Chapter 66
Sealing One's Online Wall Off From Outsiders:
Determinants of the Use of Facebook's Privacy Settings Among Young Dutch Users

Ardion Beldad
University of Twente, The Netherlands

ABSTRACT

Pieces of personal information (e.g. contact details, photos, thoughts and opinions on issues and things) on online social network sites are susceptible to third-party surveillance. While users are provided with the possibility to prevent unwarranted access using available privacy settings, such settings may not often be adequately used. This research investigated the factors influencing the use of Facebook's privacy settings among young Dutch users based on the premises of Protection Motivation Theory and Technology Acceptance Model. A paper-based survey was implemented with 295 students in a vocational school in the eastern part of the Netherlands. Results of hierarchical regression analysis indicate that privacy valuation, self-efficacy, and respondents' age positively influenced the use of Facebook's privacy settings. Furthermore, the size of Facebook users' network negatively influences the use of those settings. Important results and points for future research are discussed in the paper.

1. INTRODUCTION

Online social networking (OSN) for the last eight years, has become as common as watching TV or taking a public transportation, especially among younger Internet users. The popularity of OSN sites could easily be attributed to the benefits they extend to their users (e.g. communication, online identity management, online information sharing). Just like most OSN sites, Facebook enables its users to establish connections and maintain relations in the online environment. Nonetheless, such advantages could easily be offset by the possible negative ramifications for Facebook users' online information privacy.

DOI: 10.4018/978-1-5225-7113-1.ch066

In her book 'I Know Who You Are and I Saw What You Did: Social Networking and the Death of Privacy', Andrews (2012) argues that online social network site users have confronted different problems of varying levels of severity as a consequence of information disclosure on such sites.

Studies show that people who are concerned about their information privacy online employ different mechanisms to ensure its protection – whether the mechanism is behavioral (e.g. information fabrication, information withdrawal) or technologically-facilitated (Davis & James, 2013; Metzger, 2007; Oomen & Leenes, 2008; Youn, 2009). This study focuses on technologically-facilitated privacy protection behavior of Facebook users, specifically by using the platform's privacy settings, which allow users to limit and define non-contacts' access to their profiles. The research primarily aims at identifying the factors influencing the use of Facebook's privacy settings, specifically aimed at preventing non-contacts' access to users' profiles, specifically among young Facebook users in the Netherlands. The primary question that the current research aims at addressing is 'What factors influence the use of privacy settings among young Facebook users in the Netherlands?'.

Communication Privacy Management (CPM) postulates that people formulate guidelines that aid them in deciding whether or not to divulge personal information and in identifying the most effective strategies to safeguard their privacy. Such regulation of information disclosure, CPM stipulates, is anchored on people's belief that they own their information, and, thus, they feel entitled to control the flow of their information to others (Petronio, 2002).

Beldad, De Jong, and Steehouder (2011) claim that from the perspective of Protection Motivation Theory (PMT) people's apprehension of having their information privacy compromised online pushes them to adopt some forms of privacy protection mechanisms. More importantly, the theory posits that protection motivation emanates from a cognitive evaluation of an event as pernicious (threat severity) and is highly likely to occur, alongside the expectation that the selected protection mechanism is effective in curtailing the noxious event (response effectiveness) from transpiring and that user is competent in employing the mechanism (self-efficacy; Rogers, 1975, 1983).

Response effectiveness and self-efficacy, to a great extent, are conceptually similar to the factors influencing the adoption of technology: usefulness and ease of use, respectively. Technology Acceptance Model (TAM) proposes that people will not hesitate to use a specific technology if its use will result in positive outcomes and its deployment is effortless (Davis, 1989). An investigation of the factors influencing the use of a particular privacy protection mechanism, therefore, could substantially benefit from the pivotal premises of PMT and TAM.

While it is known that people employ various strategies to manage their online information privacy, research into the use of an OSN site's privacy settings are still limited. Those that have been published focused either on the experience with and attitude towards using those settings (boyd & Hargittai, 2010) or on the contexts precipitating the use of privacy settings (Stutzman & Kramer-Duffield, 2010). The current study aims at understanding the factors influencing the use of Facebook's privacy settings using the assumptions of PMT and TAM. The combination of the these two theories to gain insight into the mechanism behind privacy settings use is one of the study's contribution to the research into online information privacy management. Moreover, results of the current study aims at offering new insights into the effects of users' Facebook usage length (in years) and network size on privacy settings use – and the impact of these factors has not yet received sufficient research attention.

The current study proposes that risk perception (threat severity), self-efficacy (or ease of using a protection mechanism), and the effectiveness of Facebook's privacy settings (usefulness) are important determinants of the use of those settings. Additionally, the value people attach to their information pri-