

Chapter 6

Information Disclosure on Social Networking Sites: An Exploratory Survey of Factors Impacting User Behaviour on Facebook

Clare Doherty

National University of Ireland Galway, Ireland

Michael Lang

National University of Ireland Galway, Ireland

James Deane

Cora Systems, Ireland

Regina Connor

Allied Irish Bank, Ireland

ABSTRACT

This chapter explores how six constructs—control, trust, perceived risk, risk propensity, perceived legal protection, and privacy disposition—affect information disclosure on the Social Networking Site (SNS) Facebook. Building upon previous related work, an extended causal model of disclosure behaviour is proposed. The hypothesised relationships in this model were tested using survey data collected from 278 social networking site users in Ireland. The results of the analysis provide strong support for the proposed model.

INTRODUCTION

Social Networking Sites (SNS) such as Facebook, Twitter and LinkedIn offer a convenient way to maintain existing personal and professional relationships while also developing new ones. With millions of people interacting and communicating online, coupled with the amount of personal information dis-

DOI: 10.4018/978-1-5225-7113-1.ch006

closed, this can lead to personal information ending up in the wrong hands and users may unsuspectingly leave themselves susceptible to privacy and security risks in cyberspace (Harden et al. 2012). SNS are web-based services which allow people to build a public or private profile in a particular system, join users with whom they may or may not share a connection, and view other people's connections within this system (Boyd and Ellison 2007). These websites have become particularly popular tools for social experimentation; many users use Facebook for either "social searching" or "social browsing" to interact with people they already know and to meet new people.

Disclosing personal information is an important aspect of building relationships with others (Christofides, 2009; Nguyen et al, 2012). Privacy and trust are central concerns as regards on-line behavioural intentions (Liu et al 2005). A person's trusting belief can impact their loyalty of using Facebook, ultimately affecting how active they are and how much information they disclose (Wang, 2013). A trade-off is undertaken when using SNSs between the perceived benefits of using SNS on one hand and the potential risks of personal information disclosure on the other. The perceived benefits of using SNS are not discounts or free services, but social capital or the development of attachment through relationships (Xu et al 2013). A previous study has shown that there is a complimentary relationship between trust and information disclosure online (Henderson and Gilding 2004). When looking at privacy in relation to Facebook it has been said that Facebook should go beyond and try and increase the protection of users from corporate surveillance by protecting users' privacy (Fuchs 2011).

This chapter reports the findings of an exploratory opinion survey conducted in Ireland of 278 SNS users. Because the various SNS providers (e.g. Facebook, LinkedIn, Twitter, Google+, MySpace, Four-Square, Bebo, etc.) have different features, we chose in our questionnaire to specifically concentrate on the most popular SNS, Facebook, as we felt it might have led to confusion and measurement error if participants were instructed to answer questions but not given a clear context. Facebook has enjoyed a rapid increase of its users since it opened up its registration to not only college-based students in 2006 (Joinson, 2008). At the start of 2013, Facebook had 1.11 billion users using the site each month (Associated Press, 2013). Facebook has undergone radical change over the past 24 months by introducing a new "timeline" profile and updating its news feed aspect. However, it has not only changed its profile layout and its profile of users, but more importantly the potential motivations of users.

In this chapter we look at how six constructs affect information disclosure on Facebook: (1) perceived control; (2) trust; (3) perceived risk; (4) perceived legal protection; (5) risk propensity; and (6) privacy disposition. Our research model builds upon aspects of the Privacy Calculus model (Dinev and Hart 2006) and also the previous work of Krasnova et al. (2010), but is different in a number of regards. Whereas those earlier models include perceived control and perceived trust as single constructs, our factor analysis revealed that these two factors each have two distinct components, relating to (a) trust in / perceived control over individuals, and (b) trust in / perceived control over Facebook/on-line companies. Additionally, our model explores a number of factors which have received very little attention in previous studies, being the latter three of those aforementioned.

The chapter is organised as follows: Section 2 provides an overview of previous literature and sets forth the hypotheses to be explored. Section 3 outlines the research approach. A discussion of the findings of our study is presented in Section 4. A number of possible areas for future research are proposed in Section 5. We then present our conclusions in Section 6.

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/information-disclosure-on-social-networking-sites/213796

Related Content

Russian Cyberwarfare Taxonomy and Cybersecurity Contradictions Between Russia and EU: An Analysis of Management, Strategies, Standards, and Legal Aspects

Kimberly Lukin (2019). *National Security: Breakthroughs in Research and Practice* (pp. 408-425).

www.irma-international.org/chapter/russian-cyberwarfare-taxonomy-and-cybersecurity-contradictions-between-russia-and-eu/220891

Border Security and Cooperative Initiatives to Counter Illicit Drug Trafficking: The Case of Jamaica and the USA

Suzette A. Haughton (2019). *National Security: Breakthroughs in Research and Practice* (pp. 898-915).

www.irma-international.org/chapter/border-security-and-cooperative-initiatives-to-counter-illicit-drug-trafficking/220922

Compliance of Electronic Health Record Applications With HIPAA Security and Privacy Requirements

Maryam Farhadi, Hisham M. Haddad and Hossain Shahriar (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications* (pp. 1605-1618).

www.irma-international.org/chapter/compliance-of-electronic-health-record-applications-with-hipaa-security-and-privacy-requirements/213873

Defense Acquisition, Public Administration, and Pragmatism

Keith F. Snider (2019). *National Security: Breakthroughs in Research and Practice* (pp. 774-792).

www.irma-international.org/chapter/defense-acquisition-public-administration-and-pragmatism/220915

Artificial Intelligence: A Tool for Detection of Pandemics

Kumud Pant, Bhasker Pant and Somya Sinha (2023). *Cyber Trafficking, Threat Behavior, and Malicious Activity Monitoring for Healthcare Organizations* (pp. 120-142).

www.irma-international.org/chapter/artificial-intelligence/328129