Chapter 5.10
Effects of Individual Trust in Broadcast Media and the Internet on Privacy-Risking Uses of E-Health: An Expanded Analysis

E. Vance Wilson
Arizona State University, USA

David D. Dobrzykowski
Eastern Michigan University, USA

Joseph A. Cazier
Appalachian State University, USA

ABSTRACT

People claim to be concerned about information privacy on the Internet, yet they frequently give out personal information to online vendors and correspondents with whom they have little, if any, prior experience. This behavior is known as the privacy paradox and is particularly relevant to the context of e-health, due to the special risks of health information exposure. Using data from the 2005 Health Information National Trends Survey (HINTS), this study addresses a key question regarding online health information privacy: Do individuals self-police risky e-health activities (i.e., uses where personal information is given out) or are they indifferent to risk based upon generalized trust in broadcast media and the Internet as sources for health information? In exploring this question, our study contrasts several alternative models of health trust, and recommends a new partial-mediation model for future studies. The results show that Internet trust mediates most effects of broadcast media trust on Internet use and that Internet trust plays a much smaller role in motivating Internet uses that are risky than is the case for low-risk uses. These results have important implications for researchers, policymakers, and healthcare administrators in determining the level of privacy protection individuals need in their use of e-health applications.

DOI: 10.4018/978-1-61350-323-2.ch5.10

INTRODUCTION

Early e-health offerings were primarily informational, but an increasing variety of online healthcare services are now being developed. These services include online access to health records (Masys, Baker, Butros, & Cowles, 2002), electronic billing and payment services (Altinkemer, De, & Ozdemir, 2006), and public health reporting (Järvinen, 2009). Patients can interact with peers and mentors in online support groups (Zrebiec & Jacobson, 2001) and engage in computer-mediated communication with physicians and clinical staff (Wilson, 2003). And even though many of the early e-health vendors failed (Itagaki, Berli, & Schatz, 2002), leading e-business organizations, including Microsoft and Google, are now turning their attention toward e-health development (Lohr, 2007). The new e-health services are prized by the public (Homan, 2003), yet they entail important information privacy risks that are inherent to communication and personalization.

Exchange of information during communication creates opportunities for personal information to be exposed, either through an accident, such as inadvertently overhearing a conversation, or by design, as is the case with surreptitious "phishing" strategies (Hesse, Nelson, Kreps, Croyle, Arora, Rimer & Viswanath, 2005). Information privacy risks also emerge in personalization, defined as "the ability to proactively tailor products and product purchasing experience to tastes of individual consumers based upon their personal and preference information" (Chellappa & Sin, 2005, p. 181). In the case of e-health, personalization can be applied to acquire and organize health information according to the patient's preferences, to automatically generate health forms and records, or to provide monitoring capabilities to help manage chronic disease. However, information used for personalization can be exposed due to events beyond an individual's control, as illustrated by the recent exposure of records relating to 1.8 million patients and physicians that occurred when a laptop computer belonging to the U.S. Veterans Administration was stolen (Gaudin, 2007). Although individuals clearly benefit from having access to personalized e-health that can do more than simply provide health information, personalization does tend to increase the risk that privacy will be compromised.

Population sample surveys show that individuals strongly desire privacy in their use of the Internet (Fox, Rainie, Horrigan, Lenhart, Spooner, & Carter, 2000), yet they are increasingly pragmatic about providing personal information online (Taylor, 2003). This *privacy paradox* of individuals seeking privacy while giving out their information is especially relevant to the context of e-health due to the sensitivity of health information. Harm from the exposure of health information can have unique financial and emotional effects, such as obstructing insurance coverage, limiting job prospects, damaging personal relationships, and inviting social ostracism. If individuals perceive the potential for privacy risk harm to be especially high in the context of health information, this will reduce their motivation to use e-health (Cazier, Wilson, & Medlin, 2007).

Healthcare policymakers and regulators have responded to the public's privacy concerns by creating specialized professional privacy standards (Mason, McCall, & Smith, 1999) and stringent privacy regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which instates severe penalties for violations. These standards and regulations are intended to protect individuals from having their health information exposed, but they have proved to be cumbersome and relatively ineffective (Choy, Hudson, Pritts, & Goldman, 2001). Thus, current standards and regulations that apply to health information may actually reduce benefits and increase costs of e-health use.

We propose that it is important to learn more about the factors that drive use of e-health services, the nature of the relationships, and the impacts of the relationships on privacy risk. This knowledge