Chapter 1
Examining an Individual's Perceived Need for Privacy and Security:
Construct and Scale Development

Taner Pirim
Mississippi Center for Supercomputing Research, USA

Tabitha James
Virginia Polytechnic Institute, USA

Katherine Boswell
University of Louisiana – Monroe, USA

Brian Reithel
University of Mississippi, USA

Reza Barkhi
Virginia Polytechnic Institute, USA

ABSTRACT

Security and privacy issues have risen in importance as the use of technology increases. Newly developed technological devices for asset security can only be successful if people are willing to use them. Gaining an understanding of individuals' acceptance and possible use of new security technologies would be beneficial to entities that are developing, marketing, and implementing new security technologies. This study develops an instrument to determine an individual's need for security and privacy and investigates the relationship between these two constructs. The results show that the instrument developed is reliable and that a significant relationship exists between the two constructs.

DOI: 10.4018/978-1-61692-000-5.ch001

INTRODUCTION

Privacy refers to the ability of an individual to "control the terms under which personal information is acquired and used" (Henderson & Snyder, 1999; Westin, 1967). A certain expectation of an individual's right to privacy has always been present; however, there is some disagreement as to what this expectation should be (Milberg et al., 2000). Privacy concerns have garnered much attention in recent years with the rise in identity fraud and the new capabilities to collect and process information brought about by technology. In 2008 alone there were 313,982 cases of identity theft reported to the FTC, an increase of over 50,000 from 2007 (FTC, 2009). Considering that only 31,140 cases were reported in 2000, a definite upward trend can be seen in the number of identity theft cases. In fact, the identity theft category was the largest subset of fraud complaints reported to the FTC, at 26% of the total (FTC, 2009). The public concern over this threat is evident in the report by the FTC to the Ways and Means Committee of the U.S. House of Representatives in March, 2006. This report stated that the commission is contacted between 15,000 and 20,000 times per week by individuals requesting information about identity theft avoidance practices. The Consumer Sentinel Network, which is the national repository for identity theft and consumer fraud, now contains over 7.2 million complaints (FTC, 2009).

One major reason for the rise of identity fraud is that increases in Internet transactions make the authentication of persons more difficult than ever before, since there is no human contact and less opportunity for identification checks. Hence, methods for identification and verification in e-commerce environments are becoming increasingly necessary to avoid potential issues such as identity fraud. Online banking, electronic financial transactions, online data stores, and Internet commerce, for example, are becoming extremely popular. The technologies to prevent misuse of these systems continue to expand as their importance increases and the potential for financial loss grows.

With advances in technology, companies have ever-increasing abilities to collect and analyze data to make assumptions about consumer behaviors. Increasing concerns about the misuse of such data, or the use of this information in a way not intended by the individual, have pushed privacy issues to the forefront of social consciousness.

Government regulations to control the collection and use of information illustrate the growing importance of privacy to individuals. Opt-out policies for secondary use of information from credit card companies, for example, now give individuals in the United States more control over who has access to their personal information. The use of information to derive valuable insights about individuals has become an increasingly important issue due to increased capabilities in collecting, processing and joining information by corporations and government entities. This information once collected can provide companies and government agencies with data that can be used for financial gain (Mason, 1986). These increased capabilities to collect and process data create an ethical dilemma in terms of financial profitability versus an individual's right to privacy (Mason, 1986).

Security as defined by the dictionary refers to "freedom from danger" or "freedom from fear or anxiety" (http://www.m-w.com/cgi-bin/dictionary). The importance of security has been highlighted in recent years due to uncertainties in world events as well as the ever-growing threat of vulnerabilities in systems crucial to normal operation of many functions of society. Physical security has always been a concern that individuals have placed importance upon. Recent events and rises in crime have compounded this concern as individuals are now more aware of threats to their physical safety in public areas such as airports, planes, sporting events, and their places of