Available online at www.sciencedirect.com

ScienceDirect

Journal of Strategic Information Systems 17 (2008) 214–233

Strategic Information Systems

www.elsevier.com/locate/jsis

Internet privacy concerns and beliefs about government surveillance – An empirical investigation

Tamara Dinev [a,*], Paul Hart [a], Michael R. Mullen [b]

[a] *Department of Information Technology and Operations Management, Barry Kaye College of Business, Florida Atlantic University, Boca Raton, FL 33431, USA*

[b] *Department of Marketing, Barry Kaye College of Business, Florida Atlantic University, Boca Raton, FL 33431, USA*

Received 16 January 2006; accepted 11 September 2007
Available online 19 November 2007

Abstract

This U.S.-based research attempts to understand the relationships between users' perceptions about Internet privacy concerns, the need for government surveillance, government intrusion concerns, and the willingness to disclose personal information required to complete online transactions. We test a theoretical model based on a privacy calculus framework and Asymmetric Information Theory using data collected from 422 respondents. Using LISREL, we found that privacy concerns have an important influence on the willingness to disclose personal information required to transact online. The perceived need for government surveillance was negatively related to privacy concerns and positively related to willingness to disclose personal information. On the other hand, concerns about government intrusion were positively related to privacy concerns. The theoretical framework of our study can be applied across other countries.

Keywords: E-commerce; Privacy; Government; Surveillance; LISREL

1. Introduction

Sociologists have argued that the current American society is a surveillance society (Lyon, 2001; Norris and Armstrong, 1999; Stadler, 2002). Surveillance refers to any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered (Lyon, 2001, p. 2). Both private corporations and government agencies take advantage of the increasing technical capability of information systems to collect and process consumer and citizen data. They use this vast amount of data to build profiles to acquire knowledge about consumer preferences for commercial purposes and citizen behaviors to detect and prevent security breaches, fraud and other crimes, and terrorist activities.

This study focuses on Internet users' responses to government initiatives intended to address the above mentioned threats to society. The international diffusion of the Internet has provided many social benefits

[*] Corresponding author. Tel.: +1 561 297 3181.
E-mail addresses: tdinev@fau.edu (T. Dinev), hart@fau.edu (P. Hart), mullen@fau.edu (M.R. Mullen).

0963-8687/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.jsis.2007.09.002

but at the same time the Internet provides an online venue for opportunistic and malicious activity. Thus, numerous sources of crime and security threats have emerged online. The possibility of terrorist threats led Clarke (2001) to warn of the dangers of digital sabotage intended to disrupt and damage the economy. Professional and organized cybercrime targeting financial institutions and the e-commerce infrastructure grew 35 times over during the last 4 years (Grow, 2005). Cybercrime (i.e., virus attacks, network break-ins, online scams) has been identified as the U.S. Federal Bureau of Investigation's (FBI) third highest priority, after counter-terrorism and counter-intelligence (Grow, 2005). The FBI's cybercrime strategy created in 2002 includes extensive Internet surveillance and intelligence gathering at both vendor and online service provider levels (Grow, 2005). Clearly, there has been less public tolerance for security compromises and crimes since September 11th(Kary, 2002). Thus, the nature and the seriousness of the security threats would seem to make surveillance a welcome and justifiable practice and the subjects – voluntary participants (Lyon, 2001).

However, at the same time, American legal precedent and public opinion reflect a society in which privacy is highly valued (Laufer and Wolfe, 1977; Rosen, 2001). Americans view privacy as an expression and safeguard of personal dignity (Cohen, 2000; Swire, 1999, 2003). Privacy is among the highest of individual rights (Etzioni, 1999; Westin, 1967, 2001). When asked what Americans feared the most in the upcoming century, a 1999 Wall Street Journal poll found that 29% of the respondents ranked erosion of personal privacy first among a list of more frightening concerns including world war, global warming, and international terrorism, none of which was ranked first by more than 23% of the respondents (Harvey, 1999). In Congressional testimony to the House Subcommittee on Commerce, Trade, and Consumer Protection, Westin (2001) summarized the results of a series of polls conducted in collaboration with Louis Harris and Associates and Equifax throughout the 1990s. In one poll, 79% of the respondents believed that if the Framers of the Declaration of Independence were rewriting that document today, they would add privacy to the trinity of life, liberty, and pursuit of happiness (p.11). In another, a majority ranked privacy just behind freedom of speech and ahead of freedom of religion and the right to vote as the most important American right (p. 11). And in still another poll, 94% said they are worried about the potential misuse of their personal information, with 77% of those responding that they are very concerned (p. 11). The unmistakable belief in the right to privacy in American culture makes a recent observation by Rosen (2001) poignant and timely: in comparing British and American societies, Britain has embraced new surveillance technologies more readily, while America has strenuously resisted them.

Chapman (2000) observed that public concerns about privacy tend to exhibit cyclical patterns. Each cycle, of roughly 10 years, is triggered by events that catalyze public fears about losing privacy. At the beginning of each cycle, the erosion of privacy has been substantially consolidated and extended in depth and breadth as compared to the end of the previous cycle. The rapid development and prolific use of digital and Internet technologies and their capability for improving surveillance techniques explain the recent beginning of such a cycle of growing privacy concerns (Clarke, 1988; Marx, 2003). In commenting on this cycle over recent years, a number of social scientists have noted that greater privacy threats have been attributed to the private sector rather than the Orwellean prediction that placed big brother in the realm of the public sector (Laudon, 1997; Varian, 1997). This phenomenon has been referred to as the privacy paradox (Etzioni, 1999). Thus, the private sector, rather than the public sector, has been attributed with making consumers, as distinct from citizens, vulnerable (Marx, 2003; Noam, 1997).

The U.S. government has made some effort in the past to regulate to a certain extent the protection of personal information in the private sector, especially regarding health care. The Health Insurance Portability and Accountability Act (HIPAA) enacted by the U.S. Congress in 1996 contains the Privacy Rule establishing regulations for the use and disclosure of protected personal health information. Another notable effort in that direction is the Electronic Freedom of Information Act (FOIA) Amendments of 1996 that expand the scope of the original FOIA of 1966 to encompass electronic records and require the creation of electronic reading rooms to make federal agencies' records more easily and widely available to the public. The incorporated Privacy Act (PA) of 1974 further regulates the rights of an individual to gain access to information held by the government about oneself; the right to amend that information if it is inaccurate, irrelevant, untimely, or incomplete; and the right to sue the government for violations of the statute.

The events that have taken place since September 11th to fight terrorist threats appear to be shifting concerns about privacy vulnerability back to the public sector. In the U.S. alone, a number of initiatives based on the need to improve security to ensure social order have been undertaken. These include the Total Information