On the road – listening to data subjects' personal mobility data privacy concerns

Anna Rohunen[a] (corresponding author)

Jouni Markkula[a]

[a]*University of Oulu, Faculty of Information Technology and Electrical Engineering (ITEE), Empirical Software Engineering in Software, Systems and Services (M3S) research unit*

P.O. Box 4500, FI-90014, University of Oulu, Finland

Tel.: +358 40 7316016 (Anna Rohunen), +358 50 3536025 (Jouni Markkula)

E-mail address: {Anna.Rohunen, Jouni.Markkula}@oulu.fi

ABSTRACT

Efficient utilisation of new mobility data-based services and promotion of acceptance of data collection from vehicles and people demand an understanding of mobility data privacy concerns, associated with increasing use of tracking technologies, diverse data usages and complex data collection environments. Understanding privacy concerns enables improved service and system development and identification of appropriate data management solutions that contribute to data subjects' privacy protection, as well as efficient utilisation of the collected data. This study aimed to explore earlier research findings on privacy concerns evaluation and investigate their validity in mobility data collection. Explorative multimethod research was conducted in a mobility service pilot through data controller interviews, user interviews and a user survey. The study's results indicated the need to revise and complement existing privacy concerns evaluation in mobility data collection contexts. The primary findings were as follows: (1) Privacy concerns specific to the mobility data collection context exist. (2) Privacy concerns may change during the service use. (3) Users are not necessarily personally worried about their privacy although they ponder on privacy issues. (4) In contrast to traditional 'privacy calculus' thinking, users' expected benefits from data disclosure may also be driven by altruistic motives.

Keywords: personal data, mobility data, personal data management, information privacy, privacy concerns, privacy concerns evaluation

1. Introduction

Westin's "Privacy and Freedom" evoked discussions on information privacy and privacy protection in 1967 during the surveillance technology revolution. Since then, research on information privacy has become increasingly important, along with technological changes that have enabled expanded collection of information about individuals and recording of this information as personal data. With the development of the Internet and the increasing collection of personal data for Internet-

Authors' draft published in Behaviour & Information Technology in 2019; 38:5, 486–502
(https://doi.org/10.1080/0144929X.2018.1540658)

based services, information privacy has evolved into an active socio-technological research area. In the Internet context, privacy research has been typically conducted in online shopping and social networking services. However, application areas of personal data utilisation have expanded to new and distinct domains, such as strongly evolving intelligent traffic systems and services based on personal mobility data. In these applications, personal data collection is typically extensive, continuous and based on monitoring of data subjects' behaviour. These data are collected to produce the service subscribed for by the data subject, rather than for a specific commercial transaction (cf. Junglas, Johnson, and Spitzmüller 2008; Raschke, Krishen, and Kachroo 2014). Legislation has already been forced to respond to privacy challenges raised by technological changes and new application contexts. For example, in the European Union, the General Data Protection Regulation (GDPR) (European Commission 2016) that came into force in 2018 has replaced Data Protection Directive 95/46/EC (DIR95) (European Commission 1995). Initiatives on personal data management with an emphasis on digital human rights have emerged as well (cf. MyData 2017). Therefore, an open question is whether earlier research results remain valid in the new application contexts.

Personal mobility data based on tracking of vehicles and persons are increasingly collected for new types of commercial and governmental applications and can even be made publicly available as open data. Tracking data consist of location data and associated information on the data subject's routes and behaviour, for example. Vehicles' tracking data can be complemented with on-board diagnostic (OBD) data, including speed, revolutions per minute and fuel consumption, to produce rich driving data. Such data can be used for various purposes, such as driving-based taxation, road tolls and commercial driving information services (cf. the Finnish Ministry of Transport and Communications 2013, 2017; 4icom Steer Davies Gleave 2015; OnStar 2016; Traffic Lab 2016). Regarding the collected tracking data about persons, their location data can be complemented with their transportation modes. Personal mobility data of this type can be utilised in future Mobility as a Service (MaaS) concepts that aim to optimise travel time or costs by combining different transportation modes (e.g., maas.global; matka.fi). The mobility data collected from mandatory applications (e.g., driving-based charging) can be complemented with voluntarily disclosed data, provided that the data subjects have explicitly consented to have their data used. These voluntarily disclosed data can be used to produce additional services.

From the practical perspective, understanding changing privacy issues and perceptions associated with new personal data collection domains is highly relevant, specifically to personal data collecting organisations, as these changes often have implications for their data management and usage practices. Due to the GDPR requirements, many of these organisations need to plan and implement new policies and organisational processes, as well as redesign their information systems and data management to respond to new privacy challenges (Tikkinen-Piri, Rohunen, and Markkula 2017; Bird & Bird 2017). In new and evolving service systems, personal data from different sources are typically combined; therefore, data management across various services should be reconsidered.

Data subjects typically worry about the consequences of the different usages of their personal data and the use of erroneous or incomplete data. For example, they may have concerns about who can access their data and to whom their data are disclosed. These privacy concerns may negatively affect the data subjects' willingness to disclose their personal data and consequently, the adoption and usage of services that utilise these data. Privacy concerns can be expected to change with evolving personal data collection contexts and the increasingly comprehensive data collection. As personal data collection becomes part of everyday life and people adapt to the inclusive data collection culture, their attitudes towards data use may change (cf. Nosko, Wood, and Molema 2010). On the other hand, people are increasingly aware of possible privacy issues regarding personal data use due to their continuous exposure to privacy-related news and public discussions (e.g., on the GDPR's new requirements). Furthermore, the consequences of recent privacy breaches show that incidents of this type may cause substantial harm to businesses (cf. Wilcox 2017; Lunden 2017), indicating that privacy still matters to people. In intelligent traffic, privacy concerns are specifically related to mobility data utilisation and often caused by people's reluctance to be monitored since most of them consider tracking their physical location a highly sensitive issue. Human traces are highly distinct; it is relatively easy to identify individuals based on their mobility data (cf. Montjoye et al. 2013). For example, an individual's home can be inferred directly if his or her mobility data are observed regularly. Therefore, the new forms of personal mobility data collection can be expected to have an impact on data subjects' privacy concerns. Privacy will be challenged in new ways due to the increasing use of vehicle and person tracking and on-board data collection technologies, the diverse new usages of the collected data, the possibilities to interlink the data, and complex data collection environments, including different organisations processing the data. For instance, drivers may be worried about their privacy when their data are collected for pay-as-you-drive services, such as a vehicle insurance company determining a customer's driving pattern. On the other hand, public discussions related to mobility data collection are frequent and can be expected to affect people's attitudes towards privacy. For example, privacy concerns may increase when future government services, such as the possibility of driving-based charging, are discussed in public (cf. the Finnish Ministry of Transport and Communications 2017). When privacy concerns are understood in the new context, service providers can respond to users' privacy needs and plan their personal data management accordingly. In this way, mobility data-based services' adoption and usage can be promoted, and their benefits can be reaped.

The adoption and usage of services and technologies that require personal data disclosure (i.e., privacy behaviour) depend not only on data subjects' information privacy concerns but also on their whole cost-benefit consideration of both positive and negative consequences of sharing their data (cf. Acquisti 2009). Based on this 'privacy calculus', data subjects decide whether to disclose their personal information in exchange for certain economic or social benefits (Laufer and Wolfe 1977; Culnan and Armstrong 1999; Li 2012; Kehr et al. 2015). Because data subjects often view their personal data as their private property, they are unwilling to disclose such information without receiving any compensation. However, privacy calculus and its related behaviour are not always this straightforward. For example, Lee et al. (2015) found that monetary rewards offered by data collecting companies do not necessarily promote personal data disclosure in all data collection contexts; instead, the offered compensation may increase privacy concerns and make data subjects worry about the companies' motives. Because data subjects perceive their privacy as having value, it is necessary to take into account their cost-benefit consideration when developing systems that gather personal data. When dealing with voluntary data disclosure related to the usage of mobility data-based services, data subjects' perceived costs can lead to service non-adoption, refusal of information disclosure or limiting it (e.g., by turning off the data collection). If the benefits perceived by the data subjects do not outweigh the costs of the disclosure, the data subjects may also provide false information or omit certain data, hence decreasing the data quality and its completeness (cf. Horne, Norberg, and Ekin 2007; Metzger 2007; Son and Kim 2008). This situation results in decreased amount and coverage of the collected data, as well as lower service quality. In case of mandatory mobility data collection of statutory payment systems (e.g., pay-as-you-drive insurance or road tolls), the data subjects may consciously behave fraudulently. They may falsify their data, resulting in compromised reliability and accuracy of the data.

Understanding data subjects' information privacy concerns and their cost-benefit consideration in evolving personal data collection contexts enables improved systems and service development and helps with finding appropriate data management solutions that are beneficial for both data subjects and data controllers. Knowledge of this kind contributes to the production of personal data intensive services and the implementation of their users' privacy protection in the following ways. When implementing the principles of data protection by design and default (PbD) (cf. Cavoukian 2009) (required by the GDPR, for example), insights into the data subjects' views about their privacy can be utilised. These principles demand a proactive approach to privacy and privacy becoming integral to organisational priorities, project objectives, design processes and planning operations. Specifically, the GDPR advises personal data collecting companies to seek data subjects' views on data processing as part of the data protection impact assessment that it requires. Based on the understanding of the data subjects' privacy concerns, privacy protection and its actual risks can also be efficiently communicated – both to the data subjects and the public in general – through informed consent, audits and external validations of a service, as well as descriptions of fair information practices and the used privacy protection technologies. If the data subjects' cost-benefit consideration is known, they can be encouraged regarding voluntary data disclosure by providing them with control over their information and by offering benefits in return for releasing information (e.g., financial compensation, improved or personalised services or the common good derived from data usage).

The earlier information privacy research is extensive and covers personal information privacy concerns and privacy behaviour related to the use of personal data collecting services, privacy-enhancing technologies (PET), as well as organisational, business and legal aspects of personal data management (cf. Li 2011; Smith, Dinev, and Xu 2011; De Cristofaro and Wright 2013; Dinev, McConnell, and Smith 2015). However, privacy behaviour studies in the context of mobility data-based services are scarce. Additionally, many of the existing studies on privacy concerns and their effect on data disclosure have focused on behavioural intention to disclose personal data, instead of actual data disclosure. Therefore, there is a need for studies on real-world experiences with mobility data disclosure.

This study's objective was to explore whether mobility service users' privacy concerns and privacy behaviour would differ from the findings in the earlier data collection contexts (i.e., Internet and organisational contexts). Differences between these contexts can be expected due to mobility services' increasing use of tracking technologies, the diverse new usages of the collected data, the possibilities to interlink the data, complex data collection environments and frequent public discussions related to mobility data collection. These may affect data subjects' willingness to disclose their data and result in non-adoption of services due to their mobility data privacy concerns and corresponding cost-benefit consideration. In this study, mobility service users' privacy concerns and privacy behaviour were empirically investigated through an explorative multimethod research conducted in a driving data-based mobility service system pilot. The studied system can be considered an example of evolving mobility data-based systems with increasing data collection and utilisation for multiple uses. It investigated what kinds of privacy concerns the mobility service users had, how strong these concerns were and how they changed in the course of service usage. The types of benefits for which mobility service users would like to trade their data (if any) were studied as well. As separate user groups could perceive their cost-benefit considerations in various ways, the differences between the two user groups (private and company users) in the pilot system were investigated. Differences among users can be studied with respect to their personality traits or previous experiences with personal data collecting services (cf. Schrammel, Koffel, and Tscheligi 2009; Quercia et al. 2012; Osatuyi 2015; Bansal, Zahedi, and Gefen 2016). However, this study focused on the distinct user groups involved in the pilot system, instead of personality traits as such. Specifically in mobility services, the purpose of data usage may be an even more determining factor regarding privacy concerns and privacy behaviour.

2. Dimensions of information privacy concerns and how to evaluate them

Several researchers have investigated data subjects' concerns about their personal data disclosure. Different ways to evaluate information privacy concerns have also been proposed. In the beginning of the 1990s, Culnan (1993) surveyed students' attitudes towards the secondary usage of their personal information for the purpose of direct marketing by organisations dealing with commercial transaction data. The students had enrolled in an undergraduate course in information systems in the US, the majority of them having engaged in activities (e.g., subscribing to a magazine or ordering by mail) that resulted in personal data disclosure. Based on the results, Culnan identified a two-dimensional privacy concern construct, comprising loss of control over the information and unauthorised secondary use of the information. A few years later, Smith, Milberg, and Burke (1996) developed and validated an instrument for evaluating individuals' concerns about organisational information practices related to their personal data usage by the companies collecting their data. The authors derived their instrument iteratively from the existing literature, legislation and privacy advocates' writings. For the final validation of the instrument, graduate business students attending four US universities were surveyed. Based on these data, Smith, Milberg, and Burke identified four primary dimensions of data subjects' information privacy concerns. One of these dimensions – secondary use of information, both within an organisation and externally (i.e., disclosing information to another organisation), without the data subjects' authorisation – was similar to the unauthorised secondary use found by Culnan. The three other dimensions noted by Smith, Milberg, and Burke were defined as follows: data collection (i.e., whether data about a data subject are collected excessively), improper access to personal information (i.e., within an organisation, whether an employee without the 'need to know' is able to access personal information stored in the files) and errors in personal data, such as accidental mistakes or obsolete data. Stewart and Segars (2002) further developed Smith, Milberg, and Burke's instrument, aiming at improved comparison, accumulation and synthesis of findings across studies on information privacy. They collected their survey data by using the mall-intercept approach in four US sites (i.e., they approached and interviewed people in these malls). Their study's results suggest that data subjects' information privacy concerns are more complex than previously thought – data subjects are concerned about all of the dimensions of organisational information practices simultaneously, rather than any dimension in particular. The authors also found interrelationships among the separate dimensions, and the control dimension (originally proposed by Culnan) might account for these interrelationships.

In 2004, Dinev and Hart developed and validated an instrument for evaluating information privacy concerns in the Internet context. They based their instrument on Smith, Milberg, and Burke's (1996) dimensions and adapted it to this context. The instrument was validated based on survey data from individuals using the Internet in the US, including students and employees of companies and public sector schools. Dinev and Hart identified two dimensions of privacy concerns: information finding (representing tracking of data subjects' activities and personal information) and information abuse. Their study's results also suggest that control over information disclosure is a separate construct from privacy concerns. Around the same time, Malhotra, Kim, and Agarwal (2004) presented the dimensionality of Internet users' information privacy concerns related to personal information collection in e-commerce. Their results were based on an information provision scenario survey of household respondents using the Internet in the US. Malhotra, Kim, and Agarwal conceptualised privacy concerns as the degree of a data subject's concern about the collection of personal information, the lack of the user's control over the collected information and the user's inadequate awareness of how the collected information would be used. Compared with previous research, the dimension of inadequate awareness of information usage was new. Similar to Stewart and Segars' (2002) suggestion, Malhotra, Kim, and Agarwal proposed a second-order construct for privacy concerns. Castaneda, Montoso, and Luque (2007) continued the development of privacy concerns evaluation in the Internet context. They sought to distinguish between general Internet privacy concerns and e-commerce website-specific privacy concerns. Both concerns were included in their evaluation instrument that they validated by carrying out two studies. The first one was conducted with a convenience sample of undergraduate business students with Internet experience. The second one involved a random sample of e-commerce hypermarket buyers who had previously made an online purchase. Castaneda, Montoso, and Luque identified two privacy concern dimensions: concern for personal information collection and concern for its use. Similar to the recommendations of Stewart and Segars (2002) and Malhotra, Kim, and Agarwal (2004), Castaneda, Montoso, and Luque proposed a second-order construct for privacy concerns evaluation.

The development and the validations of the existing privacy concerns evaluation instruments have led to a decrease in their dimensions in some cases (specifically in the Internet context). However, two dimensions are included in most of the instruments: the extent of the collected data and its secondary use. Variations in the dimensions and their number in the instruments may indicate that the appropriate dimensions to be included in a measurement depend on the data collection context and the related possibilities of data usage and secondary disclosure. Based on the development and the validations of the instruments, some evidence for the interrelationships among the dimensions of privacy concerns has been gathered. It also seems that a separate dimension may account for the interrelationships.

In some studies, the questionnaire items of the privacy concerns evaluation instruments have been tailored to continuous and large-scale data collection contexts (e.g., Xu and Gupta 2009; Raschke, Krishen, and Kachroo 2014). Existing research on privacy concerns evaluation has mainly been conducted in organisational and Internet contexts, the two more established contexts of personal information collection. In the organisational context, the research has focused on privacy concerns related to organisational information management. Regarding the Internet context, the studies have examined the data subjects' cost-benefit consideration related to data disclosure in separate commercial transactions. Both contexts differ from the one explored in this study. As stated by Joinson et al. (2006), it is essential to take into account the context of disclosure regarding costs and benefits, trust, and perceived anonymity and privacy. Some real-setting studies have investigated privacy behaviour and privacy concerns (e.g., Perentis et al. 2017), but it should be noted that in many of the earlier studies, the surveyed people had been students, not necessarily fully representing the real users of personal data intensive services. Therefore, the validity of the existing evaluation instruments for personal mobility data collection, as well as for the current increasingly extensive personal data collection, should be investigated.

3. Research methodology

The objective of this study was to investigate whether data subjects' privacy concerns and privacy behaviour would differ in mobility services compared with the data collection contexts of earlier research. This study also aimed to explore possible differences between separate groups using mobility services, in terms of their privacy concerns and privacy behaviour. The mobility service users' privacy concerns and privacy behaviour were investigated in a mobility service system pilot, referred to as the driving data multiservice system (DMS). The research problem was formulated as four research questions (RQs):

> *RQ1. What are the dimensions of mobility service users' privacy concerns?*
> *RQ2. How strong are mobility service users' privacy concerns?*
> *RQ3. How do mobility service users' privacy concerns change in the course of their service usage?*
> *RQ4. What are the types of benefits for which mobility service users are willing to trade their data?*

For each research question, the groups of private users and company users were compared. In this way, possible differences between these groups, regarding users' privacy concerns and willingness to trade their data, could be identified.

3.1 Driving data multiservice system

The DMS service concept builds on vehicle tracking-based driving data that are collected, managed and processed by a driving data operator. The data collection can be either mandatory or voluntary, and the same data in different forms and combinations can be used for various applications and services. These driving data-based services can include the driver's automatic log, fleet management, vehicle route and driving style information, as well as pay-as-you-drive vehicle insurance. Applications for government services, such as the pay-as-you-drive road toll and taxation, may also be added to the system. The DMS focuses on cooperative and data-sharing aspects, as well as collecting data for possible statutory purposes. The customer, subscriber and vehicle owner using the DMS services can be either a private person or an organisation. In the case of private customers, it is also possible that several drivers use the same vehicle, as common in families. Therefore, in addition to the drivers of a vehicle, other users of the service can access their driving data.

The DMS (Figure 1) can be considered a cooperative information system, consisting of the following general components:

- tracked vehicle, containing on-board equipment (OBE) installed in it,
- driving data operator's information system,
- customer's information system (e.g., driving habit analysis, drive reports for billing claims, fleet management) and
- external (third-party) information systems (e.g., insurance company's system for pay-as-you-drive services, driving-based taxation, road tolls).

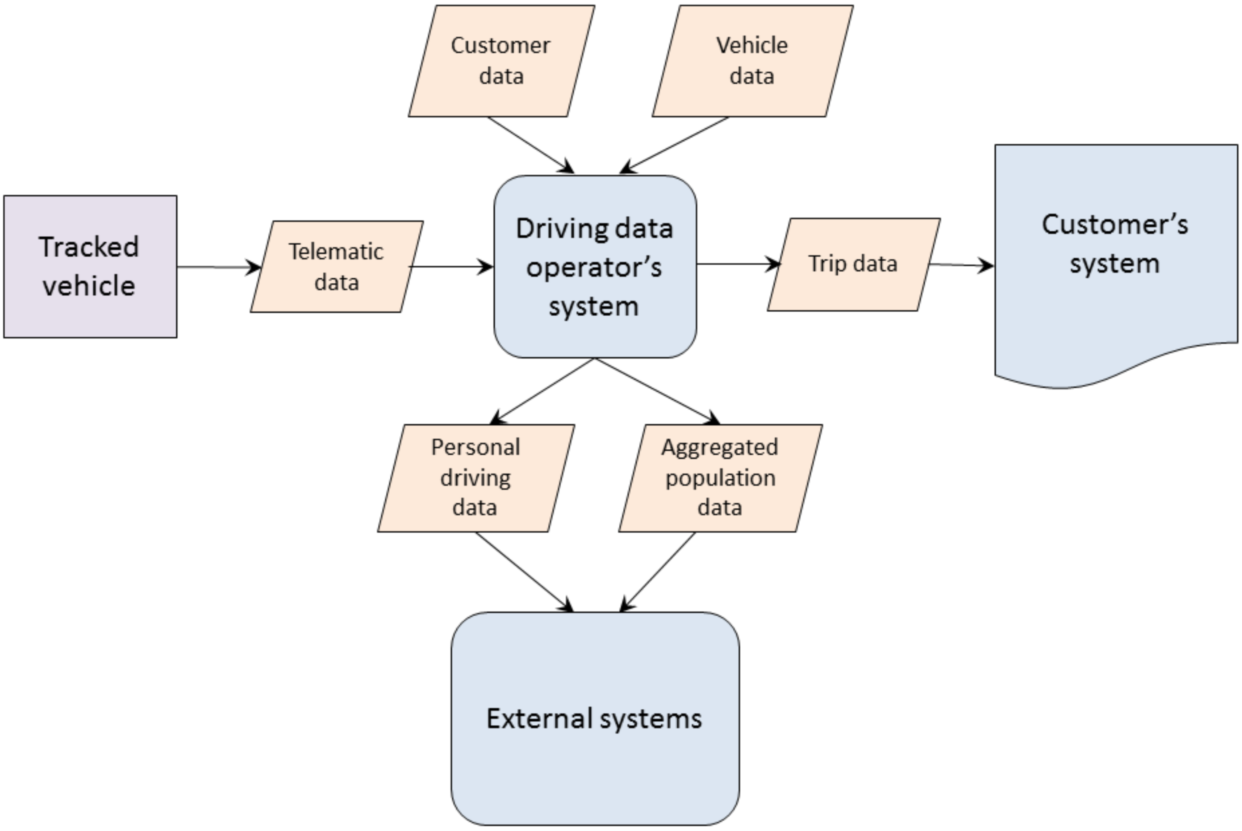

Figure 1. Driving data multiservice system.

The tracked vehicle has an OBE for collecting both the GPS position and the vehicle's on-board sensor data (e.g., fuel consumption). The OBE transmits this raw telematic data to the driving data operator's information system for processing. The vehicle telematic data can be combined with data from other sources (e.g., vehicle information data from the vehicle register), and personal driving data or aggregate data can be produced. The resulting data can be transferred to the customer's own information system. The customer's system can be a company's fleet management system or in the simplest form, the driving data operator's web service accessed by the customer by using his or her own service account. The processed data can also be further shared with external (third-party) information systems, such as an insurance company's system, to produce pay-as-you-drive services.

Each component of the system can include several subcomponents. Some parts of the cooperative system are often in the domain of control of different parties (e.g., the external information systems). The extended DMS systems can include various external systems that send and receive data to and from the driving data operator's system.

Within the driving data operator's system, the following data are collected, used and maintained:

- **Customer data** include the service subscriber, service user, vehicle possessor and vehicle owner. These are personal data or otherwise confidential in nature.

  Data subjects: persons registered in the DMS services, employees of the companies using the DMS services

  Data controller: driving data operator

  Data location: data storage controlled by the driving data operator
- **Telematic data** comprise the data related to the vehicle and its mobility. These are not personal data per se, but in most cases, there is a high probability that the vehicle can be associated with the person(s). In this respect, telematic data can be defined as probable personal data.

  Data subjects: drivers of the vehicles

  Data controller: driving data operator (the data can also be transferred to the customer's own self-controlled system and to third-party systems)

  Data location: OBE and data storage controlled by the driving data operator
- **Other personal data** refer to other personal data related to the vehicle's drivers and passengers.
- **Other non-personal data** pertain to other data, such as geographic data for geocoding driving data and vehicle information data.

3.2 Research setting

The empirical research was conducted in a DMS pilot with a broad base of real users (roughly 500 users). The pilot included an existing commercial driving data operator's service and was part of the national cooperative traffic research programme that was carried out in 2008–2011 in Finland. The users of the pilot represented both private and company customers that were using the service in the whole country. For the research setting, an explorative sequential multimethod approach (cf. Plano Clark and Creswell 2008) was utilised to obtain diverse and comprehensive data on the DMS users' privacy concerns and privacy behaviour. The research consisted of the following three stages: 1) *data controller interviews*, 2) *user interviews* and 3) a *user survey*. Figure 2 presents these stages.

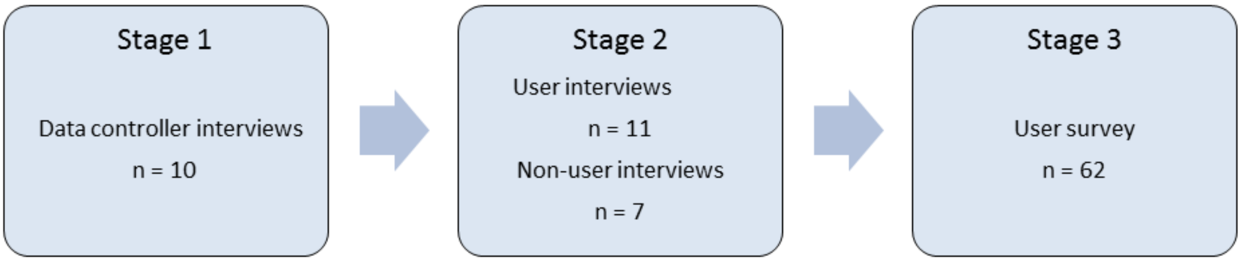

Figure 2. Stages of the research.

The interviews, conducted in Stages 1 and 2, were designed for initial exploration and for gaining an understanding of users' privacy concerns in the studied application context that differed from many of the earlier ones (cf. Lazar, Feng, and Hochheiser 2010). The research then emphasised the user survey and its quantitative results to obtain an extensive view of the target population's privacy concerns (cf. Lazar, Feng, and Hochheiser 2010).

In Stage 1, semi-structured interviews were conducted with representatives of data controller organisations that had prior experience with large systems involving the collection and the utilisation of personal data in the traffic and transportation context. These interviews aimed to obtain insights into the privacy concerns faced by the controllers, as personal data collecting and utilising stakeholders, when dealing with the data subjects (cf. Lazar, Feng, and Hochheiser 2010). The interviews also intended to find out the controllers' personal data usages and ways of managing privacy protection and privacy issues. The obtained knowledge about the data controllers' experiences was tapped to lay the solid, comprehensive and up-to-date foundation for the user interviews and the user survey in the subsequent stages of the research.

In Stage 2, semi-structured interviews were conducted to explore the users' privacy concerns and privacy behaviour in the personal mobility data collection context. In addition to the current users, service non-adopters were interviewed to determine whether privacy concerns had affected their decision about non-adoption. Building on the findings from the data controller interviews, the following was expected about privacy concerns. At least some data subjects, perhaps depending on the user type (private or company user), either had had privacy concerns or had been pondering on privacy protection issues during their adoption or usage of the service. Furthermore, privacy concerns could possibly have affected their decision to use the service. Differences between private and company users were also expected, as it was found that private users were possibly more concerned about their privacy. The results of this stage were used to determine whether the existing privacy concerns evaluation instruments should be further developed for the user survey to be conducted in the mobility data collection context.

In Stage 3, the user survey was designed, building on the findings of the previous stages and the literature on privacy concerns evaluation. Through the survey, the users' privacy concerns, levels of these concerns and changes in them during the use of the service were investigated, as well as users' willingness to trade personal mobility data for various benefits.

In all stages, this study only aimed to collect the information that was necessary to address the research questions. Specifically, it limited the collection of the users' demographic information that could possibly make them identifiable. In this way, the study took into account the confidential nature of the personal mobility data that were collected to produce a real commercial service.

3.2.1 Stage 1: Data controller interviews

In Stage 1 of the research, the representatives of the data controller organisations (n = 10) were interviewed. They were recruited according to the proposal by the research programme's steering group that comprised experts in the intelligent traffic field. The representatives were from government agencies, public bodies and companies that extensively collected or utilised personal data, such as a public transportation provider, the Finnish Transport Safety Agency and the Finnish Ministry of Transport and Communications. The interviews consisted of questions on the following themes: challenges related to data privacy protection (from the perspectives of both the organisation and its employees if the employees were the data subjects), the data subjects' privacy concerns and issues stemming from the use of the system that collected the data, how the data controllers were dealing with privacy issues, how they managed privacy protection and what kinds of plans they had for managing privacy issues.

The interviewers recorded and transcribed all the interviews. The transcription resulted in interview summaries, consisting of the research material organised according to the interview themes. Another interviewer cross-checked the interview summaries to ensure their consistency with the original data.

3.2.2 Stage 2: User interviews

In Stage 2, the DMS user interviews (n = 18) were conducted with the current users (n = 11) and the non-adopters (n = 7). The non-adopters were persons who had shown interest in the service but had decided not to subscribe to it or had quit during the adoption stage. Both user and non-adopter groups included private and company users. The driving data operator provided two lists of interviewee candidates based on their customer register for recruiting the interviewees (one list included users who were possibly willing to be interviewed, and the other included persons who had contacted the company and considered subscribing to the service but finally did not adopt it). The researchers contacted these candidates, who consented to be interviewed. Of the interviewees, 44% were private users, and 56% were company users. The private users were typically most interested in using the driving-style monitoring or just trying out the DMS services. The company users were typically using the driver's log service. They mostly worked for small companies or were private entrepreneurs. Other background information of the interviewees was not collected due to the study's aim to limit the collection of any possibly identifiable personal data. The semi-structured interviews with the users were designed based on the results of the data controller interviews. The interview themes were separately designed for users and non-adopters. The interviews with the current users focused on the interviewees' information privacy concerns and trust in DMS parties, whereas the non-adopter interviews aimed to comprehensively explore the reasons for non-adoption (e.g., in addition to privacy concerns, the non-adopters were asked about the services' added value). The interviews with the current users consisted of questions on whether the user had been pondering on privacy matters (e.g., access to data and data disclosure to third parties) when subscribing to the service or adopting it, whether any doubts had been raised about privacy protection during the use of the service, whether the user's attitudes towards privacy matters had been changed after adopting the service and whether the user trusted the DMS parties. The users were also asked about their future needs for new DMS services. The non-adopter interviews consisted of the following themes: the interviewees' needs and expectations for the added value of the DMS service, their use of alternative services or means to fulfil their needs, the service cost (price and effort) versus the value added, data privacy issues and concerns and their effect on the non-adoption decision, and their perceived trustworthiness of the service provider network.

Similar to the data controller interviews, all the user interviews were recorded. The interviewers transcribed the interviews with the current users, resulting in interview summaries of the research material organised according to the interview themes. Another interviewer cross-checked the interview summaries to ensure their consistency with the original data. The data from the interviews with the non-adopters were arranged in a tabular form, where the research material was organised according to the interview themes.

3.2.3 Stage 3: User survey

In Stage 3, an online survey was conducted among the DMS users. The survey was designed based on the existing literature on information privacy concerns evaluation instruments and the privacy concerns' dimensions (presented in Section 2 of this paper), the legislation on personal data privacy and the results of this study's previous stages. Smith, Milberg, and Burke's (1996) three dimensions of individuals' privacy concerns were utilised, comprising collection, unauthorised secondary use and improper access. Information processing and duration of the information storage – two items covered by EC Privacy Directives 95/46 (European Commission 1995) and 2002/58 (European Commission 2002) – were utilised as well. One context-specific item – combining the driving data with other personal information, identified when conducting the interviews – was also included in the questionnaire. The survey was conducted as part of a more extensive service adoption questionnaire for DMS users to mitigate the possible nonresponse bias due to the disinterest in information privacy.

Finally, based on the dimensions of information privacy concerns, the survey contained questions on users' privacy concerns in the service adoption stage, as follows: what information is collected, how the information is processed, what purposes the information is used for, how long the information is stored, who has access to the information, where the information is disclosed, combining the driving data with other information, and personal concerns about information protection issues (a five-point scale with the choices of 'not at all concerned', 'very little concerned', 'a little concerned', 'much concerned' and 'very much concerned' was used to evaluate the strengths of the separate concerns). The last item was included in the questionnaire to deal with the difference between the users' subjective experience with privacy concerns and just pondering on various privacy issues discussed in public. Furthermore, generic privacy concerns were intended to be evaluated based on the separate dimensions of privacy concerns, except personal privacy concerns. This was done by calculating the sum variable of privacy concerns (the mean of the separate dimensions of privacy concerns) and scaling it similarly to the separate dimensions.

Similar to the DMS interviews, in addition to privacy concerns as such, the change in the concerns during the service use was investigated. The users' cost-benefit consideration were also examined based on the existing privacy behaviour models and the interviewees' identified needs and improvement ideas for future DMS services. This was done by asking about the users' willingness to disclose their personal driving data to gain various benefits, including compensation for user costs, better service, personalised service, services provided by different parties and advanced traffic information services for common use.

A representative of the driving data service operator emailed all its users (approximately 500) a request to participate in the online survey; the e-mail included a link to the questionnaire. The invitation also mentioned that after filling in the questionnaire, the respondents would be offered the opportunity to participate in a prize draw, with a chance to win a first-aid kit. The questionnaire was available for three weeks. Of the users, 62 responded to the survey, yielding a 12.4% response rate. Of the respondents, 16 were private users, and 46 were company users. Half of them used the service daily, one-third used it weekly, and the rest did so monthly or more seldom. About 81% of the respondents were males, and 19% were females. Similar to the user interviews, the collection of the users' demographic information was limited, and no more background information about the users was collected. Despite their high relevance to this research, any customer or vehicle data from the DMS could not be directly utilised. Due to these data's confidential nature, the study could only obtain separate data through the survey. Not all of the respondents gave their answers to every questionnaire item; therefore, the number of responses varied item-wise between 60 and 62.

4. Results

This study aimed to address the research questions through a three-stage multimethod study that explored the users' personal mobility data privacy concerns and privacy behaviour in a DMS pilot. Correspondingly, the results consisted of the findings from all these stages and the stages' contributions to one another.

4.1 Stage 1: Data controller interviews

The data controller interviews revealed that the data subjects with privacy concerns made enquiries to data controllers about privacy protection and the use of their data. Three out of the 10 interviewees reported enquiries of this type. Additionally, one interviewee reported his awareness of this tendency. Notably, not all controllers were collecting personal data by themselves but were utilising the data provided by other organisations. For this reason, they probably had not received direct entries about privacy protection. Regarding the entries, the data subjects might also pose critiques on how privacy protection had been implemented.

> *From time to time, we receive requests from citizens, and they may wonder how our system works. [...] Our mobility data was once used in a police investigation for clearing up a crime (reported in the media). As a result, citizens started to show some concern about their privacy and to request from us information about their personal data protection.* (Representative of a public transportation provider)

> *When getting familiar with the service and considering whether to subscribe to it, they pose questions like 'Will my driving data be delivered to the authorities?' [...] This seems the biggest concern, but also the employers' and family members' access to driving data is enquired about as well.* (Representative of a driving data operator)

The requests to the data controllers show that the data subjects do not necessarily know what personal data are collected about them, for what purposes the information is used, who can access the data in the DMS, and to what parties the information is disclosed and in which form. For example, the data subjects were concerned about whether the privacy of their GPS data could be guaranteed in the services that collected mobility data and in possible driving-based taxation in the future. Specifically, they considered it a possible problem how detailed the collected data were, as well as the possibilities to identify data subjects based on their data.

Three out of the 10 interviewees mentioned about the possible difference between private and company users' privacy concerns. One (a representative of a traffic information service provider) speculated about the forthcoming privacy issues, along with the diffusion of mobility data collection devices in private cars compared with the company vehicles with several drivers. Another interviewee (a representative of a public transportation provider) reported that in the organisation where he worked, privacy concerns had not been shown among professional drivers. Based on these findings, it could be assumed that the private users tend to be more concerned about their information privacy. On the other hand, an interviewee (a driving data operator's representative) pointed out that privacy concerns might arise in the company context due to the possibility that other people in the organisation may access the driving data.

4.2 Stage 2: User interviews

According to the service user interviews, in the service adoption stage, *the majority of the interviewees* (seven out of 11) *had no information privacy concerns or only had minor ones*. For example, a user had pondered on whether somebody had access to his or her information but he or she still thought that the information was not very useful to anybody and was thus not worried about the issue. For example, the users who were apprehensive about privacy protection issues had *concerns related to data disclosure to third parties* and *data access*, either in an authorised or unauthorised way. These users had been thinking about where the data were released, who had access to their data, for what purposes the data were used and whether the authorities monitored the users' driving speed to impose fines.

Contrary to the expectation based on the results of the data controller interviews, *the results* of the user interviews *did not show any clear difference between the user types* – it seemed that private users did not have more concerns. Of the four private users, three had no information privacy concerns or only had minor ones, whereas of the seven company users, four did not have privacy concerns. Some concerns about data disclosure or utilisation by third parties occurred in both groups. Both private and company users also had concerns about access to their data. Privacy concerns stemming from the organisational context (e.g., who had access to employees' driving data in a company) did not appear among the company users during the service adoption stage, perhaps because the interviewees in this group were working at the management level or were private entrepreneurs. However, most of the interviewees representing private users or private entrepreneurs reported increased privacy concerns or had been pondering on privacy issues during their use of the service. Two of these users were concerned about monitoring vehicles and viewing routes, and another two were apprehensive about the use of their data for creating profiles and marketing purposes.

Unexpectedly, *none of the non-adopters considered information privacy concerns critical to the adoption decision*. However, four out of the seven interviewees reported that they had pondered on information privacy issues when making their decision, after reading critical comments in the magazines about privacy problems related to services of this kind and discussing the topic with their friends. Nevertheless, none of the interviewees considered privacy issues problematic in this service.

4.3 Stage 3: User survey

After the survey, a generic and comprehensive view about the data subjects' information privacy concerns was obtained. This was done by calculating the sum variable *generic privacy concerns* as the mean of separate dimensions of privacy concerns (except personal privacy concerns). The analysis of the generic privacy concerns showed that the levels of information privacy concerns varied quite symmetrically among all the classes – from 'not at all concerned' to 'very much concerned' (in other words, the values were relatively normally distributed). There were *no strong tendencies* towards low or high levels of concerns, and the *majority of the users appeared a little concerned about information privacy issues* in the service adoption stage. Figure 3 illustrates this observation by presenting the distribution of the levels of generic privacy concerns.

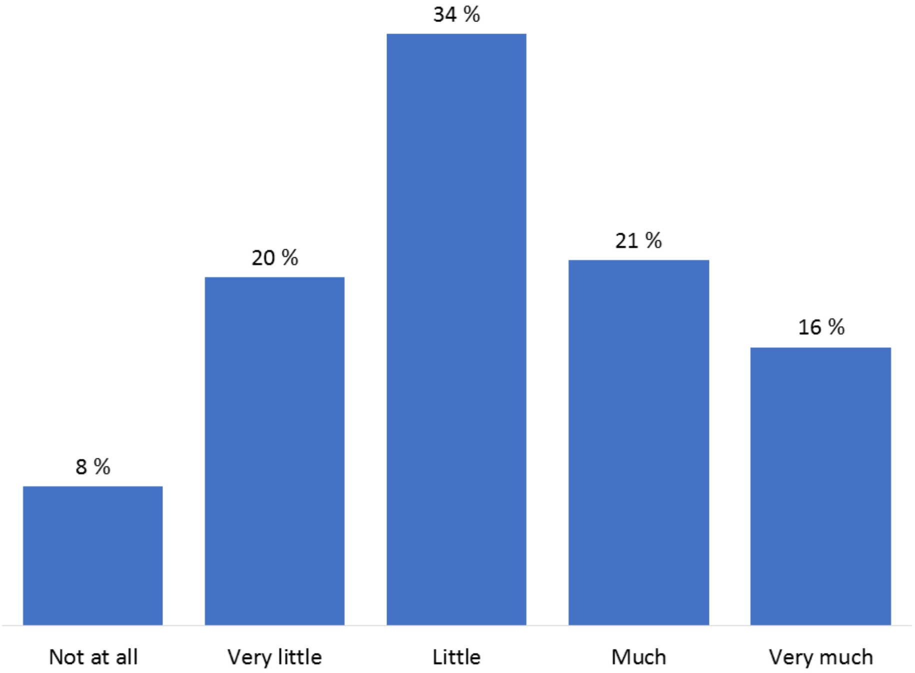

Figure 3. Distribution of the levels of generic privacy concerns.

To study the differences among the separate dimensions of information privacy concerns and to identify the strongest ones, the distributions of their levels were analysed, and their means were calculated. It is noteworthy that based on the data, it seems that the users may be pondering on various information privacy issues but are not necessarily personally worried about their information privacy. Figure 4 illustrates this finding about the difference between specific dimensions of users' privacy concerns and their personal privacy concerns. The figure presents the distributions of the levels of all evaluated dimensions of privacy concerns, generic privacy concerns and personal privacy concerns.

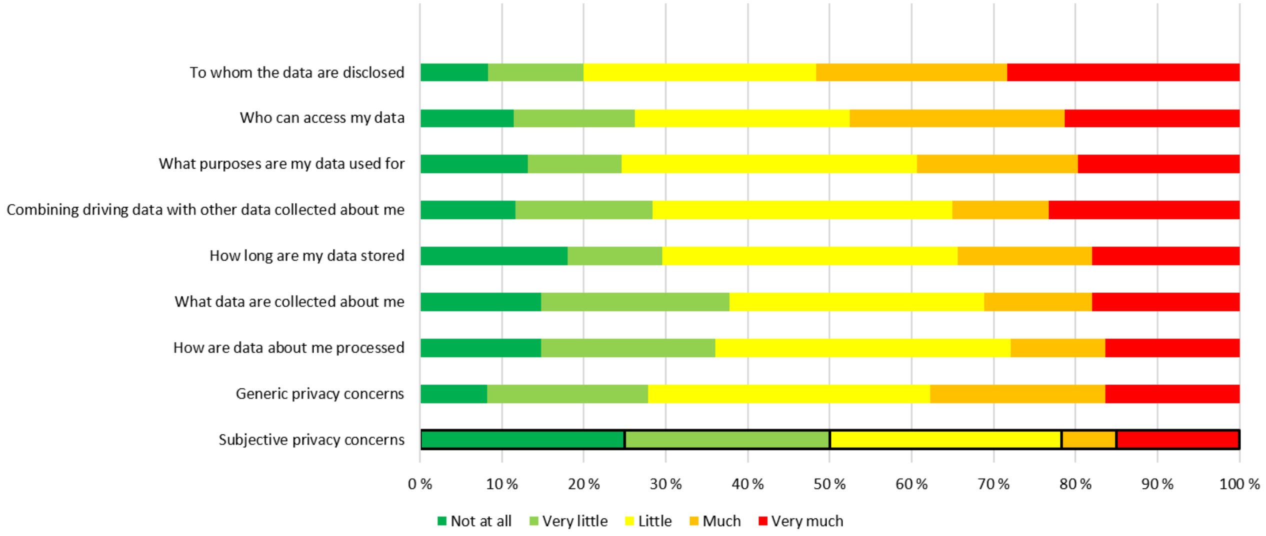

Figure 4. Distributions of the levels of specific privacy concerns, generic privacy concerns and personal privacy concerns.

The service users reported *the strongest information privacy concerns* about the questionnaire statements *'To whom the data are disclosed'* (mean = 3.52, observations concentrated on the high end of the distribution), *'Who can access the data'* (mean = 3.31, observations centred in the middle of the distribution) and '*What purposes the information is used for'* (mean = 3.21, observations centred in the middle of the distribution). These findings are in line with the results of the user interviews. The proportion of private users with strong concerns about these three issues seemed higher compared with the company users. For example, 38% of the private users reported being very much concerned about where their data were disclosed versus 25% of the company users. However, based on the calculation with Pearson's chi-square test of independence, the difference between the user groups was not statistically significant ($\chi^2 = 1.93$, $df = 4$, $p = 0.748$). Similarly, 31% of the private users and 18% of the company users reported being very much concerned about who could access their data. Corresponding to the concerns about data disclosure, the difference between the user groups was not statistically significant ($\chi^2 = 6.67$, $df = 4$, $p = 0.155$). Regarding concerns about what purposes the data were used for, the difference between the groups was also not statistically significant ($\chi^2 = 1.93$, $df = 4$, $p = 0.748$). For the rest of the separate concerns, no significant differences between the groups were indicated as well.

The results also showed that users' *personal information privacy concerns might change during their use of the service* but not necessarily considerably. Small groups of users had either decreased or increased concerns – the percentage of users who reported that their concerns had decreased with time since the service adoption varied concern-wise between 17% and 26%, whereas the percentage of users who reported increased concerns varied between 7% and 14%. The majority of the users reported equivalent concerns about different privacy issues, with the percentage varying concern-wise between 62% and 74%.

The different dimensions (what information is collected, how the information is processed, etc.) of individual users' information privacy concerns had relatively strong correlations. Pearson's correlation coefficients varied between 0.70 and 0.94, and all were statistically significant ($p \leq 0.01$). In other words, *a user with much concern about one dimension of privacy concerns can be expected to be much concerned about other dimensions as well*. This finding is in line with Stewart and Segars' (2002) discovery.

Next, the study revealed how the provision of various benefits as compensation for data disclosure affected the data subjects' willingness to disclose their data. The majority of the benefits listed in the questionnaire were of the privacy calculus type, personally benefiting the user in question and associated with the current DMS, including compensation for service costs, better service, personalised service and services provided by different parties. One of the benefits offered wider usage of the data for the benefit of the general public and was not explicitly related to the current DMS, namely, *advanced traffic information services for common use*. The data subjects seemed *most willing to disclose their data to be compensated for user costs and to receive advanced traffic information services for common use*. Regarding the latter, this is an interesting finding as this kind of service can be considered a common-good type of benefit chosen for *altruistic* motives, different from the conventional privacy calculus benefits that are more *egoistic* by nature.

The private users indicated remarkable willingness to disclose their data compared with the company users. Of the private users, 81% reported their willingness to disclose their data to receive compensation for user costs versus 35% of the company users. Based on the calculation with Pearson's chi-square test of independence, this difference between the user groups was statistically significant (χ^2 = 10.30, df = 1, p = 0.001). Similarly, 75% of the private users indicated their willingness to disclose their data to receive advanced traffic information services for common use compared with 22% of the company customers. Again, the difference between the user groups was statistically significant (χ^2 = 14.71, df = 1, p = 0.000). The difference between the user groups' willingness to disclose their data to obtain personalised services was also statistically significant, although the willingness to disclose was much less in this case. Approximately 38% of the private users and 13% of the company users expressed their willingness to disclose their data in exchange for personalised services (χ^2 = 4.55, df = 1, p = 0.033).

Figure 5 illustrates the difference between private and company users' willingness to disclose their data in the case of advanced traffic information services for common use as compensation.

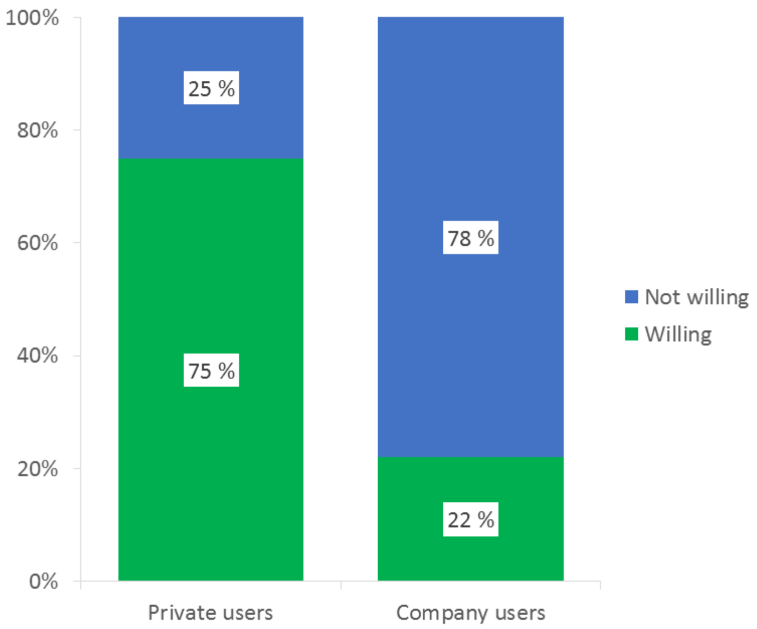

Figure 5. Private and company users’ willingness to disclose data in exchange for advanced traffic information services for common use.

Private users’ strong willingness to disclose their data to be compensated for user costs confirms the expectation based on privacy calculus thinking. On the other hand, their strong willingness to disclose their data to obtain advanced traffic information services for common use is a new finding and may indicate that benefits of data disclosure can also be altruistic. Correspondingly, the remarkable difference between private and company users’ willingness to disclose their data is an important finding to take into account when discussing provision of benefits as compensation for data disclosure.

5. Discussion

Data subjects’ privacy concerns stemming from increasing collection and use of mobility data may affect their willingness to disclose their data and hence lead to non-adoption of services, decline in data disclosure, decrease in data quality and incompleteness of data. For this reason, this study investigated mobility service users’ privacy concerns and privacy behaviour. The study’s results were then examined relative to the earlier data collection contexts. It found that the majority of the users were concerned about their privacy to some extent. A small group of users also expressed strong concerns about their privacy; symmetrically, a small group of users was not concerned about privacy or only had minor concerns. These findings roughly correspond with the results of Westin’survey (conducted in 2003) that used a privacy orientation index that classified respondents as privacy fundamentalists, privacy pragmatists and privacy unconcerned (Kumaraguru and Cranor 2005). In Westin’s study, the data collection context was unspecified; instead, the questionnaire statements just referred to companies as data collectors. In this light, data subjects’ levels of privacy concerns in the mobility data collection context seem similar to those in the earlier data collection contexts.

The research results indicate that a larger segment of the studied population did not have *personal privacy concerns* compared with the separate dimensions of information privacy concerns and generic privacy concerns. This difference may be related to the *privacy paradox* phenomenon discussed at the end of this section. The large number of service users with no personal concerns about their privacy may also be explained by their trust in some parties of the piloted service system or their familiarity with the services utilising their personal data. Contrary to expectations, the differences in privacy concerns were not explained by user group. Some slight differences observed between private and company users regarding their concerns were not statistically significant. Pell, Starkl, and Menrad (2012) noted a corresponding finding about road users' acceptance of mobility data collection via company-owned and private cars. However, their study did not report any statistical significance of the difference. It is still natural to expect differences caused by varying roles of mobility service users. For example, it is often easier to accept work-related data collection when it is a prerequisite for performing tasks.

The users reported the strongest concerns about the following dimensions of privacy concerns: *data disclosure to third parties*, *data access* and *data usage purpose*. The detected dependencies between the privacy concerns' dimensions indicate that a user who expresses concerns about privacy is typically worried about most of its dimensions. These results are consistent with those of the earlier research on information privacy concerns evaluation instruments. In contrast, a new finding indicates a dimension that is not yet included in the existing evaluation instruments, specifically, *concerns about combining driving data with other personal information*. It is highly relevant to the privacy concerns evaluation in mobility services as data subjects' perceived risks of interlinking the data are increased due to tracking of their spatiotemporal behaviour. Overall, it seems that the dimensions included in the existing privacy concerns evaluation instruments remain valid in the mobility data collection context but need to be complemented with new context-specific dimensions.

Future intelligent traffic and personal mobility innovations depend on the wide acceptance and adoption of new mobility data-based services. Users' increasing privacy concerns may result in non-adoption or dropping out of these services. Therefore, this study investigated *privacy concerns' effect on service adoption* and the *change in privacy concerns, along with the experience with service usage*. Contrary to expectations, the results showed that privacy concerns did not affect drivers' decision to adopt the service. Instead, other factors (such as the added value of the DMS services) were emphasised in their decision making. For the majority of the users, their levels of concerns remained the same during their use of the service, but there was a small number of users whose *privacy concerns slightly decreased or increased in time after their service adoption*. Although the changes in privacy concerns were not that common, a significant observation was that they might be bidirectional, that is, users could become less or more concerned in the course of their experience with the service. This finding can possibly be explained by the mobility data collection environment's complexity and the users' lack of awareness about its processing operations in the beginning of their service usage. When they gain experience with their service usage and an understanding of the underlying system, privacy concerns may decrease; on the other hand, new questions about privacy may also be raised. Concerning the two user segments (private and company users), no differences were found in the changes in their levels of concerns. All these results have several practical implications for the provision of mobility data-based services. It should be taken into account that the use of the service does not necessarily decrease privacy concerns. Instead, concerns may increase when the users become aware of the possible issues in data collection, such as secondary use of the data. Based on this finding, dropping out can be prevented by informing users about the actual risks of data disclosure. Regarding potential users with decreasing privacy concerns, it is important to offer them opportunities to try the service and gain experience with its usage to promote service adoption. From the theoretical perspective, the finding about the bidirectional change in privacy concerns is highly relevant, especially when dealing with empirical privacy behaviour models describing data subjects' disclosure behaviour.

To evaluate information privacy concerns in a valid manner, it is vital to distinguish users' personal privacy concerns from just pondering on privacy issues that arise, for example, after following a public discussion on privacy protection. This study investigated possible differences between such pondering and mobility service users' personal privacy concerns. It seems that *although they ponder on privacy issues, users may not necessarily be personally worried about their information privacy*. No differences were found between private and company users in this respect. The difference between pondering on information privacy and personal privacy concerns possibly reflects the *privacy paradox* phenomenon (cf. Acquisti, Brandimarte, and Loewenstein 2015), indicating that despite expressing concerns, data subjects do not necessarily limit their data disclosure. People's attitudes towards privacy may be affected, for example, by public discussions on privacy issues, but they are neither really worried about their privacy nor change their privacy behaviour. Acquisti, Brandimarte, and Loewenstein presented other explanations for the privacy paradox resulting from the data subjects' bounded rationality in their decision making, including misperceptions of the costs and the benefits of data disclosure, social norms, emotions and heuristics. Specifically, the aspects related to misperceptions and heuristics are relevant to future mobility data-based services due to the complex nature of the underlying systems with various data processors. Regarding different types of privacy concerns, Li (2014) identified the following three levels of privacy beliefs: general privacy concerns, situational privacy concerns and disposition to privacy. These differ from one another in scope, stability and behavioural outcomes. The differences between pondering on privacy issues and personal privacy concerns may also be explained by conceptualisation of this type. The observed differences between them have important implications for privacy concerns evaluation and the development of evaluation instruments that do not commonly deal with personal privacy concerns. Therefore, further investigation is needed on the relationship between pondering on privacy issues and personal privacy concerns, also in contexts other than mobility data collection.

Because personal data are often considered private property, data subjects may expect to receive some benefits as compensation for disclosing their data. To provide an understanding of data subjects' cost-benefit consideration in mobility services, this study investigated the types of benefits for which the users were willing to trade their data. The study's results emphasise the effect of benefits, offered as compensation for data disclosure, on users' willingness to disclose their mobility data. This finding supports traditional privacy calculus thinking. However, it is possible that benefits even play a more important role in personal data disclosure in mobility data collection compared with the earlier contexts. The results further suggest that in addition to *egoistic benefits* (e.g., financial compensation), mobility service users are willing to exchange their data for *altruistic benefits* (e.g., services for common use). This aspect is not considered in the traditional privacy calculus, with its focus on the costs and the benefits of data disclosure that are realised personally by data subjects. Future traffic-related applications and information services, such as MaaS systems, may afford many possibilities to gather personal mobility data on a voluntary basis, as well as to produce various services based on the collected data. For this reason, it is important to account for different types of benefits when planning the mobility data collection. For example, if enough users are willing to trade their data for producing traffic information services, it will not be problematic if the users with high privacy concerns prefer to withhold their data. Regarding the differences between the attitudes of the user segments, it seems that *private users may be more willing to disclose their data to gain benefits* compared with company users. This finding may be related to the possibility that many company users drive company-owned cars. For this reason, personalisation or cost compensation may not work for them as opposed to private users. Company users also showed low willingness to disclose their data on altruistic grounds compared with private users. Overall, the results suggest that to promote the disclosure of mobility data, *in addition to financial benefits or services for personal usage, it is advisable to offer customers the possibilities to disclose their data for the common good (e.g., to produce traffic information services for common use)*. Furthermore, the findings on the differences between the user segments are highly relevant when launching new personal mobility data-based services because the results can guide the development of compensation options matching the preferences of different user segments. First, benefits that are perceived useful specifically by private users should be identified and offered as compensation. According to the results, these benefits could be compensation for user costs and advanced traffic information services for common use. Understanding private users' altruistic preferences also makes voluntary open data collection feasible, enabling the development of open data-based services. Second, it is important to seek compensation options matching company users' preferences to promote their data disclosure. It would also be useful to investigate how company users could be motivated to share their information for the production of services that return value to other users. The adoption of practices that make information sharing more secure and transparent could help in such motivation. For example, the principles of the MyData (2017) initiative's human-centric approach to personal data could be followed.

The research conducted resulted in some new and unexpected findings on information privacy concerns, significant specifically for the development of mobility services and privacy concerns evaluation instruments. The results suggest that data subjects' cost-benefit consideration related to their data disclosure is not necessarily as straightforward as described in the previous models. This implies that data subjects' views about the costs and the benefits of the disclosure should be carefully investigated and analysed when developing new systems and services that collect personal data and when planning their data management. In the light of the results, the idea of how to correctly evaluate privacy concerns should also be revised.

6. Conclusion

The objective of this study was to investigate whether data subjects' privacy concerns and privacy behaviour would differ in the mobility data collection context compared with the earlier data collection contexts. Privacy concerns and privacy behaviour related to mobility data collection can be expected to differ from the Internet and organisational contexts due to the increasing use of tracking technologies, the diverse new usages of mobility data, the possibilities to interlink the data, complex data collection environments with different organisations processing the data and frequent public discussions about mobility data collection. This study explored differences between data collection contexts through examination of mobility service users' privacy concerns and their role in service adoption, as well as by investigating mobility service users' cost-benefit consideration as representing their data disclosure behaviour and hence helping to offer benefits valuable to them as compensation for disclosure. Separate user groups may perceive their cost-benefit considerations in different ways. For this reason, possible differences between private and company users' privacy behaviour were examined by comparing these groups. Empirical research was conducted in a DMS pilot through an explorative multimethod approach consisting of data controller interviews, user interviews and a user survey, with an emphasis on the third method. The knowledge gathered from the interviews was utilised to adjust the existing privacy concerns evaluation instruments to the survey questionnaire in order to specifically evaluate personal mobility data privacy concerns.

The user survey results show that the majority of the mobility service users are either slightly concerned about their privacy or have been pondering on privacy issues related to mobility data collection. Despite the latter consideration, it seems that users are not necessarily personally worried about their privacy. This observation can be explained by the *privacy paradox* phenomenon. Regarding privacy concerns evaluation in the mobility data collection context, indication was found of a new context-specific dimension – *concerns about combining driving data with other personal information*. This finding suggests the need to revise and complement the existing privacy concerns evaluation instruments when used in new contexts. The levels of privacy concerns remained the same for the majority of the users during their service use. However, there was a small group of users whose privacy concerns either slightly decreased or increased after service adoption. This bidirectional change is of practical importance regarding information provision to mobility service users during their service adoption. Theoretically, it is relevant to the development of privacy behaviour models that describe data subjects' data disclosure behaviour. In line with the privacy calculus theory, the data subjects are willing to disclose their mobility data for compensation of user costs (i.e., they want to benefit personally from the disclosure). Unexpectedly, the data subjects are also willing to disclose their data for the common good. This means that data disclosure benefits can also be *altruistic* in contrast to conventional and often more *egoistic* privacy calculus benefits. Overall, private users seem remarkably more willing to trade their data for benefits compared with company users.

The empirical research was conducted in a DMS pilot that could be considered an example of the evolving mobility data-based systems with extensive data collection and utilisation for multiple purposes across different services. Therefore, the pilot afforded an opportunity to explore mobility service users' views on their personal data collection and corresponding privacy concerns. The data subjects were real service users of the pilot and subscribers of the driver's automatic log and fleet management services, for example. This kind of pilot provided a sound setting for the study, in contrast to many privacy behaviour studies with student samples or experimental research settings. However, some limitations should be borne in mind when interpreting the results. The survey sample size was relatively small due to the limited number of users in the pilot. Nonetheless, the survey request was sent to the whole population of service users, instead of a more limited random or a convenience sample that are commonly used. Furthermore, over 10% of the users subscribing to the service during the survey gave their responses. Due to the limited population, the generalisability of the results should be considered with respect to the country in question because the data subjects' privacy concerns and privacy behaviour depend on both cultural and political contexts. Many of the pilot service users were also possibly early adopters interested in new technologies and open to trying them. Users of this kind may have a better understanding of the data collection context and awareness of its actual privacy risks compared with average users. On the other hand, they may also be more willing to take risks regarding their personal mobility data processing. Therefore, if the study would be replicated with a different user population, the results could differ from those presented here.

This study has identified several starting points for future empirical research. The research has generated some unexpected findings, not yet reported in earlier research. First, the results show that the way in which information privacy concerns have been evaluated so far does not necessarily reflect data subjects' personal privacy concerns. The existing privacy concerns evaluation instruments do not distinguish between pondering on various aspects of information privacy and personal privacy concerns. This finding should be taken into account when further developing privacy concerns evaluation, as well as empirical privacy behaviour models. Second, the available evaluation instruments do not necessarily include dimensions that are specific to new data collection contexts. Therefore, there is a need to revise the earlier instruments for their valid use in the future. Third, an interesting observation reveals a data disclosure benefit of an altruistic nature in the mobility data collection context where traffic information services for common use can be produced based on the disclosed data. It could be fruitful to investigate data subjects' willingness to disclose their personal data for altruistic benefits in different contexts. For example, in the healthcare sector, altruistic benefits could be available by offering data subjects the possibility to share their personal health and fitness data for the purpose of investigating diseases and their treatments. Regarding the limited generalisability of the results, cross-sectional studies are needed to investigate differences in personal mobility data privacy concerns and privacy behaviour by country. Mobility services with established user populations should be studied as well. Overall, future mobility data-based services where personal mobility data would be shared among multiple organisations would bring new data management challenges and would thus require context-specific privacy concerns evaluation. Current personal mobility data collection contexts, such as MaaS systems, are rapidly evolving, pointing to the necessity for continuous monitoring of data subjects' views on their privacy in these contexts.

Acknowledgements

This work was financially supported by the Finnish Foundation for Technology Promotion and the Tauno Tönning Foundation. The empirical data used in this study were collected via the Cooperative Traffic research programme, funded by Tekes and a consortium of companies.

Disclosure of interest

The authors report no conflict of interest.

References

4icom Steer Davies Gleave. 2015. *Study on "State of the Art of Electronic Road Tolling"*. http://ec.europa.eu/transport/sites/transport/files/modes/road/road_charging/doc/study-electronic-road-tolling.pdf

Acquisti, A. 2009. "Nudging Privacy: The Behavioral Economics of Personal Information." *IEEE Security & Privacy* 7 (6): 82–85.

Acquisti, A., L. Brandimarte, and G. Loewenstein. 2015. "Privacy and Human Behavior in the Age of Information." *Science* 347 (6221): 509–514.

Bansal G., F. M. Zahedi, and D. Gefen. 2016. "Do Context and Personality Matter? Trust and Privacy Concerns in Disclosing Private Information Online." *Information & Management* 53 (1): 1–21.

Bird & Bird. 2017. *Guide to the General Data Protection Regulation*. https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf

Castaneda, J. A., F. J. Montoso, and T. Luque. 2007. "The Dimensionality of Customer Privacy Concern on the Internet." *Online Information Review* 31 (4): 420–439.

Cavoukian, A. 2009. *Privacy by Design: The 7 Foundational Principles*. Ontario: Information and Privacy Commissioner of Ontario, Canada.

Culnan, M. J. 1993. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use." *MIS Quarterly* 17 (3): 341–363.

Culnan, M. J., and P. K. Armstrong. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science* 10 (1): 104–115.

De Cristofaro, E., and M. Wright, eds. 2013. *Privacy Enhancing Technologies. Proceedings of 13th International Symposium, PETS 2013*. Bloomington, IN: Springer.

Dinev, T., and P. Hart. 2004. "Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model." *Behaviour & Information Technology* 23 (6): 413–422.

Dinev, T., A. R. McConnell, and H. J. Smith. 2015. "Research Commentary–Informing Privacy Research through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the 'APCO' Box." *Information Systems Research* 26 (4): 639–655.

European Commission. 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data." *Official Journal L* 281, 23/11/1995: 0031–0050.

European Commission. 2002. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)." *Official Journal L* 201, 31/07/2002: 0037–0047.

European Commission. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing the Directive 95/46/EC (General Data Protection Regulation)." *Official Journal L* 119, 04/05/2016.

Finnish Ministry of Transport and Communications. 2013. *Working Group Chaired by Mr Jorma Ollila: Towards Kilometre-based Taxation*. Press release. http://www.lvm.fi/pressreleases/4374272

Finnish Ministry of Transport and Communications. 2017. *Corporate Model Would Resolve Transport Network Funding*. Press release. https://www.lvm.fi/en/-/corporate-model-would-resolve-transport-network-funding-919989

Horne, D. R., P. A. Norberg, and A. C. Ekin. 2007. "Exploring Consumer Lying in Information-based Exchanges." *Journal of Consumer Marketing* 24 (2): 90–99.

Joinson, A. N., C. Paine, U.-D. Reips, and T. Buchanan. 2006. "Privacy and Trust: The Role of Situational and Dispositional Variables in Online Disclosure." *Workshop on Privacy, Trust and Identity Issues for Ambient Intelligence.*

Junglas, I. A., N. A. Johnson, and C. Spitzmüller. 2008. "Personality Traits and Concern for Privacy: An Empirical Study in the Context of Location-based Services." *European Journal of Information Systems* 17 (4): 387–402.

Kehr, F., T. Kowatsch, D. Wentzel, and E. Fleisch. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus." *Information Systems Journal* 25 (6): 607–635.

Kumaraguru, P., and L. F. Cranor. 2005. *Privacy Indexes: A Survey of Westin's Studies*. Technical Report. Pittsburgh, PA: Carnegie Mellon University.

Laufer, R. S., and M. Wolfe. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory." *Journal of Social Issues* 33 (3): 22–42.

Lazar, J., J. H. Feng, and H. Hochheiser. 2010. *Research Methods in Human-Computer Interaction*. Chichester: Wiley.

Lee, H., D. Lim, H. Kim, H. Zo, and A. P. Ciganek. 2015. "Compensation Paradox: The Influence of Monetary Rewards on User Behavior." *Behaviour & Information Technology* 34 (1): 45–56.

Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework." *Communications of the Association for Information Systems* 28: 453–496.

Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework." *Decision Support Systems* 54 (1): 471–481.

Li, Y. 2014. "A Multi-level Model of Individual Information Privacy Beliefs." *Electronic Commerce Research and Applications* 13 (1): 32–44.

Lunden, I. 2017. "After Data Breaches, Verizon Knocks $350M off Yahoo Sale, Now Valued at $4.48B." *TechCrunch,* February 21. https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/

Maas.global. 2016. http://maas.global/maas-as-a-concept/

Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale and a Causal Model." *Information Systems Research* 15 (4): 336–355.

Matka.fi. Accessed 10 March 2017. https://opas.matka.fi/

Metzger, M. J. 2007. "Communication Privacy Management in Electronic Commerce." *Journal of Computer-Mediated Communication* 12 (2): 335–361.

Montjoye de, Y.-A., C. A. Hidalgo, M. Verleysen, and V. D. Blondel. 2013. “Unique in the Crowd: The Privacy Bounds of Human Mobility.” *Scientific Reports* 3: 1–5.

MyData. 2017. MyData Declaration. https://mydata.org/declaration/

Nosko, S., E. Wood, and S. Molema. 2010. “All about Me: Disclosure in Online Social Networking Profiles: The Case of Facebook.” *Computers in Human Behavior* 26 (3): 406–418.

OnStar. Accessed 28 November 2016. https://www.onstar.com/us/en/home.html

Osatuyi, B. 2015. “Personality Traits and Information Privacy Concern on Social Media Platforms.” *Journal of Computer Information Systems* 55 (4): 11–19.

Pell, A., F. Starkl, and M. Menrad. 2012. “A Field Study on the Acceptance of Extended Floating Car Data for Real-time Monitoring Traffic Conditions.” *2012 IEEE International Symposium on Sustainable Systems and Technology*. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6227986

Perentis, C., M. Vescovi, C. Leonardi, C. Moiso, M. Musolesi, F. Pianesi, and B. Lepri. 2017. “Anonymous or Not? Understanding the Factors Affecting Personal Mobile Data Disclosure.” *ACM Transactions on Internet Technology* 17 (2): 13:1–13:19.

Plano Clark, V. L., and J. W. Creswell. 2008. *The Mixed Methods Reader*. Thousand Oaks, CA: Sage Publications.

Quercia, D., D. B. L. Casas, J. P. Pesce, D. Stillwell, M. Kosinski, V. A. F. Almeida, and J. Crowcroft. 2012. “Facebook and Privacy: The Balancing Act of Personality, Gender, and Relationship Currency.” In *Proceedings of the Sixth International Conference on Weblogs and Social Media*, 306–313. Palo Alto, CA: AAAI Press.

Raschke, R. L., A. S. Krishen, and P. Kachroo. 2014. “Understanding the Components of Information Privacy Threats for Location-based Services.” *Journal of Information Systems* 28 (1): 227–242.

Schrammel, J., C. Koffel, and M. Tscheligi. 2009. “Personality Traits, Usage Patterns and Information Disclosure in Online Communities.” In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, 169–174. Swindon: British Computer Society.

Smith, H. J., T. Dinev, and H. Xu. 2011. “Information Privacy Research: An Interdisciplinary Review.” *MIS Quarterly* 35 (4): 989–1015.

Smith, H. J., J. S. Milberg, and J. S. Burke. 1996. “Information Privacy: Measuring Individuals’ Concerns about Organizational Practices.” *MIS Quarterly* 20 (2): 167–196.

Son, J. Y., and S. S. Kim. 2008. “Internet Users’ Information Privacy-Protective Responses: A Taxonomy and a Nomological Model.” *MIS Quarterly* 32 (3): 503–529.

Stewart, K. A., and A. H. Segars. 2002. “An Empirical Examination of the Concern for Information Privacy Instrument.” *Information Systems Research* 13 (1): 36–49.

Tikkinen-Piri, C., A. Rohunen, and J. Markkula. 2017. “EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies.” *Computer Law & Security Review: International Journal of Technology Law and Practice* 34 (1): 134-153. doi: 10.1016/j.clsr.2017.05.015

Traffic Lab. 2016. #Trafficlab. https://www.trafficlab.fi/

Westin, A. 1967. *Privacy and Freedom*. New York: McClelland & Stewart.

Authors’ draft published in Behaviour & Information Technology in 2019; 38:5, 486–502
(https://doi.org/10.1080/0144929X.2018.1540658)

Wilcox, P. 2017. “The True Impact of a Cyber Breach on Share Price.” *Computer Weekly,* March. http://www.computerweekly.com/opinion/The-true-impact-of-a-cyber-breach-on-share-price

Xu, H., and S. Gupta. 2009. “The Effects of Privacy Concerns and Personal Innovativeness on Potential and Experienced Customers’ Adoption of Location-based Services.” *Electronic Markets* 2 (19): 137–149.