Location Privacy Preferences: A Survey-Based Analysis of Consumer Awareness, Trade-off and Decision-Making

Authors:

Dr. Caitlin D. Cottrill (Corresponding Author), Lecturer
University of Aberdeen
School of Geosciences
Elphinstone Road
Aberdeen, Scotland, UK AB24 3UF
Phone: +44 (0)1224 273694
c.cottrill@abdn.ac.uk

Dr. Piyushimita "Vonu" Thakuriah, Halcrow Chair of Transportation
Director, UK ESRC Urban Big Data Centre
University of Glasgow
Glasgow, G12 8RS, UK
Phone: +44 (0) 141 330 4079
Piyushimita.Thakuriah@glasgow.ac.uk

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

Keywords:
Location Privacy, privacy-utility trade-off, willingness-to-trade privacy, risk

1. Introduction

One of the most well-known definitions of privacy is "the right to be left alone", as set forth by Warren and Brandeis in their 1890 Harvard Law Review article, "The Right to Privacy." In ensuing years, however, such a broad conception of privacy has proven insufficient, particularly as technologies allowing for the near-continuous monitoring of our actions, behaviors, and preferences have multiplied, and methods and techniques for cataloguing and mining this data have increased in both power and scope. In part, Warren and Brandeis's conception was constructed upon the foundation of *personal* (or physical) privacy. Smith, *et al.* (2011) differentiate between information and personal privacy, stating that, "The latter concerns physical access to an individual and/or the individual's surroundings and private space; the former concerns access to individually identifiable personal information." Given the advent of widely distributed sensor equipped personal mobile devices such as smartphones, concerns around information privacy are quickly mounting. For example, a 2012 Pew Research Report found that of those Americans with application ("app") enabled cellular phones, over half had either decided not to install or uninstalled an app due to personal information concerns (Boyles et al., 2012). Such findings have brought information privacy to the forefront of concern, and made it necessary to determine more concretely how consumers view the value of their personal information, and under what circumstances they are willing to trade this private information for benefits and services. The complexity of this task is illustrated by Pavlou (2011), who states that, "…much ambiguity and disagreement still surrounds the concept of information privacy. This is because information privacy is an arguably complex concept that can be studied from many perspectives, including law, economics, psychology, management, marketing, and Information Systems." In addition, as elaborated below, preferences regarding information privacy are also arguably contingent upon both contextual and personal circumstances – they should not be conceptualized as static.

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

2. Background

2.1 Technical Methods of Privacy Protection

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

2.2 Conceptualizing Privacy: Context and preferences

As noted above, privacy as a concept has many definitions, but key components tend to be issues of control and flow of information. Westin (2003), for example, has defined privacy as, "the claim of an individual to determine what information about himself or herself should be known to others." This definition contains veiled reference to one of the complicating considerations of privacy: namely, the context in which information sharing should take place. As Nissenbaum (2010) states, "…a right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information." This concept of appropriateness specifically introduces the idea of context, as it raises the claim that norms of privacy may differ depending upon who is on the receiving end of the flow of information, the type of information to be shared, and the uses to which shared information will be put. The concept of this structure of privacy has been called *contextual integrity* (Nissenbaum 2010, Zimmer 2008), and it is particularly relevant to discussions of privacy in the transport realm. The use context of location-sensing technologies vary with great rapidity, whether on the public roadway, in a place of business, or in one's own home, and in each case, the context of use may influence and impact the expectations that a user has in relation to his data being collected, shared, and employed.

By approaching the privacy claim from the viewpoint of context, emerging literature on economic variations inherent in the valuation of information privacy reveal a range of expectations dependent upon the person's individual understanding. The concept of privacy as based upon a subjective or contextually-based understanding is consistent with legal framing of the subject – for example, the Fourth Amendment, central to legal justifications for privacy protection in the United States, has been understood by the courts to be centered on "reasonable expectations of privacy" (Slobogin, 2003). For purposes of this paper and the survey instrument, we take the viewpoint that privacy is a contextually based concept, with ramifications for both adoption and economic valuation within the realm of location services.

Another contextual point is that of the person under consideration. As noted in Korzaan and Boswell (2008), in which they expanded upon work conducted by Stewart and Segars (2002), a person's individual characteristics may have an influence on his or her concern for privacy. Stewart and Segars take a multidimensional approach, using the Concern for Information Privacy (CFIP) instrument developed by Smith et al. (1996) reflecting four factors of concern in information privacy: collection, errors, secondary use, and unauthorized access. This construct suggests that, "individuals with a high concern for information privacy perceive that: (1) too much data are collected, (2) much of the data is inaccurate, (3) corporations use personal information for undisclosed purposes, and (4) corporations fail to protect access to personal information" (Stewart and Segars, 2002). Using a survey of 400 consumers, Stewart and Segars assessed if the posited construct adequately reflected information privacy concerns, with findings indicating that these four factors likely function as second-order factors, subject to a larger theme such as consumer control of information or procedural fairness. In expanding these factors, Korzaan and Boswell (2008) used an examination of the 'Big Five' personality factors (extraversion, agreeableness, conscientious, emotional stability, and openness to new experiences) as described in (Gosling et al., 2003a) to assess their potential influence on CFIP, finding that 'agreeableness' had a significant influence on information privacy concerns. Due to limitations of the sample tested, it was recommended that further assessment of these factors be conducted to determine if there are further influences. In this study, we include an examination of these factors to further assess the potential impacts of personality characteristics on location information privacy preferences, in order to more fully contextualize potential concerns.

2.3 Dissemination of Smart Mobility ICTs

While technologies have advanced to allow for real-time information to be collected, shared, and used, and applications (or "apps") can be used for social networking and wayfinding, without widespread adoption these ICT systems do not necessarily have the data inputs to function effectively. In particular, unlike ITS projects, which are generally adopted at the systemic level by agencies for the purpose of system management and then passed down to the consumer, LBS adoption generally takes place at the level of the consumer; thus, their benefits must be clearly apparent to individual users. The range of LBS available and the manner in which they allow adopters to interact with their social networks and the space around them begins to demonstrate why LBS have grown rapidly in adoption in recent years. A recent report from the Pew Research Internet Project (Zickuhr, 2012) found that:

- 74% of adult (18+) smartphone owners use their phone to get directions or other information based on their current location;
- Among social media users aged 18+, 30% report that at least one of their accounts is set to include their location in posts, an increase from 14% in 2011; and
- 12% of smartphone owners aged 18+ use a geosocial service to “check in” to locations or share their location with friends, down from 18% in early 2012.

The emergence and seeming ubiquity of such technologies has revealed a plethora of data collection possibilities, particularly in combination with the widespread use of GPS enabled cellular phones. As of January 2014, 90% of American adults have a cell phone, with 58% of those being smartphones (Pew Research Internet Project, 2014). In addition, the number of persons using mobile cellular devices for non-phone uses is also growing, particularly in conjunction with GPS enabling of these devices. The U.S. market for LBS is expected to grow from US$2.8 billion in 2010 to US$10.3 billion in 2015. Expectations are that navigation, local search, and people locating apps will show the strongest growth (ten Sythoff and Morrison, 2011).

Benefits that can be gained from use of LBS applications vary widely depending on the type of LBS used. Benefits to the user of mobile social networking applications such as Foursquare may come in the guise of maintaining contact with parties of interest, economic incentives from retailers or other businesses, or increased knowledge of the whereabouts of persons in one’s social network. Mobile navigation services such as Google Maps, on the other hand, allow a user to query location and direction information from a static point or while in transit, thus allowing for more effective decision-making regarding route planning. Recently, some of these services have been partnering with transit services, state DOTs, and other transportation data providers to provide more comprehensive and timely transportation information to, for example, allow travelers to adjust their route-planning decisions based on real-time information regarding travel times and traffic conditions. These services provide a number of benefits for the consumer, including time and cost savings, as well as security regarding the accuracy of their travel decisions. Mobile automotive assistance and emergency service applications, such as OnStar, which provides a variety of services ranging from navigation and direction assistance to emergency services and diagnostics, have also seen increased adoption as their safety and security benefits are acknowledged by consumers.

Balancing the benefits of ITS and LBS adoption are concerns that individuals and organizations may have regarding their use, including privacy concerns regarding collected data and general unease with new technologies. As we increasingly rely on technology for the performance of both personal and professional tasks, adoption of innovative technologies at individual and organizational levels has become of interest both in system design and in personal interactions. A number of demographic characteristics, such as age, education, and prior experience with technology may influence an individual’s adoption of innovative technologies for personal use (Munnukka, 2007), while other characteristics, described above, may also have impacts on concern for privacy (Junglas et al., 2008). Finally, context of use will also play a role, as some consumers may be more or less willing to share their personal location information dependent upon the time of use and location, and upon the variety of interested parties.

Properly valuing the benefits of adopting these smart mobility ICTs may be difficult for the consumer due to imbalances in information. The following section will review some of the economic considerations that may influence determination of adoption, and will provide context for discussion of the current survey.

2.4 The Economics of Privacy

In discussion of privacy economics, the concept of control in relation to data ownership is perhaps of primary concern. According to Stigler (1980), "'Privacy' connotes the "restriction of the collection or use of information about a person or corporation; the information in question 'belongs' to the individual." Stigler assumes that control of data has an economic grounding –ownership and control of data is defined in relation to economic evaluation and individual willingness-to-trade. Here, the desire of the individual for privacy is balanced against the market's willingness to "buy" information, whether through economic incentives (such as offering discounts to persons who use frequent shopper cards that track purchasing habits) or through incentives of convenience (such as "Trusted Traveler" programs). In this framing, the market for personal data will self-regulate as customers establish the price at which they will be willing to sell personal data, while the market will establish the price at which it is willing to buy the data. In an economy based on the exchange of physical goods, this explanation works reasonably well, considering DeLong and Froomkin's (2000) argument that in a traditional market system the three features of excludability, rivalry, and transparency dominate property rights and exchange. Information, however, functions as a public good (Stigler, 1980), thus, information purchased in one market may be sold for use in a second market without diminishing use by the initial purchaser.

According to Hui and Png (2006), "In deciding how much personal information to reveal, consumers balance the benefit from consuming the primary item against direct privacy costs. The higher the rate at which consumers expect sellers to cross-sell personal information, the less information consumers would reveal." The ability of the seller to accurately price his or her own identifying data, however, is contingent upon this knowledge of how data will be used by the buyer. Hui and Png (2006) also note the potential for cross-selling to result in unsolicited promotions, which may intrude on the value of seclusion. Here, an imbalance of knowledge in the marketplace may lead to an under-valuation by the original information seller. On the other hand, the potential benefits of cross-selling in some instances (such as dissemination of location data from a state department of transportation to a city office of emergency management) may be beneficial enough that a potential seller would over-value certain aspects of privacy. In this case, it is reasonable for some regulatory intervention to ensure that adequate knowledge about both primary and secondary markets is given to the individual.

A final consideration that should be addressed is that of personal valuation versus societal valuation. Some of the greatest societal benefits from collection of travel and location data are related to the potential to make transportation networks more efficient (Zhang and Levinson, 2008). In this case, while the individual traveler whose data are collected may not receive significant individual benefits, the society that uses the information network will. Given that it is the aggregation of individual data records that would allow this potential benefit to accrue, the individual must make his valuation based not only on his individual preferences, but also on potential societal benefits; however, the pathway as to how individual data leads to improved travel at a network-wide level (e.g. through improved traffic management or travel information services) may not be apparent to the user. In the case of government entities subject to legal requirements for use and dissemination of individual data, the valuation may be relatively simple. However, the transport network is composed of both public and private entities, and the potential for sharing of collected location data for uses beyond network efficiency and subject to legal restrictions is great. Given these conditions, the traveler ideally would determine her value of location data based on both individual and societal benefits versus potential cost of intrusion and dissemination beyond the primary market.

As described here, the treatment of private data and information as marketable commodities is somewhat problematic given competing notions of valuation, ownership, and use. With good information and reasonable understanding of primary and secondary uses, the individual and societal benefits would likely make a market price for information acceptable to the seller. However, without this information, the potential for the seller to significantly over- or under-value his or her privacy is great. For the buyer, less information is likely beneficial, as studies have indicated that while persons may indicate a high preference for privacy, their actions regarding privacy do not always reflect this preference (Acquisti and Grossklags, 2005; Xu et al., 2011). The market argument for privacy is compelling to a point; however, the barriers identified above should be taken into consideration. For purposes of this research, location privacy will be studied in response to economic questions (what are the risks associated with providing data in the mobile environment and what compensation or benefits do travelers expect to receive in return), as well as in context (with whom and for what purposes are travelers willing to share private information). It is hoped that such an approach will allow for exploration of privacy matters relevant to travelers in the mobile environment.

3. Privacy Survey

3.1 Hypotheses

In this paper, we draw upon the areas described above, along with additional research (Tang et al., 2010; Barkhuus and Dey, 2003; Krumm, 2008; Danezis et al., 2005). Unlike these studies, we focus here on both user preferences regarding location privacy, as well as contextual elements that potentially influence their agreement to generate and make location, travel time and other information available for a variety of end uses. Examples of such end uses include more accurate estimation of transportation network conditions for overall system management and operations, calculation of travel speeds, travel times or delays for personal vehicle routing or real-time fleet vehicle arrival information, data to support the formation of social arrangements with respect to transportation such as dynamic ride-sharing or car-sharing, and a variety of other end uses by means of which not only the person who generates the information ultimately benefits but which also benefits other service users. Such agreements are made either with the user's comprehension of the implications of information submission on their locational or other privacy aspects, or are a pro-forma agreement, motivated by the personal mobility benefits to be received from using the service. Such agreement (by agreeing to specific terms of service or privacy policies) indicates willingness-to-trade information for various benefits. By providing a basis for economic valuation of privacy, we hope to expand upon previous findings by considering the following hypotheses:

- Hypothesis 1: Relationships will be seen between willingness to trade privacy (WTTP) and self-reported personality characteristics.
- Hypothesis 2: Survey respondents will demonstrate a relationship between WTTP and perceived utility of transportation benefits.

- Hypothesis 3: Persons will display a relationship between WTTP and risk due to perceptions of perceived privacy loss.
- Hypothesis 4: Respondents will be more willing to reduce compensation for trading private information for purposes of safety or efficiency than for cost savings.

These hypotheses will be tested using a survey instrument as described below, and included as Appendix A.

3.2 Survey Development and Administration

As identified above, a primary topic of interest in privacy studies is that of the willingness of consumers to provide (or "trade") private data in exchange for assorted benefits. Here, we address this issue in the context of the trading of personal and location data for the receipt of transport-related benefits. While there are issues associated with stated preference surveys and contingent valuation (such as inconsistencies between a person's stated preference and how they will actually act (Berendt et al., 2005), and difficulties in assigning accurate values to goods that are generally not market priced), in the context of this paper the need to evaluate traveler preferences regarding willingness to trade in reference to proposed or hypothesized mobility applications indicates that a stated preference survey including contingent valuation measures is the most reasonable method for ascertaining likely trade-off preferences. This section will describe both survey development and sampling.

The survey design process consisted, first, of identifying the major topics of interest related to the willingness to trade privacy for perceived transportation benefits. It was determined that information was needed related to current use of general personal technologies (such as computers and smartphones) as well as transportation-related technologies (such as GPS devices), current consumer concerns related to privacy in the mobile environment, and expectations related to benefits, in addition to general demographic information. Due to difficulties in identifying specific valuations of privacy on the part of consumers, Likert scales were used throughout the survey in order to query respondents on their relative degrees of importance and interest in privacy and benefit matters. While the use of Likert scales limits the ability to assign absolute values of importance or concern, it allows for relative measures of importance and concern to be determined. In general, five point scales were used, ranging from "Strongly Disagree" to "Strongly Agree" and "Not Important" to "Very Important." A seven point scale was used for purposes of determination of personality characteristics (Extraversion, Agreeableness, Conscientiousness, Emotional Stability, and Openness to Experiences) based on research by Gosling, Rentfrow, and Swann (2003).

For one question, "How much, in general, would you have to be compensated to provide the following information to these [transportation] agencies?" respondents were asked to quantify the amount of compensation they would require to provide specific types of personal (name and address) or travel (origin, destination, travel time and route data) information to assorted transportation agencies. They were then asked to indicate whether this amount would increase, decrease, or stay the same under various scenarios evaluating the valuation of economics, safety, and efficiency. Though respondents were asked to provide specific valuation amounts, difficulties in ascertaining the value of various types of information has resulted in these valuations being treated as ordinal scales in keeping with evaluation of other questions.

Following survey questionnaire development and pre-testing in the online survey program SurveyMonkey, notifications of the posting of a privacy survey were distributed via email listservs and social networks. Persons who received notification of the survey were additionally asked to forward the survey on to friends, colleagues, and others who might be willing to participate, producing a snowball sample.

Several limitations exist with online surveys, particularly with representativeness of the sample and selection biases, difficulties in measuring non-response rates and lack of control over the testing environment (e.g., Matsuo et al., 2004). In the case of the current survey, while the sample obtained is not representative of the population at large from a demographic standpoint, it is reflective of persons who are likely at the forefront of adoption of the types of technologies of concern to the overall research (Munnukka, 2007; Lee, 2014; Patil et al., 2012). Given the current state of fragmentation in location privacy, beginning the conversation of consumer expectations with earlier adopters may start to provide some indication of what the key privacy concerns will be over a broad population over time. While the limitations of the survey methodology indicate that the sample is not statistically random, findings do provide a basis for exploration of attitudes and expectations regarding privacy in the locational environment. It is not possible to determine the sampling rate for the survey due to a lack of information regarding the number of persons who had the opportunity to participate, nor is it possible to determine non-response rates. Persons who visited the survey but chose not to participate were asked to fill out an exit survey in order to provide general demographic information; however, no exit surveys were completed, thus no information was gathered on persons who chose not to participate in the survey.

3.4 Methodology

In this section, we focus on the analysis that was undertaken of the survey data, with the objective of identifying privacy preferences and the trade-offs that users of mobile information are willing to make for perceived utility received, and the perceived risks and expected compensation for giving up information.

3.4.1 General Survey Type

While stated preference surveys have limitations, survey information can be invaluable when determining privacy-utility tradeoffs (Krause and Horvitz, 2008). Here, benefits of ITS and LBS technologies are related to economics, safety and travel efficiency. Additionally, because ITS technologies will rely in part on fairly widespread deployment to attain maximum benefit, participants must consider both individual and societal utility. The survey used here addresses these needs by presenting survey participants with the opportunity to examine not only privacy in relation to individual benefits, but also system and network benefits.

In the context of locational privacy, the need to address the limitations of stated-preference approaches is particularly significant as much of the proposed technology and its implications are unfamiliar to the traveling public. Additionally, willingness-to-trade and privacy-utility evaluations are necessary insofar as many proposed and implemented ITS projects rely on the provision of personal information to create travel benefits in terms of time or cost. Statistical approaches to evaluating actual preferences in relation to general survey questions on stated preferences are described below.

3.4.2 Principal Component Analysis and Ordered Probit

To address the fact that many variables of interest in the survey data are likely to be correlated, Principal Components Analysis (PCA) was used to reduce correlated variables into sets of principal components, or a linear combination of optimally-weighted observed variables. This yielded a score for each survey respondent on a given principal component. The first few components, which account for most of the meaningful amounts of variance, were used in the regressions of locational privacy. In particular, constructs of interest tested through questions related to willingness to trade private information, desire for compensation, context of interest (specifically, private or public services), and knowledge of privacy policies and practices were subject to PCA in order to better evaluate related constructs to demographics, privacy expectations and risk perceptions. Respondents were queried about their preferences and values on a number of factors on Likert scales, with ordinal values. For example, one major factor of interest is a respondent's self-reported willingness to trade privacy for a number of benefits relating to their mobility conditions. To appropriately model the ordinal nature of such factors, ordered probit models were used. Following the example of the willingness-to-trade, the ordered probit model uses the following form:

$$y_i^* = \boldsymbol{\beta}' x_i + \boldsymbol{\varepsilon}_i$$

where y_i^* is the dependent variable (a continuous, composite score that gives the willingness-to-trade privacy of the i^{th} respondent), $\boldsymbol{\beta}$ is a vector of parameters to be estimated, $\boldsymbol{x}_i$ is a vector of independent variables and $\boldsymbol{\varepsilon}_i$ is the error term, which is assumed to be normally distributed with mean zero and unit variance, with cumulative distribution denoted by $\Phi(\cdot)$ and density denoted by $\phi(\cdot)$. Given a decision regarding the use of mobile technologies, an individual falls in category *n* if $\mu_{n-1} < y_i^* < \mu_n$, where the μ's are cut-off thresholds to be estimated, along with $\boldsymbol{\beta}$. Hausman tests which test whether the potentially endogenous variable acting as a regressor and the disturbance are uncorrelated were used to evaluate if willingness to trade privacy and the other constructs of interest are simultaneously determined, resulting in p values close to .1, indicating that the constructs are potentially exogenous. Since simultaneity was not strongly evident from the tests, single-equation ordered probit models were used to determine whether willingness to trade privacy by the respondents is related to utility derived from information, and other factors.

3.5 General Demographics

425 persons began the survey, with 382 (89.9%) completions. As noted above, persons who participated in the survey were not reflective of the overall population; for example, survey participants were significantly more educated and in slightly different income brackets than the general population. Also of note is that respondents tended to be overwhelmingly urban, which has implications for the survey as whole. For example, survey participants were more likely to report "Public transit," "Walking," or "Biking" as their primary mode of transportation to work than the general US population, likely due to the greater availability of public transportation, biking and walking facilities within urban areas.

It may, however, be argued that the survey sample does reflect characteristics of both first and early adopters, as discussed above. This contention is generally reflected in findings that self-reported levels of expertise with various common technologies, such as computers and smartphones, were quite high for survey respondents. Responses indicate that most survey participants were familiar with and considered themselves “expert” or “intermediate” users of many common personal technologies, including cell phones (92%) and smartphones (55.7% - significantly higher than the 25% reported nationally (Dediu, 2010)). In general, survey responses indicate that participants consider themselves intermediate or expert users of the technologies of interest.

Respondents were also queried about use of a limited number of transportation or mobile technologies, including technologies aimed at payment (including electronic toll collection (ETC) passes, transit passes, and university passes), social networking (Foursquare and Google), safety (OnStar), and navigation (OnStar and web- or phone-based mapping services). Use of these technologies is significantly lower than that of the common, stationary technologies evaluated above. Only the use of web- or phone-based mapping services, such as Google Maps, showed usage by more than 50% of respondents, a finding that may be related to the relative ease of access from either a stationary (such as a personal computer) or mobile (such as a smartphone) technology.

3.6 Attitudes and Actions Regarding Privacy

Respondents were asked to report on how often they read or skim Terms of Use or Service when they use the above mentioned transportation or mobile technologies. Of those persons who reported that they use these services, most reported that they “never” or “rarely” read the Terms of Use or Service. Of note is that persons reported a slightly higher rate of reading the terms for services provided by public or semi-public providers (Electronic Toll Passes, Electronic Transit Passes, and University passes) than those services offered by private providers. Each of the three public services evaluated showed a readership of over 50%, while none of the privately provided services reached this amount. Findings were similar in response to the question, “How often do you notice if there is a privacy policy before using the following types of services (for example, "Your privacy is important to Company X; maintaining your trust is important to us.")?” In this case, slightly fewer respondents reported noticing the presence of a privacy policy when using a University Transit Pass, while more reported noting the presence when using a web- or phone-based mapping service. In general, a significant majority of respondents reported that they “never” or “rarely” read or skim Terms of Use or Service or notice the presence of a privacy policy.

The findings reported above also hold when evaluating how often people read provided privacy policies or guidelines. Most people (averaging roughly 88% of respondents) reported that they “Never” or “Rarely” read the privacy policies of the evaluated services. Again, levels of reading privacy policies tend to be slightly higher for publicly provided services than for those offered by private providers, with the exception of University Transit Passes and web-based services such as Google maps. These findings indicate a potential overarching concern of the survey, which is the lack of understanding of privacy risks encountered when using location-aware services. Here, we have chosen to focus on the expectations that people have around such risks predicated on their overall perceptions.

Participants were then asked to respond to a series of questions regarding their beliefs about the potential risk experienced in a number of scenarios. These scenarios were designed to test responses based on privacy risks related to data gathering, use and sharing by public and private agencies in terms of economics, travel efficiency, and law enforcement. The following table shows the responses obtained to these questions, with replies ranging from “Strongly Disagree” to “Strongly Agree”.

Please indicate the degree to which you agree or disagree that the following actions will place your privacy at risk:					
Answer Options	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
Having your location or travel data collected and stored by a private company (such as Google)	6.2%	17.6%	25.2%	34.9%	16.1%
Having your location or travel data collected and stored by a public agency (such as a transit agency)	7.4%	18.3%	30.0%	29.5%	14.9%
Sharing location or travel data with friends via an application such as Google Latitude or Foursquare	4.0%	12.2%	23.4%	40.4%	20.0%
Having your location or travel data shared for marketing purposes	8.2%	10.4%	11.7%	30.3%	39.5%
Having your location or travel data shared for legal purposes	6.5%	13.0%	20.1%	32.3%	28.1%
Having your location or travel data shared for purposes of transportation efficiency (such as providing real-time traffic data or alternate routes)	11.7%	32.8%	24.6%	19.1%	11.9%
Sharing identity and financial information for travel purposes (such as electronic toll collection)	8.5%	17.5%	23.8%	29.3%	21.0%
Having location or travel information gathered by a private company (such as Google, OnStar, or Orbitz) shared with law enforcement agencies after a warrant has been issued	6.2%	15.7%	21.4%	29.7%	26.9%
Having location or travel information gathered by a private company (such as Google, OnStar, or Orbitz) shared with law enforcement agencies with no warrant issued	8.8%	9.0%	10.8%	21.3%	50.1%
Having location or travel information gathered by a public agency (such as your state Department of Transportation) shared with law enforcement agencies after a warrant has been issued	7.7%	16.9%	22.9%	26.6%	25.9%
Having location or travel information gathered by a public agency (such as your state Department of Transportation) shared with law enforcement agencies with no warrant issued	8.2%	9.7%	14.2%	23.9%	43.9%

Table 1: Reported Perceptions of Privacy Risk.

Findings here indicate that respondents believe that most of the scenarios stated have some possibility of putting one's privacy at risk. In all cases but "Having your location or travel data collected and stored by a public agency" and "Having your location and travel data shared for purposes of transportation efficiency," 50% or more respondents replied that they "Agree" or "Strongly Agree" that the scenario in question will place one's privacy at risk. The strongest responses regarding the potential for privacy risk involved the sharing of collected data with law enforcement agencies with no warrant issued. This finding was especially strong for private companies, with over 50% of respondents replying that they "Strongly Agreed" that this would put privacy at risk. Responses were weakest for the privacy risk of having location or travel data shared for purposes of transportation efficiency, with nearly 45% of respondents indicating that they disagreed or strongly disagreed that such an action would place privacy at risk. Sharing data for marketing purposes also produced a strong response, with nearly 70% of respondents indicating that they agreed or strongly agreed that such actions would place their privacy at risk. The findings represented here indicate that participants generally believe that sharing travel and transportation related data has the potential to place their privacy at risk, whether such data are shared and used by public or private agencies.

Participants were next asked to indicate which, if any, of certain types of information or practices they feel are important for agencies, companies, or organizations that collect travel or location data to share with consumers. Findings indicate that respondents believe that a wide variety of information should be shared with consumers, with the strongest responses relating to the types of data being collected, with whom these data will be shared, and for what purposes. Weakest, though still strong, support was shown for the provision of information regarding how collected data may be reviewed and corrected by the user. The strong results shown here are interesting when reviewed in the context of the findings above regarding how often respondents review privacy policies, and how much they feel that certain agency or organization actions will place their privacy at risk. As shown above, the majority of respondents "never" or "rarely" read privacy policies or agreements prior to use of smart mobility services, yet they believe that certain actions on the part of the service provider may place their privacy at risk and that a broad spectrum of information regarding data collection, use and sharing should be provided to the consumer (for example, what type of actions will be taken using collected data). Such findings may indicate a range of possibilities, including, (1) that consumers believe that the information they feel *should* be included in privacy policies *are* actually included in privacy policies; (2) that consumers are concerned about privacy in the mobile environment but do not understand privacy policies as presented and so do not read them; or (3) that consumers do not believe that privacy policies adequately address relevant concerns, but need to access the service anyway and thus simply agree to them. For cases where privacy policies were not read by the user, no follow-up question was asked on why.

A related question referring to the impact of information generation was also asked, particularly to their willingness to trade location and related information in order to receive mobility benefits such as routing and navigation information, or time savings or improved travel reliability. Findings across the three categories of cost benefits, time savings, and safety benefits indicated a consistently high willingness to trade, while respondents appeared slightly less concerned about transportation security benefits. Participants were also asked to indicate how willing they would be to share their travel information with third parties given certain caveats, with travelers most likely to agree that they would share their travel information with third parties only if the data were made anonymous or were aggregated with other's travel information. Far fewer agreed that they would be willing to share their data if notice were given or if they knew what information was being shared. This finding indicates that anonymity may be the most important deciding factor for consumers when deciding whether or not to share travel information, regardless of whether they are notified or not.

The brief analysis above indicates that privacy is of concern amongst consumers in the mobile environment. While adoption and use of certain general technologies, such as computers, cell phones and GPS-enabled devices, and certain mobile technologies, such as toll passes, transit passes, and web-based mapping tools, are shown to be quite high, question responses have also indicated a degree of concern related to privacy risk implications of use of transportation technologies. The following section will expand upon these findings, and look more closely at the trade-offs that consumers are willing to make between provision of personally identifying information related to transportation and potential mobility benefits.

3.7 Results

The above discussion provides a general overview of results obtained from the privacy survey. To further enhance our understanding of consumer attitudes towards location privacy, we next look at how respondents valued the trade-offs between sharing of personal data and concomitant transportation benefits. A number of methods were evaluated for their applicability to the data set and questions of interest. In part, the issue at hand is that "privacy" is not a static concept. As noted above, contextual and societal constructs will play a role in the desirability of the protection of private data dependent upon assessment of likely benefits, agencies or organizations involved in the management and use of data, and personal preferences relative to these factors. As such, simple regression analysis alone will not be adequate for evaluating survey results, leading to the use of PCA and ordered probit modeling.

3.7.1 Data Pre-Processing

Due to perceived similarities in ratings of privacy risk reported by respondents, a correlation matrix was developed for the perceived risk categories tested in the survey. Strong correlations were found for nearly all tested pairs, thus these factors were collapsed into one primary category by adding factor scores and dividing by 11 (the number of factors tested) to create an average score for privacy risk perception. No strong differences were seen in questions related to public or private risks, thus no differentiation was made based on these factors. In much the same way, correlations were checked for desired compensation for elements of personal data related to travel. Two factors (name and address) showed significant differences from other factors tested (vehicle information, starting point of a trip, ending point of a trip, time of day at which trips are made, and trip route and time of day), thus these were collapsed into two categories reflecting compensation for personal data and compensation for transportation data. These two factors were then used to cluster respondents in the context of privacy risk assessment.

Since many of the questions asked in the survey related to individual constructs shown above, Principal Component Analysis (PCA) was used to identify the primary components underlying the data related to these factors in order to reduce the number of variables of interest. SAS Proc Factor, which performs common factor and component analyses with rotations, was first used to conduct a principal axis method, followed by a varimax (orthogonal) rotation, which imposes a restriction disallowing correlation of factors. Four factors were retained for rotation, as described below.

Three variables relating to actions and attitudes towards privacy policies were found to load on Factor 1: (1) Reads privacy policies prior to adopting new location services or applications, (2) Perceived degree of general understanding of privacy policies, and (3) Perceived comfort regarding privacy protections. This factor will be referred to as the Knowledge Factor (KF). Two variables were found to load on Factor 2: (1) Risk perceived by having location data collected and stored by a private company, and (2) Risk perceived by having location data collected and stored by a public organization. This factor will be referred to as the Risk Factor (RF). Factor 3 had four variables displaying load, namely: (1) Willingness to trade some degree of privacy for out-of-pocket transportation cost reductions, (2) Willingness to trade some degree of privacy for transportation time savings, (3) Willingness to allow travel information to be shared with third parties if it is made anonymous, and (4) Use of transportation technologies This factor will be referred to as Willingness to Trade (WT). Finally, Factor 4 had two loading items, namely: (1) Compensation required to share personal data, and (2) Compensation required to share travel data. This factor will be referred to as the Compensation Factor (CF).

Next, factors were correlated with additional survey data to test a number of hypotheses, described in the analysis below.

3.7.2 Hypothesis 1: Relationships will be seen between WTTP and self-reported personality characteristics.

This hypothesis evaluates how certain character traits may play out in the relationship between a person's characteristics regarding personality and lifestyle in regard to willingness to trade information. Because of mild observed heteroskedasticity, a Weighted Least Squares (WLS) model was used to evaluate the personality characteristics of Extraversion (*extraver*), Agreeableness (*agrblns*), Conscientiousness (*conscien*), Emotional Stability (*emotstab*), and Openness to Experiences (*opn2exp*); demographic traits, including education (*education*), income (*income*), gender (*gender*) and age (*birthyr*); importance of travel information (calculated as a composite score of importance of receiving various types of travel information (*impben*)); and comfort with technology (*usetech*) in relationship to willingness to trade information. Two characteristics modeled (Extraversion and Importance of Benefits) were found to be significant at 0.01, while four (Conscientiousness, Gender, Education, and Income) were significant at 0.05, with extraversion, importance of benefits and education having positive influences on likelihood of willingness to share data, and conscientiousness, income, and being male having negative influences. This is in keeping with prior research indicating that more extraverted persons tend to have a higher degree of trust value in other persons or agencies. While the overall R^2 value obtained (0.1567) was fairly low, the indicators evaluated met the influences of the overall hypothesis.

3.7.3 Hypothesis 2: Survey respondents will demonstrate a relationship between willingness to trade private information (WTTP) and perceived utility of transportation benefits.

Concern for privacy is a difficult concept to quantify, as it may be measured in a number of different ways. For purposes of this paper, privacy concern is measured in terms of "willingness to trade" via use of a question asking respondents to rate how willing they are to trade certain types of information for specific benefits. Such a measurement may be seen in the form of a privacy-utility tradeoff, as described in Krause and Horvitz (2008). For purposes of this paper, general utility is measured in terms of reductions in transportation cost and travel time savings, transportation safety benefits, and transportation security benefits.

The hypothesized relationship between WTTP and perceived utility is first explored in terms of perceived importance of transportation information. It is hypothesized that the higher a respondent rates perceived importance of receiving transportation information benefits (such as reliable travel times and incident occurrence), the more willing he will be to trade personal information. Such a hypothesis is in keeping with results found in (Phelps et al., 2000) and (Krause and Horvitz, 2008). Importance of travel information is estimated via a question asking participants to rate the importance of various types of transportation information.

To first explore the relationship between willingness to trade information and utility of transportation benefits, a series of regression analyses were run testing the relationships between the following (full variable descriptions available in Table 2 below):

- Willingness to trade privacy for benefits (*privtrade*)
- Utility (*utility)*
- Total risk (*totrisk)*
- Compensation (*compen*)

Hausman tests were run to test for biases or inconsistencies in the estimators. No evidence of simultaneity was found, thus it was not necessary to use an instrumental variables method or two-stage least squares. Instead, ordinary least squares (OLS) regressions were used for the initial analyses.

Variable	Description
privtrade	Willingness to trade privacy for benefits: A composite variable composed of the summation of degree of willingness to trade privacy for cost benefits, time savings, safety benefits, and security benefits
utility	Utility: Composite value composed of respondent ranking of importance of knowing travel time, alternate routes, changes in the travel environment, transit reliability, and immediate safety information
totrisk	Total risk: Composite value composed of degree of risk that will be incurred by sharing location and travel data with a private agency, a public agency or with friends; having location and travel data shared for purposes of marketing, legal purposes and transportation efficiency; having data shared with law enforcement agencies by public or private agencies with or without a warrant; and for purposes of electronic toll collection
compen	Compensation: Composite compensation desired to share name, address, vehicle information, trip origins and destinations, time of day of trip and trip route
totalinfovalue	Composite variable representing the general value that respondents assigned to the types of travel information surveyed

totalprivacytrade	Composite variable created from the variables indicating respondent's willingness to trade private data for transportation benefits
LtechLBS	1 if respondent reports use of one or more of the following: Google Latitude, OnStar, Foursquare, or Google Maps
LTechNon	1 if respondent uses no location based services
LTechPay	1 if respondent reports use of one or more of the following electronic payment methods: Electronic toll pass, university transit pass, electronic transit pass
gpsexp	1 if respondent reports self as expert GPS user
gpsintno	1 if respondent reports self as intermediate or novice GPS user
spexpert	1 if respondent reports self as expert smartphone user
spintnov	1 if respondent reports self as intermediate or novice smartphone user
age	Reported age of user
gender	Reported gender of user
income	Reported income level of user
education	Reported educational level of user
wkcar	Respondent travels by car to work
wktrans	Respondent travels by transit to work

Table 2: Variables Used in Model Development

Three initial OLS models (all variables shown in Table 2, and results in Table 3) were estimated to test influences on the dependent variables of Utility (*utility*), Total Risk (*TotRisk*) and Compensation (*compen*). For each model, willingness to trade privacy (*privtrade*) is seen as having a significant impact on the dependent variable. In the case of utility, the parameter is positive, indicating that the higher the willingness to trade, the greater the respondent views the utility of transportation benefits. The parameter is negative for both compensation and total risk, indicating that persons with a greater degree of willingness to trade privacy both require less compensation to give up personal data, and associate lower risk with giving up such data. These findings are consistent with the literature reviewed above, as well as with the hypothesis tested here.

For utility, other variables of interest are age, which has a slightly positive impact, indicating that older persons may be more likely to place importance on having reliable and useful transportation information, and *LTechPay*, which indicates use of electronic transit fare cards or electronic toll passes. It is likely that those persons who use these methods of payment are interested in efficiency and expediency, thus their higher ranking of utility is unsurprising. For estimation of risk, age was again a factor, with an increase in age generally indicating a slight increase in estimation of risk of sharing private data. A surprising finding here is that those respondents who do not currently use location technologies report slightly less degree of risk estimation. This may be due to lack of knowledge of information that may be revealed through use of these services, or it may indicate a general unfamiliarity with such services. Educational levels had a slight positive impact on compensation requirements, indicating that more highly educated persons were likely to request less compensation to share data.

Variable	Utility Estimate	TotRisk Estimate	Compen Estimate
Intercept	15.04	42.25	58.85
privtrade	**0.22***	**-0.7***	**-1.4***
age	**0.03****	**0.12****	0.01
Gender	-0.24	1.01	-2.06
Income	0.05	-0.1	-0.26
Education	-0.12	0.33	**-1.28****
LtechLBS	-0.09	0.68	-1.34
LTechPay	**2.08***	-0.34	2.1
LTechNon	1.36	**-5.04****	-1.44
wkcar	0.1	0.42	-0.21
wktrans	0.46	-0.01	0.24
spexpert	0.46	0.5	-1.02
spintnov	0.16	0.25	-1.31
gpsexp	0.06	0.4	2.8
gpsintno	0.15	-1.02	-0.67
Fit Measures			
Root MSE	2.86	8.69	12.05
R^2	0.13	0.12	**0.16**
** Significant at 0.01*			
***Significant at 0.05*			

Table 3: OLS Models of Utility, Total Risk, and Compensation

Neither travel modes nor user-reported degree of experience with GPS or Smartphone technologies were seen to significantly impact the model, indicating that these variables are not representative overall of person's privacy and utility preferences. Model fit and R^2 statistics indicate that, while influence is consistent among tested variables, the models overall do not account for a great deal of variance in the data. The following sections will use different methods and models to test the influence of variables in more detail.

The survey used a Likert scale to indicate degree of agreement, thus the resulting data take an ordinal, or ordered, form. An ordered probit model was thus next used to estimate relationships of interest. While individual types of information were initially surveyed, a correspondence analysis was used on the responses that resulted in a standardized Cronbach's alpha of 0.651496, indicating strong correlation between the tested variables. Thus, the composite variable *totalinfovalue* was created to represent the general value that respondents assigned to the types of travel information surveyed. In a similar manner, the composite variable *totalprivacytrade* was created from the variables indicating respondent's willingness to trade private data for transportation benefits based on a standardized Cronbach's alpha of 0.837. SAS proc QLIM was used to run the ordered probit models. In order to limit the number of thresholds tested, raw scores for *totalinfovalue* were categorized into quadrants and then analyzed. A McKelvey-Zavoina goodness of fit measure of 0.16

indicates a weak fit for the overall model. Additionally, threshold estimates (designated as μ_1 (the deviation of τ_1 from τ_2), μ_2 , which is the deviation of τ_2 from τ_3, and μ_3, which is the deviation of τ_3 from τ_4) were insignificant with the exception of μ_3, indicating that the greatest relationship between willingness to trade and perceived value of information occurs for those with the highest privacy preferences. The significance of *totalprivacytrade* in relation to *totalinfovalue* is strong, indicating that for persons with higher privacy values, there is a strong relationship between willingness to trade private information and the degree of importance assigned to various types of transportation information. Weaker relationships found for those with low privacy preferences indicate that low overall privacy preferences also indicates a low degree of relationship between willingness to trade information for transportation benefits, perhaps due to the relatively low value assigned to private information. Such a finding is consistent with overall expectations, as it indicates that those with higher privacy sensitivity are more concerned with receipt of potential benefits in order to be willing to trade their personal information. Full results of the tested models can be seen in Table 4 below.

3.7.4 Hypothesis 3: Persons will display a relationship between WTTP and risk due to perceptions of perceived privacy loss.

This hypothesis states that persons who have a lower degree of willingness to trade private information will also have higher degrees of perceived privacy loss relevant to certain situations. Respondents were asked to respond to a question inquiring their perceived risk of privacy loss in the situations described in Table 1 above. A correlation analysis was run, resulting in a standardized Cronbach's alpha of 0.8834, indicating strong correlations between the tested variables. As a result, a composite variable of risk was developed titled *totalprivacyrisk*. As above, an ordered probit model was run to ascertain relationships of interest.

As above, the overall fit of the models was moderate, with low McKelvey-Zavoina pseudo R^2 values (0.14) for the overall model (results shown in Table 4 below). Threshold estimates were significant only at Limit 1, indicating that risk perceptions are perhaps most differentiated and significant for those persons who have high privacy sensitivity. From these results, we see that perceptions of privacy risk have the most influence on willingness to trade privacy for persons who demonstrate the strongest privacy preferences. As above, the higher the risk estimation, the less likely the respondent was to indicate high willingness to trade privacy. Also consistent were findings related to the influence of demographic variables (in particular education), current use of technology, and preferred transportation mode.

For the majority of respondents, willingness to trade information increases as perceptions of risk increase. However, the higher a respondent's perception of risk, the likelihood of willingness to trade information decreases. Here, it may be interpreted that, up to a point, the possibility of benefits of trading information may offset risk perception for those with lower general propensity to trade information. However, as a person's perception of risk increases beyond a certain point, the likelihood of trading information will decrease, indicating that the benefits are not perceived as outweighing risk.

	Total Value of Information Model (totalinfovalue)	Total Willingness to Trade Privacy Model (totalprivacytrade)	Willingness to Trade Privacy (totalprivacytrade) vs. Perceived Risk Model
Parameters	**Estimate**	**Estimate**	**Estimate**
totalprivacytrade	**0.09***	N/A	N/A
Factor4 (Compensation)	N/A	-0.55*	N/A
totalprivacyrisk	N/A	N/A	-0.026*
spexpert	0.16	0.00	0.036
spintnov	0.01	-0.21	-0.130
gpsexp	-0.06	0.17	0.159
gpsintno	-0.04	0.20	0.283**
LtechLBS	-0.10	0.14	0.137
LTechPay	**0.90***	0.07	-0.104
LTechNon	0.36	-0.13	-0.377
usetransit	-0.02	0.01	0.054
usewalk	0.01	-0.23**	-0.118
usebike	**-0.11*****	-0.05	-0.024
age	**0.01*****	0.00	0.005
Education	-0.03	0.09	0.216**
Gender	-0.09	-0.21***	-0.120
impshr	0.01	-0.10**	-0.091**
Income	0.01	-0.04	-0.064
μ_1	0.35	-1.83**	-1.513**
μ_2	0.92	-0.94***	-0.775
μ_3	**2.45***	0.83	0.912
Measures of Fit			
Log Likelihood	-372.348	-378.571	-406.524
AIC	782.695	795.143	851.049
Schwarz Criterion	857.256	869.084	925.405
Cragg-Uhler 1	0.139	0.188	0.120
Adjusted Estrella	0.047	0.101	0.025
McKelvey-Zavoina Pseudo R^2	0.168	0.226	0.144

** Significant at <0.0001*
*** Significant at 0.05*
**** Significant at 0.1*

Table 4: Ordered Probit Model (OPM) for Total Value of Information (*totalinfovalue*), Total Willingness to Trade Privacy (*totalprivacytrade*), and Willingness to Trade Privacy (*totalprivacytrade*) vs. Perceived Risk

3.7.5 Hypothesis 4: Respondents will be more willing to reduce compensation for trading private information for purposes of safety or efficiency than for cost savings.

Respondents were asked to indicate how much compensation they would require in order to trade various types of personal information, including name, address, and trip origin and destination data, along with other travel information. Persons showed most reluctance to sell name and address information, with nearly 70% of respondents reporting that they would be unwilling to sell these data, and prices required to provide such data were significantly higher for these than for other data types. Despite these differences, a correlation procedure was run in SAS, resulting in a standardized Cronbach's alpha of 0.9051. Due to this finding, a composite variable was created in order to test how respondent requirements for compensation changed due to various scenarios.

Respondents were presented with the following six scenarios and asked to indicate if their compensation requirements would increase, decrease, or stay the same under the given circumstances:

- Scenario 1: Reduction of travel time by an average of 15% per trip
- Scenario 2: Reduction of gas tax for all persons by $0.01/gallon
- Scenario 3: Reduction of gas tax for all persons by $0.02/gallon
- Scenario 4: Decrease in vehicular fatalities by 100 persons per year
- Scenario 5: Decrease in vehicular fatalities by 1,000 persons per year
- Scenario 6: Collection agencies will sell information to private third parties

First, a crosstabulation was developed to determine general patterns of increases or decreases in expected compensation across scenarios. The generalized results are shown in Table 5.

Scenario	Variable	Increase in compensation		Decrease		No Change		Total
		# of respondents	%	# of respondents	%	# of respondents	%	
Scenario 1: Reduction of Travel time by average of 15%	Name	5	1%	27	7%	331	91%	363
	Address	6	2%	32	9%	325	90%	363
	Vehicle	14	4%	68	19%	277	77%	359
	Origin	16	4%	93	26%	252	70%	361
	Destination	17	5%	92	25%	253	70%	362
	Time of Day	15	4%	91	25%	254	71%	360
	Trip Route	16	4%	93	26%	248	69%	357
Scenario 2: Reduction of gas tax by $0.01 per gallon	Name	21	6%	16	4%	324	90%	361
	Address	21	6%	19	5%	321	89%	361
	Vehicle	29	8%	27	8%	301	84%	357
	Origin	28	8%	38	11%	294	82%	360
	Destination	28	8%	38	11%	294	82%	360
	Time of Day	29	8%	40	11%	289	81%	358
	Trip Route	29	8%	41	11%	288	80%	358
Scenario 3: Reduction of gas tax by $0.02 per gallon	Name	19	5%	19	5%	322	89%	360
	Address	19	5%	20	6%	321	89%	360
	Vehicle	25	7%	36	10%	293	83%	354
	Origin	29	8%	44	12%	285	80%	358
	Destination	29	8%	45	13%	284	79%	358
	Time of Day	31	9%	46	13%	279	78%	356
	Trip Route	32	9%	46	13%	278	78%	356
Scenario 4: Decrease in vehicular fatalities by 100 persons per year	Name	12	3%	74	21%	270	76%	356
	Address	12	3%	78	22%	266	75%	356
	Vehicle	18	5%	114	32%	220	63%	352
	Origin	20	6%	143	40%	192	54%	355
	Destination	21	6%	143	40%	190	54%	354
	Time of Day	21	6%	142	40%	190	54%	353
	Trip Route	22	6%	141	40%	186	53%	349
Scenario 5: Decrease	Name	12	3%	104	29%	241	68%	357
	Address	12	3%	109	31%	236	66%	357
	Vehicle	19	5%	134	38%	202	57%	355

in vehicular fatalities by 1,000 persons per year	Origin	20	6%	165	46%	172	48%	357
	Destination	20	6%	164	46%	173	48%	357
	Time of Day	20	6%	164	46%	172	48%	356
	Trip Route	21	6%	161	46%	170	48%	352
Scenario 6: Collecting agencies sell data to third parties	Name	125	35%	12	3%	221	62%	358
	Address	129	36%	13	4%	217	60%	359
	Vehicle	183	51%	19	5%	154	43%	356
	Origin	217	60%	19	5%	123	34%	359
	Destination	217	60%	20	6%	122	34%	359
	Time of Day	212	59%	20	6%	126	35%	358
	Trip Route	216	61%	18	5%	123	34%	357

Table 5: Crosstabulation of compensation changes across scenarios.

Here, it is evident that for most scenarios respondents reported that their compensation requirements would not change despite various benefits evaluated. The clearest digression from this general pattern occurs for Scenario 6 (Collection agencies will sell information to private third parties, where a majority of respondents reported that their compensation requirements for vehicle, origin, destination, trip time of day, and trip route information would increase. Clear patterns for compensation decreases are also seen for the same variables in Scenarios 4 and 5 (decrease in vehicular fatalities), with a slightly higher incidence of compensation decreases seen for Scenario 5, which tested a higher degree of fatality savings.

As with the overall compensation factors, Cronbach's alpha was tested for correlation of responses to each of the above scenarios, and were found to be significant. Thus, responses were combined into composite variables for each scenario tested.

To test the hypothesis that respondents will, in general, require lower degrees of compensation for safety and efficiency benefits than for economic benefits or if they are aware that companies will receive monetary benefits for their information, a multivariate analysis of variance (MANOVA) test was run. A MANOVA tests for the difference in two or more vectors of means, allowing us to: (1) explore one statistical test on several correlated dependent variables (scenario compensation levels required), and (2) explore how the independent variable (baseline compensation) influences the patterns of the dependent variables. Here, we are interested in the relationship between changes in desired compensation and type of scenario tested (safety, efficiency, or economic).

Results of the MANOVA (shown in Table 6) indicated that changes in compensation across all tested scenarios were significant with respect to the privacy preferences of respondents. Coefficients of variance were highest for scenario 6, which tested variations in compensation levels requested if collected data were to be sold to third-parties, though the r^2 obtained for this statistic was fairly low with respect to travel data. Overall, correlations between privacy preferences and compensation required were lower in general for travel data and higher for personal data (name and address) across all scenarios, indicating that privacy preferences are likely more tied to what consumers perceive as personally identifying information. This finding, however, is somewhat disturbing given that travel data, which consumers seem more likely to sell for lower costs, may be used to determine personally identifying information. General goodness-of-fit measures, including Wilks'

Lambda and the Hotelling-Lawley Trace, were significant at <0.001, indicating that we may reject the null hypothesis that privacy preferences will not impact compensation required for the sharing of data across scenarios. Less statistical variation is seen across how respondents reacted to scenario types here, though overall variations were seen in analysis of the raw data above.

Dependent Variable	Pr > F	R-Square	Coeff Var
Compensation, scenario 1, personal information	<.0001	0.45	27.27
Compensation, scenario 1, travel information	<.0001	0.32	33.47
Compensation, scenario 2, personal information	<.0001	0.35	32.28
Compensation, scenario 2, travel information	<.0001	0.29	35.60
Compensation, scenario 3, personal information	<.0001	0.37	31.94
Compensation, scenario 3, travel information	<.0001	0.29	36.56
Compensation, scenario 4, personal information	<.0001	0.33	34.75
Compensation, scenario 4, travel information	<.0001	0.25	39.24
Compensation, scenario 5, personal information	<.0001	0.27	36.52
Compensation, scenario 5, travel information	<.0001	0.21	39.25
Compensation, scenario 6, personal information	<.0001	0.38	44.81
Compensation, scenario 6, travel information	<.0001	0.19	58.41

Table 6: Results of MANOVA Analysis Testing Privacy Preferences in Relation to Compensation Changes

4. Conclusions

The preceding analysis has revealed a number of findings relevant to consumer perceptions of privacy in the mobile environment. First is that, while respondents believe that sharing data in the mobile environment poses privacy risks, they do not generally take the steps necessary to address these risks, such as ensuring that a privacy policy exists or reading the applicable policy. Such a finding indicates that privacy policies are not adequate methods of informing consumers about the risks their use of certain applications and services may pose to the privacy of their personal and travel information. This finding indicates a disconnect between consumer perceptions of privacy in the mobile environment, and the steps they take to protect this privacy. Findings such as those related to different perceptions of the degree to which users feel different information types put their privacy at risk are quite revealing, as they emphasize the lack of understanding by users of how information used in different contexts may be highly revealing of personal habits and behaviors.

A second finding is that privacy preferences of participants are impacted in large part both by personal characteristics, such as gender, education, and degree of extraversion, and by the contextual factors surrounding the potential sharing of location data – such as whether data are to be shared with public or private agencies, with law enforcement, or within a social network. This finding indicates again that privacy policies may not be the most adequate default method of ensuring privacy protection, as they are static documents that may not effectively respond to privacy concerns in all situations.

Findings also indicate that willingness to trade private travel data is dependent upon a number of factors related to context, personal characteristics, expected benefits and degree of trust in the collecting agency (as indicated by risk perceptions). Here, acknowledgement that willingness to trade is, again, not a static concept (though related to a person's overall demographics and characteristic) supports the need to expand consumer-driven or controlled methods used for privacy protection beyond traditional privacy policies. Such methods could include both technological means of privacy protection as well as policies that acknowledge contextual conflicts and promote consumer awareness and control dependent upon situational preferences. Evidence that willingness to trade may be influenced by degree and type of compensation and benefits also supports the need to incorporate appropriate incentives into LBS and ITS systems in order to encourage adoption and use. While further research is needed to address specific systemic needs, initial findings suggest that safety and efficiency benefits may have the greatest impacts on consumer perceptions of risk mitigation, particularly if combined with attention paid to types of mobility information and benefits identified as important by the consumer.

5. Discussion

As seen above, consumers may not currently be aware of the actual privacy implications of their actions and behaviors regarding smart mobility ICTs, in particular with respect to the lack of attention paid to privacy policies relative to risk assessment. For example, consumers overall are highly unwilling to release name and address information, but will sell or trade trip origin, destination, and route data. Such data, however, may be easily used (depending on degree of cloaking or perturbation used) to aggregate and identify individual trip patterns. With this information, it is relatively simple to identify individual travelers and their route destinations if data are mined, or combined with publicly accessible records such as White Pages. If consumers are unaware of such potential uses, they are incapable of effectively valuing these data, and may share more than they would otherwise be willing. Particularly in regard to the recent increase in the use of location-sensing cell phones and smartphones, the amount of travel data available to public and private transportation and mobility agencies is growing exponentially, and with it the potential for misuse. If, for example, consumers begin to receive marketing information or political literature based on patterns of behavior or travels determined from location data sold to a third party, the public's concerns may rise and usage levels of smart mobility ICTs may drop.

In the context of trust issues outlined above, such a finding indicates that with a lack of awareness and guidance regarding specific privacy concerns relevant to use of collected data, persons with higher indicated privacy concerns may be less willing to adopt proposed and implemented transportation technologies due to a perceived risk of privacy invasion. Here, awareness of specific location-related privacy concerns may be subsumed by general feelings of distrust or privacy concern. As proposals are made for implementing ubiquitous mobile transportation technologies at the vehicular level, such a finding may have serious implications. If persons do not feel that they can trust the handling of their data by the manufacturers and/or mechanics of such vehicles, they may strive to “opt-out” of the system. This would, in turn, have implications for the efficacy of the system, as widespread adoption will be necessary to provide an adequate amount of real-time data. Such concerns are especially relevant in the context of public investments in mobile technologies such as networked ITS systems, as consumers with especially high degrees of privacy concerns may have an underlying distrust in public agencies. Here, lack of awareness of factors that might mitigate privacy concerns in the mobile environment (such as anonymizing techniques, cloaking, pseudonyms, and other such technological methods of privacy protection) may lead consumers to have a more heightened degree of privacy concern than is reasonable.

This lack of awareness, both of privacy concerns and protections, is a difficult issue to address. Currently, privacy policies are the primary method used to inform consumers about the collection, use and management of their data in the mobile environment. As consumers often do not read these policies, however, their ability to accurately evaluate the privacy risks of sharing mobile data is compromised. Many current privacy protections have focused primarily on technological and policy-oriented solutions, which essentially place the onus of privacy protection in the hands of policy-makers and technologists; however, public expectations of privacy are not necessarily reflected in the decisions of these agents. While such efforts are necessary, further efforts should be made to more effectively work on co-design efforts that marry technical, policy, and educational methods of privacy protection to better ensure both utility and understanding.

The disconnect seen here indicates that more efforts are needed to move privacy protection “downstream,” via such methods as education and grassroots efforts, in collaboration with product and system designers. While there are public-interest research groups and non-profits, such as the Electronic Privacy Information Center (epic.org) and the Privacy Rights Clearinghouse, that focus on the issue of privacy, few high-profile consumer-driven location privacy advocacy groups exist. As consumers become more aware of privacy issues in the mobile environment, this may change; however, basic educational tools will be needed to ensure that correct information is disseminated and that the risks and benefits of sharing privacy in the mobile environment are accurately represented. Incorporating the risks of sharing data via the use of smartphone apps into basic technological and computing classes would be one method of promoting greater consumer awareness, or incorporating such information into driver’s education classes. As this issue gains more visibility, grassroots groups promoting greater awareness may naturally evolve, but as a complex issue much education will be needed.

Another useful tool would be transparent and comprehensive policies related to the collection, storage, sharing, and use of data, perhaps tied to specific techniques to ensure their effectiveness. Policies that would require implementing agencies to provide clear “opt-in” choices based on types of data to be collected and disseminated and their probable uses would encourage greater consumer awareness and understanding of the relative risks and benefits of sharing data in the mobile environment. An additional step that could be taken would be analogous to the FCRA requirement that consumers have free access yearly to credit reports, including information regarding entities that have requested a person’s credit history. In this scenario, for example, location-based application providers would be required to disclose to wireless service providers those third parties with whom they have shared customer location data. This information could be aggregated and provided to customers on a yearly basis by request, in order to ensure that consumers have a clear understanding of the amount of data that has been disseminated. Taking such actions would place more onus on application developers and companies to provide clear data to consumers, and would enable consumers to make better decisions regarding sharing of data in the mobile environment. Combining these two factors would, in addition, provide consumers with a greater perception of control over their data (as they would be able to opt-out of those services which they feel are privacy invasive), thus potentially alleviating some degree of risk perception and encouraging adoption of ITS and LBS services.

A further point is that the above should take place in a collaborative environment that facilitates co-design activities between the users of mobile ICTs and their developers. If systems are developed such that consumers are able to see clear relationships between policy protections, data needs, and technological applications, it may be possible to engender a more grounded sense of trust on the part of the consumer (see related work from (Ackerman *et al.* 2001). Such activities could take place, for example, in co-design of systems to facilitate the provision of options for differentiated location privacy levels based on consumer preferences and incorporating considerations of both context and trust.

Such concerns may also be allayed by ensuring that manufacturers and distributors of ubiquitous mobile transportation technologies are bound by comprehensive rules and regulations guiding the treatment and handling of data collected in the mobile environment. By providing a groundwork of trust, consumers will have a basis for determining their use of mobile technologies in accordance with reasonable expectations of privacy as codified by law. Such a step should be augmented by providing transparent and adequate information regarding degree of data protection, including appropriate information for steps to be taken if consumers are uncomfortable with protections given, or feel that their data have been mishandled. If consumers are provided with adequate and transparent methods of addressing privacy concerns, this may help increase their trust in the implemented systems, and their overall willingness to adopt mobile technologies. Additionally, if consumers are kept informed of methods being used to protect their private data, they will be more likely to trust in collecting entities.

References

Ackerman, Mark, Trevor Darrell, and Daniel J. Weitzner. "Privacy in context." Human–Computer Interaction 16.2-4 (2001): 167-176.

Acquisti, A., Grossklags, J., 2005. Privacy and rationality in individual decision making. IEEE Secur. Priv. Mag. 3, 26–33. doi:10.1109/MSP.2005.22

Barkhuus, L., Dey, A.K., 2003. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns., in: INTERACT. Citeseer, pp. 702–712.

Berendt, B., Günther, O., Spiekermann, S., 2005. Privacy in e-commerce: stated preferences vs. actual behavior. Commun. ACM 48, 101–106. doi:10.1145/1053291.1053295

Baik Hoh, Gruteser, M., 2005. Protecting Location Privacy Through Path Confusion. IEEE, pp. 194–205. doi:10.1109/SECURECOMM.2005.33

Boyles, J.L., Smith, A., Madden, M., 2012. Privacy and data management on mobile devices. Pew Internet Am. Life Proj.

Cottrill, C.D., 2009. Approaches to Privacy Preservation in Intelligent Transportation Systems and Vehicle-Infrastructure Integration Initiative. Transp. Res. Rec. J. Transp. Res. Board 2129, 9–15. doi:10.3141/2129-02

Danezis, G., Lewis, S., Anderson, R.J., 2005. How much is location privacy worth?, in: WEIS. Citeseer.

Dediu, H., 2010. Nielsen: Nearly 25 percent of US adults use smartphones. Asymco.

DeLong, J.B., Froomkin, M., 2000. Speculative microeconomics for tomorrow's economy, in: Internet Publishing and beyond: The Economics of Digital Information and Intellectual Property. pp. 6–44.

Gosling, S.D., Rentfrow, P.J., Swann, W.B., 2003a. A very brief measure of the Big-Five personality domains. J. Res. Personal. 37, 504–528. doi:10.1016/S0092-6566(03)00046-1

Gosling, S.D., Rentfrow, P.J., Swann, W.B., 2003b. A very brief measure of the Big-Five personality domains. J. Res. Personal. 37, 504–528. doi:10.1016/S0092-6566(03)00046-1

Hoh, B., Iwuchukwu, T., Jacobson, Q., Work, D., Bayen, A.M., Herring, R., Herrera, J.-C., Gruteser, M., Annavaram, M., Ban, J., 2012. Enhancing Privacy and Accuracy in Probe Vehicle-Based Traffic Monitoring via Virtual Trip Lines. IEEE Trans. Mob. Comput. 11, 849–864. doi:10.1109/TMC.2011.116

Hui, K.-L., Png, I.P.L., 2006. The Economics of Privacy, in: Hendershott, T., Whinston, A.B. (Eds.), Economics and Information Systems, Handbooks in Information Systems. Elsevier, Boston, MA, pp. 1–27.

Junglas, I.A., Johnson, N.A., Spitzmüller, C., 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur. J. Inf. Syst. 17, 387–402. doi:10.1057/ejis.2008.29

Korzaan, M.L., Boswell, K.T., 2008. THE INFLUENCE OF PERSONALITY TRAITS AND INFORMATION PRIVACY CONCERNS ON BEHAVIORAL INTENTIONS. J. Comput. Inf. Syst. 48.

Krause, A., Horvitz, E., 2008. A Utility-Theoretic Approach to Privacy and Personalization. J. Artif. Intell. Res. 39, 1181–1188.

Krumm, J., 2008. A survey of computational location privacy. Pers. Ubiquitous Comput. 13, 391–399. doi:10.1007/s00779-008-0212-5

Lee, S.Y., 2014. Examining the factors that influence early adopters' smartphone adoption: The case of college students. Telemat. Inform. 31, 308–318. doi:10.1016/j.tele.2013.06.001

Li, N., Chen, G., 2010. Sharing location in online social networks. IEEE Netw. 24, 20–25. doi:10.1109/MNET.2010.5578914

Mascetti, S., Freni, D., Bettini, C., Wang, X.S., Jajodia, S., 2011. Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies. VLDB J. 20, 541–566. doi:10.1007/s00778-010-0213-7

Matsuo, H., McIntyre, K.P., Tomazic, T., Katz, B., 2004. The online survey: Its contributions and potential problems., in: ASA Proceedings of the Section on Survey Research Methods. Presented at the American Statistical Association, pp. 3998–4000.
Munnukka, J., 2007. Characteristics of early adopters in mobile communications markets. Mark. Intell. Plan. 25, 719–731. doi:10.1108/02634500710834188
Nissenbaum, H.F., 2010. Privacy in context technology, policy, and the integrity of social life. Stanford Law Books, Stanford, Calif.
Patil, S., Norcie, G., Kapadia, A., Lee, A., 2012. "Check out where I am!": location-sharing motivations, preferences, and practices. ACM Press, p. 1997. doi:10.1145/2212776.2223742
Pew Research Internet Project, 2014. Mobile Technology Fact Sheet | Pew Research Center's Internet & American Life Project [WWW Document]. URL http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (accessed 4.15.14).
Phelps, J., Nowak, G., Ferrell, E., 2000. Privacy concerns and consumer willingness to provide personal information. J. Public Policy Mark. 27–41.
Puttaswamy, K.P.N., Wang, S., Steinbauer, T., Agrawal, D., Abbadi, A.E., Kruegel, C., Zhao, B.Y., 2014. Preserving Location Privacy in Geosocial Applications. IEEE Trans. Mob. Comput. 13, 159–173. doi:10.1109/TMC.2012.247
Slobogin, C., 2003. Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity. SSRN Electron. J. doi:10.2139/ssrn.364600
Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information privacy: Measuring individuals' concerns about organizational practices. MIS Q. 20, 167–196.
Stewart, K.A., Segars, A.H., 2002. An empirical examination of the concern for information privacy instrument. Inf. Syst. Res. 13, 36–49.
Stigler, G., 1980. An Introduction to Privacy in Economics and Politics. J. Leg. Stud. 9, 623–644.
Sun, Z., Zan, B., Ban, X. (Jeff), Gruteser, M., 2013. Privacy protection method for fine-grained urban traffic modeling using mobile sensors. Transp. Res. Part B Methodol. 56, 50–69.
Tang, K.P., Lin, J., Hong, J.I., Siewiorek, D.P., Sadeh, N., 2010. Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing, in: Proceedings of the 12th ACM International Conference on Ubiquitous Computing. ACM, pp. 85–94.
Ten Sythoff, J., Morrison, J., 2011. Location-Based Services: Market Forecast, 2011-2015. Pyramid Research.
Thakuriah, P., and Geers, G. (2013) Transportation and Information: Trends in Technology and Policy. Series: Springer briefs in computer science . Springer, New York, NYC, USA. ISBN 9781461471288
Westin, A.F., 2003. Social and Political Dimensions of Privacy. J. Soc. Issues 59, 431–453. doi:10.1111/1540-4560.00072
Xie, H., Kulik, L., Tanin, E., 2011. Privacy-aware collection of aggregate spatial data. Data Knowl. Eng. 70, 576–595. doi:10.1016/j.datak.2011.03.007
Xu, H., Luo, X. (Robert), Carroll, J.M., Rosson, M.B., 2011. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decis. Support Syst. 51, 42–52. doi:10.1016/j.dss.2010.11.017
Zangui, M., Yin, Y., Lawphongpanich, S., Chen, S., 2013. Differentiated congestion pricing of urban transportation networks with vehicle-tracking technologies. Transp. Res. Part C Emerg. Technol. 36, 434–445.
Zhang, L., Levinson, D., 2008. Determinants of Route Choice and Value of Traveler Information: A Field Experiment. Transp. Res. Rec. J. Transp. Res. Board 2086, 81–92. doi:10.3141/2086-10
Zickuhr, K., 2012. Three-quarters of smartphone owners use location-based services. Pew Internet Am. Life Proj.

Zimmer, M., 2008. Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine. J. Bus. Technol. Law 3, 109–126.