Internet Privacy Concerns versus Behavior: A Protection Motivation Approach

Kenneth J. Sousa, Department of Computer Information Systems, Bryant University, Smithfield, RI, USA

Laurie E. MacDonald, Department of Computer Information Systems, Bryant University, Smithfield, RI, USA

Kenneth T. Fougere, Department of Computer Information Systems, Bryant University, Smithfield, RI, USA

ABSTRACT

This study examines the possible disconnect between student concerns about privacy when using the Internet and their behavior. The literature indicates that Internet users are concerned about privacy but their web-browsing habits consistently put their privacy at risk. Browsing habits were examined using five factors: (1) privacy concerns, (2) self-efficacy, (3) risk assessment, (4) threat assessment, and (5) privacy involvement. These factors were analyzed for their relationship to privacy behavior. A survey questionnaire was developed and administered to a sample drawn from university students.

Keywords: Privacy, Privacy Behavior, Privacy Concerns, Privacy Involvement, Self-Efficacy, Threat Assessment

INTRODUCTION

There were over of 200 million records involved in security breaches from January 2005 through June 2008 (Anonymous, 2004). An analysis of over 500 forensic reports of security incidents revealed that while 73% of incidents were caused by external sources, but the 18% caused by insiders were far more significant (Baker, Hylendar, & Valentine, 2008). Some of the largest data breaches in the recent past that placed individual data at risk include: TJX Companies - 94 million records in 2007, AOL - 30 million records in 2004, and U.S. Department of Veterans Affairs - 26.5 million records in 2006 (Anonymous, 2008d). There was a marked increase in the number of security incidents reported by colleges and universities in 2007. The number of schools that reported security incidents increased by 72.3% and the number of incidents increased by 67.5% (Dodge, 2007). The number of Internet security incidents grew to the point where the Computer Emergency Response Team Coordination Center (CERT/CC) stopped counting them in 2004. Efforts are now concentrated on identifying vulnerabilities
and potential exploits. Most system vulnerabilities can be exploited remotely; meaning that cyber-criminals can attack databases from a distance. It takes hackers an average of six days to develop an exploit for a newly identified vulnerability. Vendors take an average of 47 days to release corrective patches (Phifer & Piscitello, 2007).

The specter of an omnipresent “Big Brother” watching our every move has been a staple since it was introduced by Orwell in his novel 1984. Government agencies, credit bureaus, and many businesses accumulate vast amounts of personally identifiable information (PII). In 1992 over two dozen arrests were made by the U.S. Department of Justice of people engaged in buying and selling information from the Social Security Administration (SSA). Investigators found that employees of the SSA had unrestricted access to more than 130 million individual records. A second investigation discovered that IRS employees browsed through tax records (Meritt, 1998). These reports give ample support to the growing concern about privacy among the general population.

**LITERATURE REVIEW**

This research study requires the foundational constructions associated with several previously published research efforts. The following sections review the literature associated with privacy, privacy concerns and privacy behavior.

**Privacy**

Privacy has been defined in different ways by different writers. Posner (1981) suggests that the word privacy may be used to indicate efforts and actions to conceal personal information. Sundstrom et al. (1980) define psychological privacy as the control of the access to personal information by others and transmission of this information. It also entails control over inputs from others and assumes that people work to maintain some optimal level of social contact. In this construct people do not require or desire absolute privacy which would result in little or no meaningful social contact. Optimal social contact is a balance between hiding and revealing PII. Personal privacy has been defined as the state of not having others in unauthorized possession of one’s PII. The degree to which others gain unauthorized access to one’s PII is a measure of the diminishment of personal privacy (Parent, 1983). Individuals rely on the notion that there is some area of private data. That is, there exists the right to keep others from accessing our personal information (Curry, 1997). Information privacy has been defined as the ability to exercise control over one’s personal information (Smith et al., 1996).

The U.S. Supreme Court has used privacy as a synonym for freedom and personal autonomy (Posner, 1981). It is generally accepted that the origin of a right to privacy lies with an 1890 paper by Samuel Warren and future Supreme Court justice Louis D. Brandeis. The article argued for the right to be left alone (Danielson, 1999). The right to privacy is the ability to restrict what personal information that is publicly available. Privacy serves important social functions and is essential to the individual’s personal development and contentment (Curry, 1997). Schwartz (1968) argued that a stable social system requires that privacy must be guaranteed by rules that govern the collection and revelation of personal information. This argument can be seen as generally accepted given the laws and regulations present in all modern societies that govern information (Whitman & Mattord, 2008).

The concept of an Infosphere, as the realm of all types of information is analogous to the Biosphere that supports life, has been introduced by Floridi (2005). The infosphere includes cyberspace as well as off-line and analogue sources of information. Using the infosphere to model information interactions, private information exists based on an information gap between agents in the infosphere. The scope of the information gap is a function of the accessibility of PII. The lower the degree of accessibility the larger the information gap and thus privacy is increased. Floridi suggests that privacy be interpreted by assuming a per-
10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:
www.igi-global.com/article/internet-privacy-concerns-versus-behavior/72333?camid=4v1

This title is available in InfoSci-Journals, InfoSci-Journal Disciplines Communications and Social Science, InfoSci-Select, InfoSci-Select, InfoSci-Technology Adoption, Ethics, and Human Computer Interaction eJournal Collection. Recommend this product to your librarian:
www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

The Civilization Grand Model
Andrew Targowski (2009). Information Technology and Societal Development (pp. 1-44).
www.igi-global.com/chapter/civilization-grand-model/23585?camid=4v1a

Strengthening and Enriching Audit Practice: The Socio-Technical Relevance of “Decision Leaders”
www.igi-global.com/article/strengthening-enriching-audit-practice/54073?camid=4v1a

The Good, the Bad, and the Missing of the “Diffusion of Innovations” Theory: A Commentary Essay
Francisco Chia Cua (2012). International Journal of Information Systems and Social Change (pp. 64-80).
www.igi-global.com/article/good-bad-missing-diffusion-innovations/68980?camid=4v1a
From Learning Management Systems to a Social Learning Environment: A Comparative Review and the Implications
www.igi-global.com/article/from-learning-management-systems-to-a-social-learning-environment/218222?camid=4v1a