Online Privacy: Measuring Individuals' Concerns

Maria Moloney and Frank Bannister

Trinity College Dublin
Maria.Moloney@cs.tcd.ie, fbnnistr@tcd.ie

Abstract. Existing research within the Information Systems domain has shown that there is a substantial level of online privacy concern among the online community. However it is not clear from an extensive review of the literature that the complete set of online privacy concerns has yet been identified or whether the concerns that have been investigated, by way of surveys, have adequate theoretical foundations. This paper considers the work of two prominent privacy theorists Westin and Altman, and from their privacy theories infers a set of online privacy concerns. These inferred privacy concerns are then compared with a list of online privacy concerns drawn from the empirical literature. This comparison highlights the similarities and inconsistencies between both sets of concerns. From the findings, an online privacy model is devised which attempts to outline the components of the concept of online privacy and their interdependencies. By representing the concept of online privacy in the form of a model, areas where concern arises can be highlighted more easily and as a result measures can be taken to reduce such concern.

Keywords: Information Systems, Internet, Privacy, Trust, Data Security.

1 Introduction

In the last twelve months, there have been a number of high profile breaches of privacy reported in the media. In early 2008, a laptop with the confidential records of more than 170,000 Irish blood donors and 3,200 patients was stolen in New York. The stolen records included names, genders, dates and places of birth, telephone numbers and the blood groups of individuals who had given blood (Heffernan and Kennedy, 2008). The UK's Ministry of Defence lost three laptops containing personal details of hundreds of thousands of military recruits. The files contained names, addresses, passport details, national insurance numbers, drivers' licence details, family details, doctors' addresses, NHS numbers and some bank details of those who joined, or inquired about, the armed forces (Drury, 2008). In late 2007, Revenue and Customs in the UK lost the personal details of nearly half of the UK's population when they lost the entire child benefit database in the post (Webster et al., 2007).

These breaches only reflect Ireland and the UK. In the US, over 217 million records containing personal information have been involved in security breaches since 2005 (Privacy Rights Clearinghouse, 2005). Given the frequency and magnitude of these breaches, it is little wonder that concern is growing among the public for the safety of their personal information.

G. Psaila and R. Wagner (Eds.): EC-Web 2008, LNCS 5183, pp. 21 – 30, 2008.

In this paper, it is argued that an interdisciplinary approach is required to resolve the ethical issue of protecting an individual's private space. Consequently, the paper draws on the disciplines of law, social studies and information systems. The paper is organised as follows. The next section examines some theories and definitions of privacy from within these disciplines. Section three covers the formulation of the research question and section four contains a brief outline of the proposed research methodology. This is followed by a short conclusion.

2 Review of Relevant Literature

According to Westin (2003), whenever a privacy claim is recognised in law or social convention, we speak of "privacy rights". Privacy has been declared as a fundamental right for every human in many enduring bodies of law, the principle ones being Article 12 of the Universal Declaration of Human Rights (United Nations, 1948), article 8 of the European Convention on Human Rights (ECHR) (The Council of Europe, 1950), article 7 and 8 of The Charter of Fundamental Rights of the European Union (The Council of Europe, 2000).

However, to establish privacy as a fundamental human right is futile if the very notion of privacy is not understood. This paper uses privacy definitions from two domains that have contributed greatly towards the formulation of the privacy concept to which our modern society adheres. These domains are the ethical and legal domains.

A challenge, and an opportunity, in this research is that there is no agreed definition of what constitutes privacy. To give a flavour of the complexity of the problem, consider the following approaches to the subject. The theorist Charles Fried (1990) believes that privacy is not simply an absence of information about a person in the minds of others, rather it is the control that a person has over information about themselves. This view is somewhat incomplete in that privacy can be interpreted as the control that a person has over information about themselves that they wish to keep from others. As a reaction to Fried's 'control theory' of privacy Moor (1997) proposes a 'restricted access' view of privacy. Rather than regarding privacy as an all or nothing proposition, Moor regards it as a complex of situations in which information is authorized to flow to specific people, at specific times. He argues that in a highly computerized culture, it is simply impossible to control all personal information that resides on computer systems around the world. Therefore, the best way to protect our privacy is to make sure the right people have access to relevant information at the right time. Moor calls this view of privacy, the restricted access view, which has the added advantage of Fried's control theory in that it gives individuals as much control over personal data as realistically possible. For this reason he labels his theory the "control/restricted access" theory of privacy (Moor, 1997).

An advocate of Moor's control/restricted access theory is Herman Taviani. Taviani also points out that modern privacy theorists tend to analyse the notion of privacy in terms of controlling the flow of personal information and have coined the phrase "informational privacy" to express this new concept (Taviani, 2007). The term, informational privacy, is often used when referring to an individual's online privacy