Chapter 7.6
Privacy Factors for Successful Ubiquitous Computing

Linda Little
Northumbria University, UK

Pam Briggs
Northumbria University, UK

ABSTRACT

Certain privacy principles have been established by industry, (e.g. USCAM, 2006). Over the past two years, we have been trying to understand whether such principles reflect the concerns of the ordinary citizen. We have developed a method of enquiry which displays a rich context to the user in order to elicit more detailed information about those privacy factors that underpin our acceptance of ubiquitous computing. To investigate use and acceptance Videotaped Activity Scenarios specifically related to the exchange of health, financial, shopping and e-voting information and a large scale survey were used. We present a detailed analysis of user concerns firstly in terms of a set of constructs that might reflect user-generated privacy principles; secondly those factors likely to play a key role in an individuals cost-benefit analysis and thirdly, longer-term concerns of the citizen in terms of the impact of new technologies on social engagement and human values. [Article copies are available for purchase from InfoSci-on-Demand.com]

INTRODUCTION

An individual has a right to determine how, when and to what extent information about the self will be released to another person – something commonly referred to as individual privacy (USACM, 2006). Not surprisingly, new developments in technology present challenges to the individual's rights in this respect (Price, Adam, & Nuseibeh, 2005) and so privacy issues are widely discussed by academics and designers alike (Kozlov, 2004; Dine & Hart, 2004), most of whom respect the individuals' right to control and protect their personal information (Nguyen & Truong, 2003).

Users are well aware of the need for informational privacy and frequently express concern

about their rights. E-commerce consumers, for example, have major concerns about who has access to their personal data (Cranor, Reagle, & Ackerman, 1999; Jackson, et al., 2003; Earp, et al., 2005); and show a reluctance to disclose information to commercial web services (Metzger, 2004).

However, even those consumers who hold privacy in high regard are able to recognise the benefits of disclosing information (Hinz, et al., 2007). We need to understand why it is that users uphold their right to privacy whilst simultaneously giving away sensitive personal information (Malhotra, Kim, & Agarwal, 2004). In other words, we need to better understand the cost-benefit trade-off in which e-consumers will trade personal information online in order to achieve an improved service (something referred to as the 'privacy-personalisation paradox' (Awad & Krishnan, 2006)).

The perceived costs and benefits in any transaction inevitably reflect personal beliefs. People differ with respect to the value they place on privacy – and these individual differences are reflected in scales which have been designed to measure the strength of individual feeling in this regard. These include the Concern for Information Privacy (Smith, Milberg & Burke, 1996) and the Internet Users Information Privacy Concerns (Malhotra, et al., 2004).

In keeping with the concept of some kind of individualised privacy setting, designers are increasingly allowing users to manage their own concerns by setting privacy preferences. On the Internet, at least, various architectures have been suggested that allow personalized settings (Kobsa, 2003). For example the Platform for Privacy Preferences (P3P) allows users to set their own personal privacy preferences and if visited sites do not match these then warnings are shown – leaving responsibility ultimately with the individual user (Cranor, 2002). Guha, et al., (2008) propose a programme called 'none of your business (NOYB)' to protect privacy while online and have tested the system on social networking sites. NOYB provides fine-grained control over user privacy in online services while preserving much of the functionality provided by the service. They argue NOYB is a first step towards a 'new design paradigm of online services where the user plays an active role in performing the sensitive operations on data, while the service takes care of the rest' (p.53).

Such tools are useful, but they are not future-proof. Specifically, they could not cope with the kinds of seamless, anywhere, anyplace exchanges of personal information that are anticipated by designers of ubiquitous computing systems. Systems that collect, process and share personal information are prerequisites for the creation of intelligent environments that can anticipate user's needs and desires (Dritsas, Gritzalis, & Lambrinoudakis, 2006). Pervasive technologies are expected to be responsive to different contexts and to act on the user's behalf seamlessly – but will privacy violations inevitably ensue?

Researchers disagree. On the one hand, (Olsen, Grudin, & Horvitz, 2005) argue that tools could be constructed to capture quite complex privacy preferences, preferences that are tailored to the context of the exchange, the sensitivity of the enquiry and the disclosure preferences of the individual. Such tools – if feasible - would prevent privacy violations in the day to day exchanges of ubiquitous computing. On the other hand, (Palen & Dourish, 2003) argue that a-priori privacy configurations and static rules will not work, but insist that the disclosure of information needs to be controlled dynamically and needs, essentially, to be passed into the hands of software agents designed to uphold general privacy preferences.

This begs the question of just what kinds of assurances software agents might look for before agreeing to the release of personal data. As a clue to this we might start by looking at established principles underpinning the right to privacy (Kobsa, 2007). For example, the U.S. Public Policy Committee of the Association for Computing