Transportation Research Part C 63 (2016) 195–206

Contents lists available at ScienceDirect

Transportation Research Part C

journal homepage: www.elsevier.com/locate/trc

Technology engagement and privacy: A cluster analysis of reported social network use among transport survey respondents

Orla Thérèse McCarthy, Brian Caulfield, Margaret O'Mahony *

Department of Civil, Structural & Environmental Engineering, Centre for Transportation Research, Trinity College Dublin, Dublin, Ireland

ARTICLE INFO

Article history:
Received 24 August 2015
Received in revised form 9 November 2015
Accepted 28 December 2015
Available online 12 January 2016

Keywords:
Security
Privacy
Social networking

ABSTRACT

New technologies are constantly being researched and developed to improve the sense of security of transport users. However, security technologies could also pose their own risks with regard to transport users' privacy through the potential for data collection and storage. Transport, in particular, allows the data collector potential access to information on the users' habits through the location information that could be collected during an individual's interaction with technology during their travels. Some technologies, such as personal security apps (which essentially turn a smartphone into a type of panic alarm) also allow for the linking of the security technology and social networking apps. Given this link and the extent to which personal data, including location data, can be included in an individual's social networking account, it was decided to investigate if the use of social networks could be related to individuals' opinions on the use of their data through new technologies, such as personal security apps. This paper presents an exploration of the possibility of grouping respondents to a transport survey ($N = 469$) based on their answers to questions on their social networking (SNS) use. It was hypothesised that if distinct groups exist within the SNS data, then they could be used as a supplementary personal variable for underlying privacy concerns and levels of engagement with technology in future transport studies. This would be in addition to the socio-demographic information collected in the survey. This paper presents the initial dimension reduction of the response variables to create composite variables. That is followed by the exploratory clustering of responses using two-step cluster analysis. Finally, the paper discusses the hypothesis testing of the resultant clusters against the socio-demographic responses to ascertain if additional information is provided by the clustering results. The transport survey responses were collected in Ireland, and a subset of responses, from the Greater Dublin Area, were used for the analysis in this paper. The results demonstrate that there is scope for this type of method to be used when researching new security technologies in transport.

1. Introduction

There is increasing awareness and concern regarding privacy of personal data. In recent years there have been several articles in the media regarding the surveillance of data (e.g. Greenwald, 2013; Greenwald and MacAskill, 2013a, 2013b;

* Corresponding author.
E-mail addresses: otmccart@tcd.ie (O.T. McCarthy), brian.caulfield@tcd.ie (B. Caulfield), margaret.omahony@tcd.ie (M. O'Mahony).

http://dx.doi.org/10.1016/j.trc.2015.12.015
0968-090X/

Greenwald et al., 2013). Many of the personal security apps operate by turning the user's phone into a panic alarm which sends their location and a request for help to chosen contacts. As part of the research into transport security technology, it was deemed necessary to find a way to account for the survey respondents' existing technology engagement and privacy behaviour. This was in order to allow a thorough investigation of the public's opinions of security technologies in transport settings. There has been a proliferation of social networking technologies, such as Facebook and LinkedIn, for example, in recent years. Many of the personal security apps available, such as those proposed by Ovelgönne et al. (2010) and Ananda Kanagaraj et al. (2013), allow users to connect the app with their social networking accounts. Therefore, it was hypothesised that collecting data on respondents' use, or not, of similar social networking services could contribute to explaining the survey responses on the use of personal security apps, beyond the insight that could be gleaned from the socio-demographic information of the respondents.

2. Background

2.1. Transport and privacy

As Intelligent Transport Systems (ITS) become more prevalent in all modes of transport, the issue arises as to the safety of the data which is collected by these systems and the level of privacy invasion it represents for travellers. Ogden (2001) presents a review of the research literature regarding privacy and the use of electronic toll tags, which can be uniquely identifiable. The retention of location data, which could allow for profiling over time, is mentioned as the most sensitive issue. Among the other issues discussed are data's repurposing (which refers to using collected data for uses other than the one (s) for which it was collected, including the potential for tracking) and the linking of the data with other databases. Wigan and Clarke (2009) discuss how various technologies which use location information can be repurposed as surveillance technologies due to the collection of that location data. They highlight the need for effective privacy protections for data to be incorporated into such technologies. Fries et al. (2012) examined the issue of privacy in the development of ITS from the perspective of the authorities within the transportation industry. Two different surveys were conducted, examining ITS, with transportation agencies in the USA. One of the conclusions of the research was that future implementation of technologies would be influenced by public privacy concerns (Fries et al., 2012).

People's willingness to trade between privacy and freedom on the one hand and security on the other, when travelling by train, were examined by Potoglou et al. (2010). People's opinions are explored through a willingness to pay survey. On the whole the results indicated that participants would be willing to pay for security improvements. The authors draw from this the conclusion that security has therefore taken precedence over privacy and freedom in the eyes of their respondents (Potoglou et al., 2010). Cruickshanks and Waterson (2012) explored this theme through survey based research to try and identify if the level of personal information harvested in the future, with the aim of improving benefits for transport users, will reach a tipping point whereby people will feel that their travel freedom is reduced if they want to protect their privacy. Cruickshanks and Waterson (2012) conclude that the advent of some technologies in the future could impinge on the travel choices of certain groups in society. The factors identifying these groups related to: age, education, gender, ethnicity and/or having little experience of using the latest transport technologies (Cruickshanks and Waterson, 2012).

Other work by Chen et al. (2015) examines the influence of friendships in social networks on drivers' route choice. It explores the route choice process when drivers can access information about other drivers' route choices in a social network. In this case, the issue of privacy is perhaps less of a concern because drivers only share information within their own social network. However, the work does point to the possibility of calibrating spatially-based applications with the growing ability to jointly track drivers' route choice in the future.

2.2. Privacy awareness and concerns

Privacy awareness and concerns in the mobile environment (in light of the advent of ITS and Location Based Services (LBS)) were also investigated by Cottrill and Thakuriah (2012). They used a survey to test issues related to knowledge, risk, willingness to trade and benefits in relation to mobile transportation technologies. As part of the survey, respondents were asked, among other things, some questions about their use of certain transportation or mobile technologies. They were also asked to report on how often they read or skim Terms of Use or Service when they use those technologies. Among the results presented in the paper is that a significant majority reported that they never or rarely read or skim Terms of Use or Service, or notice the presence of a privacy policy (Cottrill and Thakuriah, 2012). The percentages who reported reading them, for both types of terms, were higher where the service provider was a public company rather than a private one (for example Google). The paper goes on to look in more depth at respondents' data and privacy opinions in the context of these technologies, including examining the trade-offs that consumers are willing to make between provision of personally identifying information related to transportation and potential mobility benefits (Cottrill and Thakuriah, 2012). Indeed privacy is also an issue in transport surveys particularly when people are asked to reveal location based data and socio-economic details. Cottrill (2014) also looked at app users' trust in data privacy of apps with location based elements, and the actions they took on foot of their concerns, if any existed. However, this was from the perspective of potential usability of data from these apps in transport planning. In discussing the results, the authors suggest that, while data collected from these apps are useful, it