-commerce.

DOI: 10.4018/978-1-4666-9787-4.ch125

MAIN FOCUS OF THE ARTICLE

Individuals show various levels of privacy concerns when it comes to E-commerce. Ackerman, Cranor, and Reagle (1999) gave participants four scenarios in which they had to indicate whether they were comfortable providing various types of personal information. A majority of users were very comfortable with providing general information (e.g., favorite food) and somewhat comfortable with providing directory-type information (name, address, e-mail), but they were uncomfortable with providing financial and health information (e.g., credit card, health status). For questions relating to the users' general attitudes regarding providing personal information, Ackerman et al. concluded that users can be classified as

1. Marginally concerned,
2. Privacy fundamentalists (users who are very concerned with privacy), or
3. Pragmatic (users whose concerns vary as a function of the type of transaction being performed).

Subsequently, Berendt, Günther, and Spiekermann (2005) identified four categories of users with respect to their expressed privacy concerns. Similar to Ackerman et al. (1999), they found groups of *marginally concerned* users and *privacy fundamentalists.* Instead of a single class of pragmatic users, they distinguished between two groups: *identity concerned* (users who want to protect their personal information) and *profiling averse* (users who do not want their personal information to be used to classify and target their purchasing behaviors). Berendt et al. also measured the purchasing behavior of each of their four groups' members when interacting with an online avatar. Although, overall, the groups' disclosure of personal information when solicited by the avatar matched the general categorization of user type, the authors found that "the absolute level of disclosure was alarmingly high across all clusters, belying the previously expressed reluctance to disclose information online" (p. 104). This finding indicates that many factors ultimately influence the disclosure of personal information for E-commerce.

One factor that influences online purchases is the user's self-efficacy regarding use of the Internet. Akhter (2014) surveyed users on their privacy concerns, online usage, and purchasing behavior. He found a negative correlation between privacy concern and the number of online transactions in which a person engaged. However, Akhter also found a positive correlation of Internet self-efficacy with number of online transactions. Findings from Akhter's study suggest that when users engaged successfully in E-commerce and other Internet activities, their privacy concerns could be alleviated. These findings are consistent with the literature showing that users trust familiar sites more and are more likely to make purchases from familiar E-commerce sites (Vu, Chambers, Creekmur, Cho, & Proctor, 2010).

When making online purchases, users seldom access a Web site's privacy policy (Vu, Garcia et al., 2007). One reason why this is the case is that users typically show little understanding of the policy content because privacy policies often contain a lot of legal terms and are written at a high reading level (Proctor, Ali, & Vu, 2008). Vu, Chambers et al. (2007) tested participants' comprehension of privacy policies from e-commerce sites and found that participants showed poor comprehension of the information conveyed in the policies. To examine at what participants were looking when reading privacy policies and searching for information in them, Vu et al. recorded participants' eye-gaze data. Results showed that participants rarely read an entire privacy policy, even when they knew that they would be tested on its content, instead only scanning the policy. Participants tended to look at headings and the first few words of each paragraph to determine the content covered in each section, but they did not look at the detailed information included in the policy.