



Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making



Caitlin D. Cottrill ^{a,*}, Piyushimita “Vonu” Thakuria ^{b,1}

^a University of Aberdeen, School of Geosciences, Elphinstone Road, Aberdeen, Scotland AB24 3UF, UK

^b UK ESRC Urban Big Data Centre, University of Glasgow, Glasgow G12 8RS, UK

ARTICLE INFO

Article history:

Received 8 September 2014

Received in revised form 12 March 2015

Accepted 4 April 2015

Keywords:

Location privacy

Privacy-utility trade-off

Willingness-to-trade privacy

Risk

ABSTRACT

With the advent and rapid dissemination of location-sensing information technology, the issue of location information privacy is receiving growing attention. Perhaps of greatest concern is ensuring that potential users of mobile Information and Communications Technologies (e.g., Location-Based Services and Intelligent Transportation Systems) are comfortable with the levels of privacy protection afforded them, as well as with the benefits they will receive in return for providing private location information. This paper explores the concepts of privacy risks, benefits, willingness to trade, and compensation in relationship to mobile and locational technologies using a stated preference survey to ascertain areas of interest in determining the trade-offs that consumers will be willing to make in return for mobility enhancements. Analysis of the survey leads to findings that while respondents believe that sharing data in the mobile environment may pose privacy risks, they do not generally take steps necessary to address these risks; that privacy preferences are impacted by a range of factors, including both personal and contextual considerations (such as factors arising from their specific situation at the time of information seeking); and that willingness to trade private location data is dependent upon a number of factors related to context, personal characteristics, expected benefits and degree of trust in the collecting organization.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

One of the most well-known definitions of privacy is “the right to be left alone”, as set forth by Warren and Brandeis in their 1890 Harvard Law Review article, “The Right to Privacy.” In ensuing years, however, such a broad conception of privacy has proven insufficient, particularly as technologies allowing for the near-continuous monitoring of our actions, behaviors, and preferences have multiplied, and methods and techniques for cataloguing and mining this data have increased in both power and scope. In part, Warren and Brandeis’s conception was constructed upon the foundation of *personal* (or physical) privacy. [Smith et al. \(2011\)](#) differentiate between information and personal privacy, stating that, “The latter concerns physical access to an individual and/or the individual’s surroundings and private space; the former concerns access to individually identifiable personal information.” Given the advent of widely distributed sensor equipped personal mobile devices such as smartphones, concerns around information privacy are quickly mounting. For example, a 2012 Pew Research Report found

* Corresponding author. Tel.: +44 (0)1224 273694.

E-mail addresses: c.cottrill@abdn.ac.uk (C.D. Cottrill), Piyushimita.Thakuria@glasgow.ac.uk (P. “Vonu” Thakuria).

¹ Tel.: +44 (0) 141 330 4079.

that of those Americans with application ("app") enabled cellular phones, over half had either decided not to install or uninstalled an app due to personal information concerns (Boyles et al., 2012). Such findings have brought information privacy to the forefront of concern, and made it necessary to determine more concretely how consumers view the value of their personal information, and under what circumstances they are willing to trade this private information for benefits and services. The complexity of this task is illustrated by Pavlou (2011), who states that, "...much ambiguity and disagreement still surrounds the concept of information privacy. This is because information privacy is an arguably complex concept that can be studied from many perspectives, including law, economics, psychology, management, marketing, and Information Systems." In addition, as elaborated below, preferences regarding information privacy are also arguably contingent upon both contextual and personal circumstances – they should not be conceptualized as static.

In this paper, we focus upon the concept of location privacy, defined by Duckham and Kulik (2006) as, "...a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others. In short, control of location information is the central issue in location privacy." Thakuriah and Geers (2013) note that there are three fundamental approaches to addressing location privacy: legal, consumer awareness and technology-based. While technology- (or technique) based approaches to location privacy protection are a key tool in current the current environment of dynamic data, in this paper our focus is on the consumer awareness aspects of location privacy, a particularly relevant area of concern given several recent high-profile and widespread privacy controversies. We aim to explore consumer privacy awareness and concerns via the use of a survey instrument to test issues related to knowledge, risk, willingness to trade, and benefits in relation to location sensing technologies, such as GPS enabled smartphones. Our objectives are motivated by a need to understand the level of comprehension that users of mobility ICTs have regarding locational privacy and ways in which they balance the need for information with desires for location privacy. We begin by addressing the issue of privacy in concept and context, particularly as location privacy may be linked to economic conceptions of ownership and control. Questions related to the topic of privacy in the context of ubiquitous mobility technology, in particular in relation to applications related to mobility-related Information and Communications Technologies (ICTs – such as Intelligent Transportation Systems (ITS) and Location-Based Services (LBS)), will next be analyzed in order to determine the relationships between individual privacy preferences and willingness to trade information related to personal identity (such as name or address) and location information (such as trip origins and destinations, time of travel, and route information). These questions will be addressed by evaluating survey results concerning current consumer expectations and preferences related to privacy in the mobile environment.

2. Background

2.1. Technical methods of privacy protection

While, as noted above, this paper is primarily focused on location privacy policies and consumer awareness of privacy issues, it is also relevant to make note of technical methods of privacy protection that have been employed in or suggested for the transportation arena. Given both the dynamic nature of location information and the constraints faced in balancing data privacy with usability, work on techniques for privacy preservation has seen substantial growth in recent years. Techniques for privacy preservation have ranged from methods of background data perturbation, masking, and cloaking (Hoh and Gruteser, 2005; Hoh et al., 2012; Xie et al., 2011) to methods focused on how location data are presented and shared publically (particularly within social networks) (Li and Chen, 2010; Puttaswamy et al., 2014; Mascetti et al., 2011). Additional exploration has also taken place regarding issues such as the economic valuation of privacy in cases of differentiated tolling (Zangui et al., 2013) and the implementation of 'Privacy-By-Design' approaches in the collection of mobile data for fine-grained modeling purposes (Sun et al., 2013). The variety of issues under consideration, and the degree to which they are tailored to both the type of data being incorporated and the relevant area of transportation, reveals the extent to which privacy is an open question in the transportation field. In each case, the development, testing, and analysis of proposed techniques must address questions related to how data are collected, how they are processed, and how they are used, balancing the desired degree of accuracy with the sensitivity of collected data. Such developments are relevant to the discussion here, as they are indicative of how expectations are set for privacy preservation within the development of location-aware services – a critical point is ensuring that the technical set-up of location-aware apps and services is accurately reflected in privacy policies (i.e. not promising more than can be delivered). Further exploration of how policy and technical approaches to location privacy preservation may be evaluated in conjunction is presented in Cottrill (2009).

2.2. Conceptualizing privacy: context and preferences

As noted above, privacy as a concept has many definitions, but key components tend to be issues of control and flow of information. Westin (2003), for example, has defined privacy as, "the claim of an individual to determine what information about himself or herself should be known to others." This definition contains veiled reference to one of the complicating considerations of privacy: namely, the context in which information sharing should take place. As Nissenbaum (2010) states, "...a right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information." This concept of appropriateness specifically introduces the idea of context, as it raises the claim that norms of privacy

Download English Version:

<https://daneshyari.com/en/article/6936730>

Download Persian Version:

<https://daneshyari.com/article/6936730>

[Daneshyari.com](https://daneshyari.com)