JOURNAL OF INFORMATION SYSTEMS
Vol. 28, No. 1
Spring 2014
pp. 227–242

American Accounting Association
DOI: 10.2308/isys-50696

Understanding the Components of Information Privacy Threats for Location-Based Services

Robyn L. Raschke
Anjala S. Krishen
Pushkin Kachroo
University of Nevada, Las Vegas

ABSTRACT: Given the increase in global positioning system enabled devices and the ubiquitous ability to connect wirelessly to information through location-based services, organizations are challenged to offer privacy-by-design support systems. Given this, we offer a conceptual framework to capture the impact of the individual component weights of concern for information privacy on behavioral intent of disclosing information. Through a sample of 217 respondents, our PLS model shows that privacy protection beliefs negatively impact concern for collection, unauthorized use, and improper access of information and that privacy risk beliefs positively impact concern for collection and existence of errors; additionally, concern for collection negatively impacts behavioral intentions to disclose information, as does concern for unauthorized use. With such detailed information, firms can address both cognitive and affective consumer concerns, enhance transparency, and communicate multiple services while handling privacy controls as an extension of those services.

Keywords: privacy by design; privacy protection beliefs; privacy risk beliefs; location-based services; PLS.

I. INTRODUCTION

Organizations involved in location-based services (LBS) have a tremendous potential to transform the mobile industry, as well as the user experience. Due to the increase in the number of global positioning system (GPS) enabled devices and the ubiquitous ability to connect wirelessly to information, the projected revenue for LBS is expected to increase from $2.8 billion in 2010 to $10.3 billion in 2015 (Pyramid Research 2011). LBS require a GPS-enabled device that collects location data through either a wireless connection or a cell tower. LBS applications include vehicle navigation and tracking (e.g., OnStar), social tracking (e.g., Foursquare, Twitter, Facebook), location-based search (e.g., Google, Yelp), as well as location-based advertising (e.g., on-site casino promotions).

We gratefully acknowledge the Nevada Department of Transportation for their support and feedback of this research. Robyn L. Raschke and Anjala S. Krishen contributed equally as first authors.

Editor's note: Accepted by Miklos A. Vasarhelyi.

Published Online: January 2014

However, with the opportunities provided to consumers by this technology come the responsibility and the challenges faced by organizations to provide accurate and secure information. In particular, firms need to adequately communicate their ability to protect an individual's information privacy. The business need to protect consumer privacy is so intense and timely that research suggests that accounting firms also extend their branding to include privacy-related services (Greenstein and Hunton 2003; Vandervelde 2003). Open communication and best practice with regard to consumer privacy are important not only for building trust with organizations (Culnan and Armstrong 1999), but also for fulfilling ethical and public policy standards and ensuring consumer security (Milne 2000; Weidenmier and Ramamoorti 2006).

To this end, the Federal Communications Commission (FCC 2012) issued a report on the opportunities, as well as considerations, to encourage industry best practices in safeguarding consumer's personally identifiable information. The FCC panelists find that industry and corporate responses on privacy protection are varied and, therefore, recognize the need for government to provide baseline standards for privacy. In particular, they recommend that the focus should not be overly specific, but rather be widely applied to a range of situations. The panelists discuss the concept of privacy by design (PbD) and the capability of organizations to implement this approach within their product development stage. The PbD approach advocates that organizations consider privacy from a proactive perspective and embed it in the early stages of design through seven principles of Fair Information Practices (Cavoukian 2010). In a similar vein, the Federal Trade Commission (FTC 2012) recently issued a report encouraging organizations to use a PbD solution in developing LBS products. Thus, the recommendations from the FCC and FTC reports emphasize the need for organizations to balance information privacy concerns with the advantages of LBS through a design perspective.

Importantly, product design is not one-sided and requires that organizations consider consumer feedback (Bloch 1995). A design perspective requires human knowledge to create a conceptualization of what ought to be (Simon 1969). Furthermore, Bélanger and Crossler (2011) conduct an extensive review of information privacy in the IS research and identify a "gap" in the literature noting that user input is not adequately examined in relation to conceptual design research of information privacy tools and technologies. Therefore, in order for organizations to understand how to embed privacy into LBS design, they must also understand detailed privacy components from a user perspective.

The information systems literature has developed and tested a multidimensional construct that measures the specific components that relate to an individual's privacy concern regarding an organization's information practices (Smith, Milberg, and Burke 1996; Stewart and Segars 2002). In addition, prior research proposes that risk is an antecedent to privacy concerns and suggests that individuals use a privacy calculus in their decision-making process to weigh the costs and benefits of each choice before determining whether to disclose their information online (Dinev and Hart 2006; Li, Sarathy, and Xu 2011). Privacy calculus theory assumes that an individual's intent to disclose information is based upon their consideration and tradeoffs for risks and benefits; the theory therefore elucidates the joint effects of the opposing beliefs on intentions (Xu, Teo, Tan, and Agarwal 2009; Li 2012). Privacy calculus is complex and involves a multitude of considerations that raise or reduce privacy concerns. Examples of conditions under which privacy concerns can increase include perceived risks, computer anxiety, and previous experiences (Dinev and Hart 2006; Stewart and Segars 2002; Bansal, Zahedi, and Gefen 2010). On the other hand, existing literature shows that reputation, privacy policies, and controllability may reduce privacy concerns (Andrade, Kaltcheva, and Weitz 2002; Chen, Ping, Xu, and Tan 2009).

The present research examines the relationship between the cost/benefit considerations of an individual's privacy calculus and their concern for information practices within the specific context of an LBS technology and their subsequent intent to disclose information. In particular, we propose a model that separates specific privacy subcomponents and shows the differential impact on behavioral intention to disclose information. The challenges faced by organizations in meeting privacy-by-design standards are immense; included are (1) distinguishing privacy from security in its fundamental definition, (2) developing implementation mechanisms for privacy integration into systems, and (3) furthering knowledge of the tangible and intangible benefits and risks of privacy practices by companies (Spiekermann 2012). Findings of the proposed model not only augment the recent LBS and privacy research, but also contribute to organizations by elucidating how the elements of Concern for Information Privacy (CFIP) may be incorporated into a PbD perspective in the future for other specific LBS technologies.

The remainder of the paper is organized as follows. Section II is a discussion of the LBS privacy research and the development of hypotheses. Section III describes the research method and the context of the study, data collection, and analysis. Finally, Section IV concludes with a discussion of the model results and contributions to the literature, as well as insights for practice.

II. BACKGROUND AND HYPOTHESES

Smith, Dinev, and Xu (2011) recently provide a comprehensive literature review on privacy, recommending that future researchers consider a macro model of privacy (APCO) from which to frame positivist research:

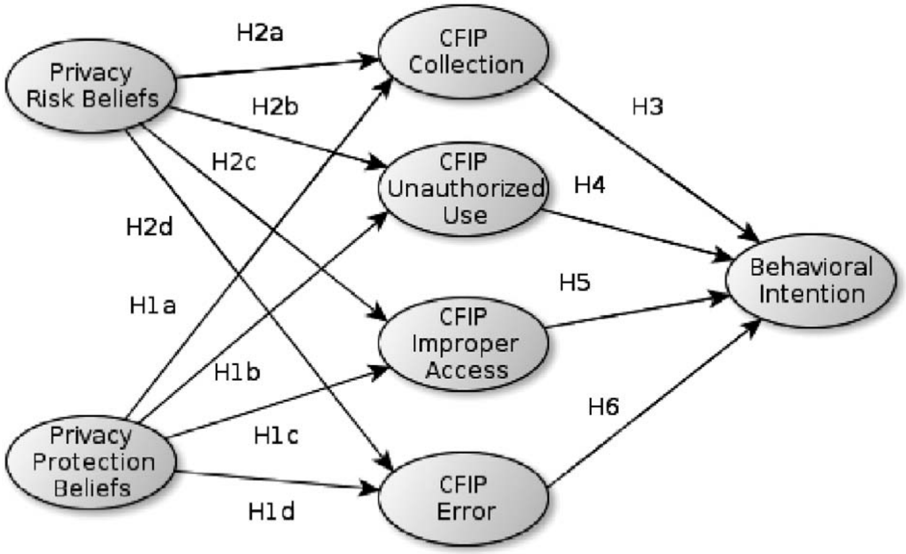
Antecedents → Privacy Concerns → Outcomes.

According to Smith and colleagues, a majority of research attention primarily focuses on the link between privacy concerns and outcomes, whereas very few studies address the link between antecedents and privacy concerns. In addition, the authors suggest that future empirical studies on privacy will add more value to the literature if researchers consider the macro model and examine the relationships between antecedents to privacy concerns and outcomes (Smith et al. 2011).

Although privacy research is multidisciplinary and broad in nature, evolving over decades, the APCO macro model of privacy provides a structure by which to guide the proposed research model, which is framed within the specific context of interest in an LBS technology. Moreover, with regard to online website privacy research, Li (2014) suggests that situation-specific privacy concerns from an online perspective may have a stronger impact on information disclosure than general privacy concerns. It is important to draw the distinction between general versus situation specific privacy concerns; by doing so, researchers can unravel the intricacies of individual privacy issues (Bennett 1992; McKnight, Choudhury, and Kacmar 2002; Malhotra, Kim, and Agarwal 2004; Li 2014). Thus, in light of the macro model and the suggestion that privacy is "situation specific," the present study contributes to existing literature by examining individual privacy concerns within the context of an LBS technology.

The constructs and hypotheses developed for this study fit appropriately within the APCO framework. In particular, Concern for Information Privacy (CFIP) is used for privacy concerns and behavioral intent is the outcome from which to examine relationships within the framework. Privacy risk beliefs are considered an antecedent of privacy concern (Pavlou 2011; Dinev and Hart 2006). This study specifically focuses on the privacy beliefs using privacy calculus theory; namely, privacy risk beliefs (PRB) and privacy protection beliefs (PPB). Privacy risk belief is the potential loss one feels in releasing personal information to an organization (Malhotra et al. 2004), whereas privacy protection belief is an individual subjective belief that a certain vendor will protect an individual's private information as expected (Pavlou and Chellappa 2001). Li et al. (2011) examine the cost/benefit calculus between PRB and PPB in an online setting and suggest that individual beliefs and dispositions can factor into the privacy calculation. For example, Li, Sarathy, and Xu (2010) show that by untangling these privacy beliefs into two separate constructs, their impact on

FIGURE 1
Conceptual Model



behavioral intentions produce varied results. They note that in an online setting, participants who exemplify high privacy protection beliefs perceive more control over their information and are more likely to disclose it. In this case the PRB is deemed as a cost of privacy while PPB is considered a benefit. On the whole, previous research shows that both PRB and PPB are impactful individual differences variables; given this importance, the present model proposes them as antecedents.

In relation to individual or personality traits, PRB and PPB are only two of an exhaustive set of antecedents from which researchers can examine privacy under the APCO framework (Smith et al. 2011). These antecedents are important for understanding how individuals compare their multiple beliefs and make tradeoffs as applied through privacy calculus theory. Therefore, this study focuses on these two antecedents to preserve the parsimony of the model.

Concern for information privacy consists of four subconstructs: (1) collection; (2) error; (3) unauthorized use; and (4) improper access (Smith et al. 1996; Junglas, Johnson, and Spitzmueller 2008). Known as a reliable construct and *de facto* measure of information privacy concerns (Bélanger and Crossler 2011), the four dimensions of CFIP are also well aligned with the FTC's fair information practices (Bansal, Zahedi, and Gefen 2008; FTC 2000). The FTC (2000) stipulates that consumers be given: (1) notice that their personal information is being collected on any activity (*CFIP-Collection*); (2) access to personal information for data accuracy (*CFIP-error*); (3) consent to appropriate use of collected information (*CFIP-unauthorized use*); and (4) security to prevent unauthorized access (*CFIP-improper access*). The conceptualized model is shown in Figure 1.

Although there are several foundational studies that examine privacy within the context of LBS technologies, none have examined it within a framework focusing on the design perspective. Barkhuus and Dey (2003) examine the relationship of several mobile location services and concern for information privacy using case study methodology with 16 participants. They find that location-tracking services generate a higher privacy concern than do position aware services. In addition, their findings indicate that if the service is useful, individuals indicated less of a concern for their privacy. Perhaps the most notable related research to date in LBS is Junglas et al. (2008);

these authors were forerunners in their examination of the link between several antecedents focusing on personality traits and concern for information privacy within the area of cellular phones. As a result of their findings, Junglas et al. (2008) suggest that potential value can be gleaned by widening the scope of their sample and including mandatory users of a technology. Finally, Xu et al. (2009) examine privacy calculus (benefits and risks) within the context of general push-and-pull-based LBS and the effect on intentions to disclose personal information. Even though all of these seminal studies investigate privacy within the specific and general context of LBS, none of them utilize the full APCO framework.

Antecedents to concern for privacy include several personality traits such as agreeableness, conscientiousness, emotional stability, extraversion, and openness (Junglas et al. 2008; Korzaan and Boswell 2008). In addition to emotional antecedents, perceived relevance, considered as a measure of consumer fairness concerns, is also an antecedent of both privacy protection belief and privacy risk belief (Li et al. 2010). Perceived fairness of privacy policies, much like perceived fairness of taxation policies (Krishen, Raschke, and Mejza 2010), is an important cognitive determinant of willingness to disclose information or voluntarily cooperate with proposed policies. Similarly, privacy risk and protection beliefs are an individual trait. The Li et al. (2011) research model mainly examines the relationship between PRB and PPB on the outcome behavioral intention within an online context, finding that PRB is negatively associated with intent, while PPB is positively associated with intent.

In relation to the proposed model and using the APCO framework, the cost/benefit analysis of privacy calculus is related to an individual's concern for information privacy for LBS technology. In addition, to understand concern for information privacy from a design perspective, the multidimensional construct of CFIP should be unraveled to understand the intricacies of privacy concern and its effects with the other constructs of interest in the model under the APCO framework. Organizations can benefit from research that considers the separate effects of each component of CFIP as the effect of these components may be contingent upon the specific context of interest. Specifically, an individual's high (low) privacy protection belief about a vendor's ability to protect their information can be related to a decrease (increase) in their concern for privacy. This leads to the following hypotheses:

H1a: PPB is negatively associated with the CFIP threat—Collection.

H1b: PPB is negatively associated with the CFIP threat—Unauthorized use.

H1c: PPB is negatively associated with the CFIP threat—Improper access.

H1d: PPB is negatively associated with the CFIP threat—Existence in errors.

Conversely, an individual's high (low) privacy risk belief can be related to high (low) feelings of threats in their concern for privacy toward LBS. It is thus contended that:

H2a: PRB is positively associated with the CFIP threat—Collection.

H2b: PRB is positively associated with the CFIP threat—Unauthorized use.

H2c: PRB is positively associated with the CFIP threat—Improper access.

H2d: PRB is positively associated with the CFIP threat—Existence in errors.

The broad construct of concern for information privacy has a direct and negative relationship on the behavioral intention to engage in privacy-related risk reduction by consumers (Stewart and Segars 2002; Korzaan and Boswell 2008). However, most existing research shows that general privacy concern directly influences behavioral intention, without specifying the differentiated impacts of each of the components of concern for privacy (Li et al. 2011). Given the conceptual

TABLE 1

Study Demographics

Variable	Frequency	Percentage	Mean	Range
Gender				
Female	153	56%		
Male	119	44%		
Majority percentage of driving spent for:				
Work ($\geq$ 50 percent)	142	52%		
Non-work ($\geq$ 50 percent)	82	30%		
Not disclosed	48	18%		
Age			30	16–78
Annual household income			$67,000	$1,500–$200,000
Miles driven per week			185	15–840

interest within a design perspective of privacy, the present study hypothesizes that the individual components of CFIP will be related to the behavioral intention to disclose private information as follows:

H3: A negative association exists between the CFIP threat of collection and intentions.

H4: A negative association exists between the CFIP threat of unauthorized use and intentions.

H5: A negative association exists between the CFIP threat of improper access and intentions.

H6: A negative association exists between the CFIP threat of existence in errors and intentions.

III. RESEARCH METHOD

A survey instrument was administered to 272 non-student respondents using a quota-convenience snowball sampling methodology to understand perspectives of privacy with an LBS technology. Qualification for the study required that respondents not be enrolled as students in a university. Previous research utilizes this method that consists of data collectors randomly asking individuals to participate in an online survey (Mick 1996; Bui, Krishen, and LaTour 2012). For the context of this study, research shows that the quota-convenience technique, also known as a structured snowball sample (S. Sarker, S. Sarker, and Jana 2010), or a respondent-driven sampling method (Warkentin, Johnston, and Shropshire 2011), produces a statistically disperse sample that is generalizable and ecologically valid (Snijders 1992). In fact, newer research indicates that in comparison to several other sampling techniques, quasi-convenience samples, such as snowball, do not create estimation issues or biases, especially when the sample size is large, as in this study (X. Chen, Y. Chen, and Xiao 2013). The context for the survey involved the use of an LBS technology as an alternative solution to collect fuel tax. This LBS technology will keep track of mileage driven and will not record locations driven. Currently, fuel tax is calculated per gallon of fuel purchased and paid at the pump; however, the alternative proposed solution is based on actual miles driven (Krishen et al. 2010; Krishen, Raschke, Kachroo, LaTour, and Verma forthcoming). In order to explain the vehicle tax policy to our respondents, the survey included a short explanation (see Appendix A). Table 1 includes demographic information of the respondents. The sample consists of respondents who are 56 percent female and 44 percent male. The respondents have an average annual salary of $67,000, and drive an average of 185 miles each week. Of the 272 respondents surveyed, 217 surveys were complete and were therefore used in the analysis to test the model. All items in the survey use 7-point Likert scales (anchored with 1 = strongly disagree and 7 = strongly agree) and have been validated in prior literature lending to the reliability of the measures; these are provided in Table 2 for each construct.

Results

Prior to testing the hypotheses, we first assess the initial loadings of the measures on each construct. Table 3 provides the cross loadings for all of the measures for the model constructs. Three measures were dropped due to poor loadings (Iacobucci 2009, 2010). Table 4 shows the cross loadings of the model with the remaining measures. The model constructs are assessed for reliability, and convergent and discriminant validity. Table 5 provides the construct convergent and discriminant validity (Panels A and B, respectively). The model shows convergent validity because all average variance extracted (AVE) scores are greater than 0.50 and discriminant validity because the AVE is larger than cross correlations with other constructs (Fornell and Larker 1981). We also tested for common methods bias, because respondents answered questions about both the independent and dependent variables. The Harmon one-factor test indicated that one factor accounts for only 29 percent of the total variance in the independent and dependent measures. This is below the 50 percent threshold for common method bias (Podsakoff and Organ 1986).

Partial Least Squares (PLS) is used to test the hypotheses and examine the predictiveness of the model (Chin 1995). H1a through H1d relate to the negative relationship between privacy protection beliefs and the component threats of concern for information privacy. All paths are significant ($p < 0.05$) with the exception of the relationship between PPB and Error, which is not significant. Thus, H1d is not supported. H2a through H2d relate to the positive relationship between privacy risk beliefs and the component threats of concern for information privacy. The paths between PRB and Collection, as well as PRB and Error are significant ($p < 0.05$); however, the paths between PRB and Unauthorized use, as well as the path PRB and Improper Access, are not significant. Thus, H2b and H2c are not supported.

H3 through H6 examine the relationships between the components of concern for information privacy and the intent to disclose private information. We hypothesized a negative relationship between these constructs. The paths between Collection and Intent, as well as the path between Unauthorized use and Intent are significant ($p < 0.05$), whereas the paths between Error and Intent are not significant. The path between Improper Access and Intent is significant, but not in the intended direction. Thus, H3 and H4 are supported, whereas H5 and H6 are not supported. Table 6 provides a summary of the results of the hypotheses.

The model is tested for its predictive quality using the Stone-Geisser's (Q^2) test of predictive relevance for the dependent variable (Intent). The Stone-Geisser Q^2 value (Geisser 1974; Stone 1974) is 0.13. Given that the Q^2 value for an endogenous construct is greater than 0, the model has predictive relevance (Hair, Ringle, and Sarstedt 2011).

Although we did not hypothesize the relationships between PPB and Intent, as well as PRB and Intent, prior literature shows that PPB is positively related to Intent, whereas PRB is negatively related to Intent (Li et al. 2011). To confirm that the model fits with previously confirmed research, we *post hoc* ran the model with these relationships and found that these relationships are indeed significant. In addition, we also ran *post hoc* analysis assessing the mediating qualities of the individual threat components of CFIP as theorized by Smith et al. (1996) and also depicted from the APCO framework. The only significant mediating component is Collection, which is a partially mediating variable for both PPB and Intent (Sobel Test $p = 0.04$, one-tailed) as well as PRB and

TABLE 2

Constructs and Measures

Privacy Protection Belief (Li et al. 2011)	
PPB1	I am confident that I know all of the parties who would collect information if I transact with the NDOT VMT system.
PPB2	I am aware of the exact nature of information that will be collected during a transaction with the NDOT VMT system.
PPB3	I believe I have control over how my information will be used by NDOT if I transact with the VMT system.
PPB4	I believe I can subsequently verify the information I provide during a transaction with NDOT.
PPB5	I believe there is a mechanism to address violation of information I provide to NDOT.
Privacy Risk Belief (Li et al. 2011)	
PRB1	It would be risky to disclose my VMT information to NDOT.
PRB2	There would be high potential for loss associated with disclosing my VMT information to NDOT.
PRB3	There would be too much uncertainty associated with giving my VMT information to NDOT.
PRB4	Providing NDOT with my VMT information would involve many unexpected problems.
Concern for Privacy—Collection (Junglas et al. 2008)	
COLL1	It bothers me that NDOT stores my information.
COLL2	It bothers me when my information is available to NDOT.
COLL3	I am concerned that NDOT will collect too much information about me.
COLL4	I am comfortable with the idea that NDOT is able to track me at any time.
COLL5	I would rather not provide my information to NDOT.
Concern for Privacy—Unauthorized Use (Junglas et al. 2008)	
UNAUTH1	NDOT should not disclose information to unauthorized parties.
UNAUTH2	NDOT should never share information without my consent.
UNAUTH3	NDOT should not use my information for any purpose unless it has been authorized by me.
UNAUTH4	NDOT should never sell information about its customers to other companies.
Concern for Privacy—Improper Access (Junglas et al. 2008)	
ACCESS1	NDOT should devote a lot of time and effort to preventing unauthorized access to information.
ACCESS2	Databases that contain location information should be protected from unauthorized access—no matter how much it costs.
ACCESS3	NDOT should take more steps to make sure that unauthorized people cannot access personal information.
Concern for Privacy—Error (Junglas et al. 2008)	
ERROR1	All information should be double-checked for accuracy—no matter how much it costs.
ERROR2	NDOT should take a lot of steps to make sure that the information in their databases is accurate.
ERROR3	NDOT should have thorough procedures to correct errors in information.
Behavioral Intent to Give Personal Information (Li et al. 2011)	
INTENT1	I am likely to reveal my VMT information to NDOT.
INTENT2	It is probable that I will reveal my VMT information to NDOT.
INTENT3	It is possible that I will reveal my VMT information to NDOT.
INTENT4	I am willing to reveal my VMT information to NDOT.

TABLE 3

Initial Factor Analysis

	PPB	PRB	Collect	Unauth.	Access	Error	Intent
PPB1	0.853	−0.079	−0.209	−0.342	−0.201	−0.087	0.334
PPB2	0.797	−0.130	−0.210	−0.206	−0.078	−0.048	0.303
PPB3	0.879	−0.126	−0.258	−0.357	−0.255	−0.156	0.355
PPB4[a]	0.503	−0.185	−0.164	−0.121	−0.009	0.002	0.384
PPB5[a]	0.479	−0.047	−0.105	−0.068	0.052	0.038	0.310
PRB1	−0.087	0.858	0.462	0.031	0.051	0.145	−0.387
PRB2	−0.053	0.884	0.447	0.006	−0.013	0.148	−0.367
PRB3	−0.204	0.915	0.555	0.190	0.095	0.253	−0.479
PRB4	−0.142	0.877	0.486	0.172	0.134	0.224	−0.391
COLL1	−0.194	0.530	0.909	0.035	0.050	0.127	−0.373
COLL2	−0.174	0.475	0.860	0.015	0.044	0.149	−0.331
COLL3	−0.208	0.489	0.853	0.176	0.121	0.172	−0.323
COLL4[a]	−0.320	0.077	0.153	0.312	0.196	0.085	−0.249
COLL5	−0.187	0.321	0.650	0.241	0.158	0.117	−0.319
UNAUTH1	−0.275	0.007	0.012	0.786	0.479	0.390	0.017
UNAUTH2	−0.240	0.064	0.088	0.837	0.520	0.370	−0.106
UNAUTH3	−0.375	0.160	0.229	0.899	0.534	0.349	−0.246
UNAUTH4	−0.270	0.132	0.174	0.837	0.663	0.371	−0.201
ACCESS1	−0.195	0.069	0.094	0.617	0.908	0.551	−0.053
ACCESS2	−0.192	0.069	0.146	0.552	0.917	0.523	−0.076
ACCESS3	−0.172	0.090	0.128	0.635	0.928	0.485	−0.044
ERROR1	−0.038	0.213	0.146	0.171	0.335	0.801	−0.104
ERROR2	−0.098	0.209	0.183	0.432	0.574	0.934	−0.141
ERROR3	−0.154	0.165	0.140	0.527	0.574	0.882	−0.089
Intent1	0.412	−0.428	−0.432	−0.193	−0.075	−0.151	0.925
Intent2	0.411	−0.401	−0.374	−0.171	−0.046	−0.091	0.952
Intent3	0.351	−0.401	−0.335	−0.121	−0.022	−0.079	0.914
Intent4	0.406	−0.480	−0.452	−0.197	−0.082	−0.144	0.918

[a] Items dropped due to low loadings.

Intent (Sobel Test p = 0.02, one-tailed). Figure 2 provides the path coefficients for all hypothesized relationships in our model.

IV. DISCUSSION AND CONCLUSION

Given recent research that calls for studies in the area of privacy, including consumer attitudes and beliefs regarding privacy, the present study proposes and validates a conceptual model that weighs the relative importance of different types of consumer privacy concerns related to location-based services on behavioral intentions (Kauffman, Lee, Prosch, and Steinbart 2011). The resultant findings indicate the importance of unraveling the intricacies related to the specific components of privacy concerns and their relative weight on consumer intentions to disclose.

Even though the hypotheses indicate that PRB and PPB have impacts on all four components of CFIP, the findings ultimately show that certain relationships are significant, whereas others are not. In particular, PRB does not have a significant influence on either the unauthorized use or the improper access dimensions of CFIP. Those relationships were not significant, in major part,

TABLE 4

Final Factor Analysis

	PPB	PRB	Collect	Unauth.	Access	Error	Intent
PPB1	0.876	−0.078	−0.168	−0.342	−0.201	−0.089	0.334
PPB2	0.800	−0.130	−0.191	−0.206	−0.079	−0.049	0.303
PPB3	0.890	−0.126	−0.216	−0.357	−0.255	−0.158	0.355
PRB1	−0.066	0.858	0.460	0.030	0.051	0.143	−0.387
PRB2	−0.037	0.884	0.446	0.005	−0.013	0.147	−0.367
PRB3	−0.189	0.915	0.551	0.190	0.095	0.253	−0.479
PRB4	−0.126	0.876	0.477	0.170	0.134	0.224	−0.390
COLL1	−0.187	0.530	0.917	0.034	0.050	0.125	−0.373
COLL2	−0.171	0.475	0.881	0.014	0.043	0.148	−0.330
COLL3	−0.199	0.489	0.860	0.175	0.121	0.171	−0.323
COLL5	−0.192	0.321	0.649	0.240	0.158	0.118	−0.319
UNAUTH1	−0.285	0.007	−0.029	0.788	0.480	0.395	0.017
UNAUTH2	−0.257	0.064	0.041	0.840	0.521	0.376	−0.106
UNAUTH3	−0.389	0.159	0.192	0.899	0.534	0.353	−0.246
UNAUTH4	−0.268	0.132	0.143	0.833	0.663	0.374	−0.201
ACCESS1	−0.219	0.068	0.067	0.616	0.910	0.555	−0.053
ACCESS2	−0.211	0.068	0.124	0.551	0.915	0.525	−0.076
ACCESS3	−0.191	0.090	0.101	0.633	0.928	0.489	−0.044
ERROR1	−0.026	0.213	0.161	0.171	0.335	0.790	−0.104
ERROR2	−0.124	0.209	0.166	0.432	0.574	0.937	−0.141
ERROR3	−0.174	0.165	0.114	0.528	0.574	0.889	−0.089
Intent1	0.377	−0.428	−0.400	−0.192	−0.075	−0.151	0.925
Intent2	0.375	−0.401	−0.345	−0.170	−0.045	−0.091	0.952
Intent3	0.305	−0.402	−0.315	−0.120	−0.022	−0.077	0.914
Intent4	0.371	−0.480	−0.418	−0.196	−0.082	−0.144	0.918

because of the possibility that the government context does not increase risk beliefs for these components. The present study contextualizes LBS privacy in the setting of a transportation tax through a governmental institution; as such, individuals may not be as concerned with the unauthorized use or improper access to their information because they may have more trust in the government than they would in a private organization. In addition, since the LBS collects mileage driven and the information is considered at the aggregate level and not detailed with locations driven to, this may also be a reason that the relationships between these constructs are not significant. However, the results do suggest that future research address these insignificant paths in a for-profit commercial setting to determine whether those relationships would become significant, as well as consider the level of specificity of the information. In addition, PPB does not significantly impact concern for error in our model; possibly this finding is due to the fact that individuals may not believe they have much control over errors from governmental agencies, especially in relation to taxes. Whereas concern for collection and unauthorized use both have a significant impact on behavioral intention to disclose information, the model did not indicate significant impacts for concern for error. We attribute the non-significant results of this path due to the definition of error that includes cost terminology that may force the individual to contemplate costs associated with privacy. This becomes particularly relevant when considering that the context for the study is a government tax and, as such, costs are particularly avoidable to the general public. Future research may be able to examine the effects of cost by understanding the cost burden within different

TABLE 5
Construct Validation

Panel A: Construct Values and Reliability Measures

Construct	Mean	Std. Dev.	AVE	CR	Cronbach's Alpha
PPB	2.92	1.55	0.73	0.89	0.82
PRB	3.99	1.73	0.78	0.93	0.91
Collect	4.54	1.69	0.69	0.90	0.85
Unauth.	6.35	1.19	0.71	0.91	0.87
Access	6.14	1.35	0.84	0.94	0.91
Error	5.26	1.42	0.76	0.91	0.84
Intent	3.77	1.62	0.86	0.96	0.95

Definitions:
AVE = Average Variance Extracted; and
CR = Composite Reliability.

Panel B: Construct Correlation Table

Construct	PPB	PRB	Collect	Unauth.	Access	Error	Intent
PPB	**0.86**						
PRB	−0.13	**0.88**					
Collect	−0.22	0.55	**0.83**				
Unauth.	−0.37	0.12	0.13	**0.84**			
Access	−0.23	0.08	0.11	0.65	**0.92**		
Error	−0.13	0.22	0.17	0.44	0.57	**0.87**	
Intent	0.39	−0.46	−0.40	−0.19	−0.06	−0.13	**0.93**

Latent Variable square root of the AVE is on the diagonal in bold.

contexts of a consumer's "willingness to pay" versus the cost burden to a for-profit concern to correct errors. Furthermore, the relationship between concern for improper access and behavioral intention is significant, but the hypothesized relationship is opposite of what was expected. It is clear to see that with this component, the privacy calculus tradeoffs are evident. In this case, privacy protection beliefs are much stronger than privacy risk beliefs for concern for improper access; as such, the concern for improper access is reduced, and participants are more likely to disclose information.

Most importantly, the present findings suggest that since privacy is context specific, technology designers should consider privacy calculus feedback of potential users during the design phase for the specific components of information privacy concerns. In particular, by understanding which information privacy concern component has more bearing on behavioral intentions, design efforts can become better focused and can reduce or mitigate any potential concerns. In particular, when government policies mandate the use of a technology, the effects of poor planning may potentially result in low trust in the organization and low perceived fairness of the proposed policy. In the case of profit-oriented firms, the effect of inadequate *a priori* privacy measures could ultimately result in loss of reputation and revenues. Therefore, it is important that informational communications and promotions address both cognitive and affective consumer concerns, enhance transparency, and communicate multiple services while addressing privacy controls as an extension of those services

TABLE 6

Summary of Hypothesis Testing

Hypothesis	Finding
H1a: PPB is negatively associated with the CFIP threat—Collection.	Supported
H1b: PPB is negatively associated with the CFIP threat—Unauthorized use.	Supported
H1c: PPB is negatively associated with the CFIP threat—Improper access.	Supported
H1d: PPB is negatively associated with the CFIP threat—Existence in errors.	Not Supported
H2a: PRB is positively associated with the CFIP threat—Collection.	Supported
H2b: PRB is positively associated with the CFIP threat—Unauthorized use.	Not Supported
H2c: PRB is positively associated with the CFIP threat—Improper access.	Not Supported
H2d: PRB is positively associated with the CFIP threat—Existence in errors.	Supported
H3: A negative association exists between the CFIP threat of collection and intentions.	Supported
H4: A negative association exists between the CFIP threat of unauthorized use and intentions.	Supported
H5: A negative association exists between the CFIP threat of improper access and intentions.	Not Supported
H6: A negative association exists between the CFIP threat of existence in errors and intentions.	Not Supported

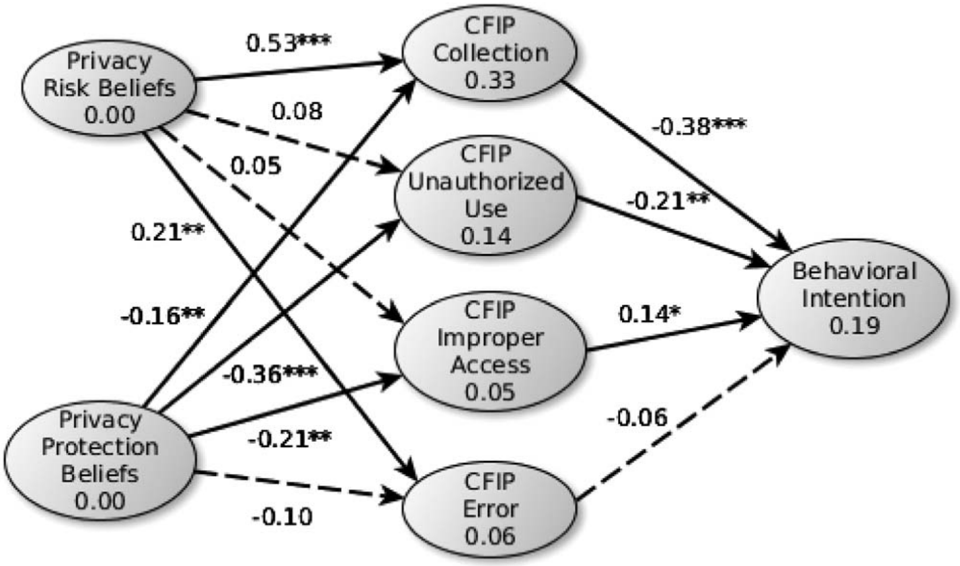
(Greenstein and Hunton 2003). According to Boritz and No (2011), the three areas of privacy focus include the customer perspective, the privacy solution provider, and government regulation. Our research focuses mainly on the customer perspective, but provides guidelines for both government institutions and privacy solution providers for ways to communicate privacy components and the relative importance of each of them.

Limitations and Future Research

Although our research was limited to the specific context of an LBS solution from a government entity, future research should examine the generalizability of the CFIP component relationships to determine if they behave consistently without regard to type of LBS technology, as well as provider of the application (government versus commercial). In addition, whereas the study context was limited to the approach of an LBS technology to calculate miles traveled, future research should examine if our model produces consistent results when more sensitive information is collected, such as location tracking LBS technology. Recent research by Xu, Crossler, and Belanger (2012) proposes a privacy enhancing decision support tool that would enable users to control their privacy settings in a more interactive fashion and thus increase their privacy perceptions. In their privacy-by-design approach, Xu and colleagues (2012) follow up their design by acquiring feedback from potential users. Future research could survey users of their privacy-by-design system to ascertain the relative weightings of privacy components for individuals and their impact on behavioral intent to disclose information.

An additional avenue for future research would be the cross-cultural extensions of the model, specifically testing whether independent (such as U.S.) versus interdependent (such as China) cultural orientations have similar or different perceptual effects on privacy components. As such, previous research shows that whereas both the U.S. and China have privacy concerns, they originate from legal issues for U.S. consumers and family relationships for Chinese consumers (Eining and Lee 1997). Finally, future research could augment our ideas and model with additional

FIGURE 2
Final Model



*, **, *** p-value < 0.05 (one-tailed t-statistic > 1.65), < 0.01 (one-tailed t-statistic > 2.343), and < 0.001 (one-tailed t-statistic > 3.126), respectively.

individual differences or traits such as need for cognition, internal and external locus of control, and regulatory focus orientation (i.e., prevention versus promotion).

This study extends existing research that specifically addresses LBS applications and privacy concerns. We examined an LBS privacy model using the proposed APCO macro framework suggested by Smith et al. (2011). Our findings show that the individual component threats of concern for information privacy have differing levels of impact on the behavioral intent to disclose private information. These results are of use for practitioners who are interested in developing LBS applications using the privacy-by-design perspective.

REFERENCES

Andrade, E. B., V. Kaltcheva, and B. Weitz. 2002. Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research* 29 (1): 350–353.

Bansal, G., F. M. Zahedi, and D. Gefen. 2010. The impact of personal dispositions on information sensitivity, privacy concern, and trust in disclosing health information online. *Decision Support Systems* 49 (2): 138–150.

Bansal, G., F. Zahedi, and D. Gefen. 2008. *The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation*. Proceedings of 29th Annual International Conference on Information Systems, Paris, France.

Barkhuus, L., and A. Dey. 2003. *Location-Based Services for Mobile Telephony: A Study of User's Privacy Concerns*. Proceedings of the 9th IFIP TC13 International Conference on Human-Computer Interaction (INTERACT), Zurich, Switzerland.

Bélanger, F., and R. E. Crossler. 2011. Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* 35 (4): 1017–1041.

Bennett, C. J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

Bloch, P. H. 1995. Seeking the ideal form: Product design and consumer response. *Journal of Marketing* 59 (3): 16–29.

Boritz, J. E., and W. G. No. 2011. E-Commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems* 25 (2): 11–45.

Bui, M., A. S. Krishen, and M. LaTour. 2012. When kiosk retailing intimidates shoppers: How gender-focused advertising can mitigate the perceived risks of the unfamiliar. *Journal of Advertising Research* 52 (3): 1–18.

Cavoukian, A. 2010. *Privacy by Design: The 7 Foundational Principles*. Available at: http://www.privacybydesign.ca/

Chen, J., W. Ping, Y. Xu, and B. C. Y. Tan. 2009. *Am I Afraid of My Peers? Understanding the Antecedents of Information Privacy Concerns in the Online Social Context*. Proceedings of the Thirtieth International Conference on Information Systems, Phoenix, AZ, December 15–18.

Chen, X. L., Y. X. Chen, and P. Xiao. 2013. The impact of sampling and network topology on the estimation of social inter-correlations. *Journal of Marketing Research* 50 (1): 95–110.

Chin, W. W. 1995. Partial Least Squares is to LISREL as principal components analysis is to common factor analysis. *Technology Studies* 2: 315–319.

Culnan, M. J., and P. K. Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science* 10 (1): 104–115.

Dinev, T., and P. Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17 (1): 61–80.

Eining, M. M., and G. M. Lee. 1997. Information ethics: An exploratory study from an international perspective. *Journal of Information Systems* 11 (1): 1–17.

Federal Communications Commission (FCC). 2012. *Location-Based Services: An Overview of Opportunities and Other Considerations*. Available at: http://www.fcc.gov/document/location-based-services-report

Federal Trade Commission (FTC). 2000. *Privacy Online for Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*. Available at: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Fornell, C., and D. F. Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18 (3): 39–50.

Geisser, S. 1974. A predictive approach to the random effects model. *Biometrika* 61 (1): 101–107.

Greenstein, M. M., and J. E. Hunton. 2003. Extending the accounting brand to privacy services. *Journal of Information Systems* 17 (2): 87–110.

Hair, J. F., C. M. Ringle, and M. Sarstedt. 2011. PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice* 19 (2): 139–151.

Iacobucci, D. 2009. Everything you always wanted to know about SEM (structural equations modeling) but were afraid to ask. *Journal of Consumer Psychology* 19 (4): 673–680.

Iacobucci, D. 2010. Structural equations modeling: Fit indices, sample size, and advanced topics. *Journal of Consumer Psychology* 20 (1): 90–98.

Junglas, I. A., N. A. Johnson, and C. Spitzmueller. 2008. Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems* 17 (4): 387–402.

Kauffman, R. J., Y. J. Lee, M. Prosch, and P. J. Steinbart. 2011. A survey of consumer information privacy from the accounting information systems perspective. *Journal of Information Systems* 25 (2): 47–79.

Korzaan, M. L., and K. T. Boswell. 2008. The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems* 48 (4): 15–24.

Krishen, A. S., R. L. Raschke, and M. Mejza. 2010. Guidelines for shaping perceptions of fairness of transportation infrastructure policies: The case of the vehicle mileage tax. *Transportation Journal* 49 (3): 24–38.

Krishen, A. S., R. Raschke, P. Kachroo, M. LaTour, and P. Verma. Forthcoming. Promote me or protect us? The framing of policy for collective good. *European Journal of Marketing*.

Li, H., R. Sarathy, and H. Xu. 2010. Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems* 51 (1): 62–71.

Li, H., R. Sarathy, and H. Xu. 2011. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems* 51 (3): 434–445.

Li, Y. 2012. Theories in online information privacy research: A critical review and an integrative framework. *Decision Support Systems* 54: 471–481.

Li, Y. 2014. A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications* 13 (1): 32–44.

Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15 (4): 336–355.

McKnight, D. H., V. Choudhury, and C. Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research* 13 (3): 334–359.

Mick, D. G. 1996. Are studies of dark side variables confounded by socially desirable responding? The case of materialism. *Journal of Consumer Research* 23 (2): 106–119.

Milne, G. R. 2000. Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing* 19 (1): 1–6.

Pavlou, P. A. 2011. State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly* 35 (4): 977–988.

Pavlou, P. A., and R. K. Chellappa. 2001. *The Role of Perceived Privacy and Perceived Security in the Development of Trust in Electronic Commerce Transactions*. Los Angeles, CA: USC.

Podsakoff, P. M., and D. W. Organ. 1986. Self-reports in organizational research: Problems and prospects. *Journal of Management* 12 (4): 531–544.

Pyramid Research. 2011. *Research Report: Location-Based Services Market Forecast, 2011–2015*. Available at: http://www.pyramidresearch.com/store/Report-Location-Based-Services.htm

Sarker, S., S. Sarker, and D. Jana. 2010. The impact of the nature of globally distributed work arrangement on work-life conflict and valence: The Indian GSD professionals' perspective. *European Journal of Information Systems* 19 (2): 209–222.

Simon, H. 1969. *The Sciences of the Artificial*. Cambridge, MA: MIT Press.

Smith, H. J., S. J. Milberg, and S. J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20 (2): 167–196.

Smith, H. J., T. Dinev, and H. Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35 (4): 989–1015.

Snijders, T. A. B. 1992. Estimation on the basis of snowball samples: How to weight? *Bulletin of Sociological Methodology* 36 (1): 59–70.

Spiekermann, S. 2012. The challenges of privacy by design. *Communications of the ACM* 55 (7): 38–40.

Stewart, K. A., and A. H. Segars. 2002. An empirical examination of the concern for information privacy instrument. *Information Systems Research* 13 (1): 36–49.

Stone, M. 1974. Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society* 36 (2): 111–147.

Vandervelde, S. D. 2003. Discussion of extending the accounting brand to privacy services. *Journal of Information Systems* 17 (2): 111–114.

Warkentin, M., A. Johnston, and J. Shropshire. 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems* 20 (3): 267–284.

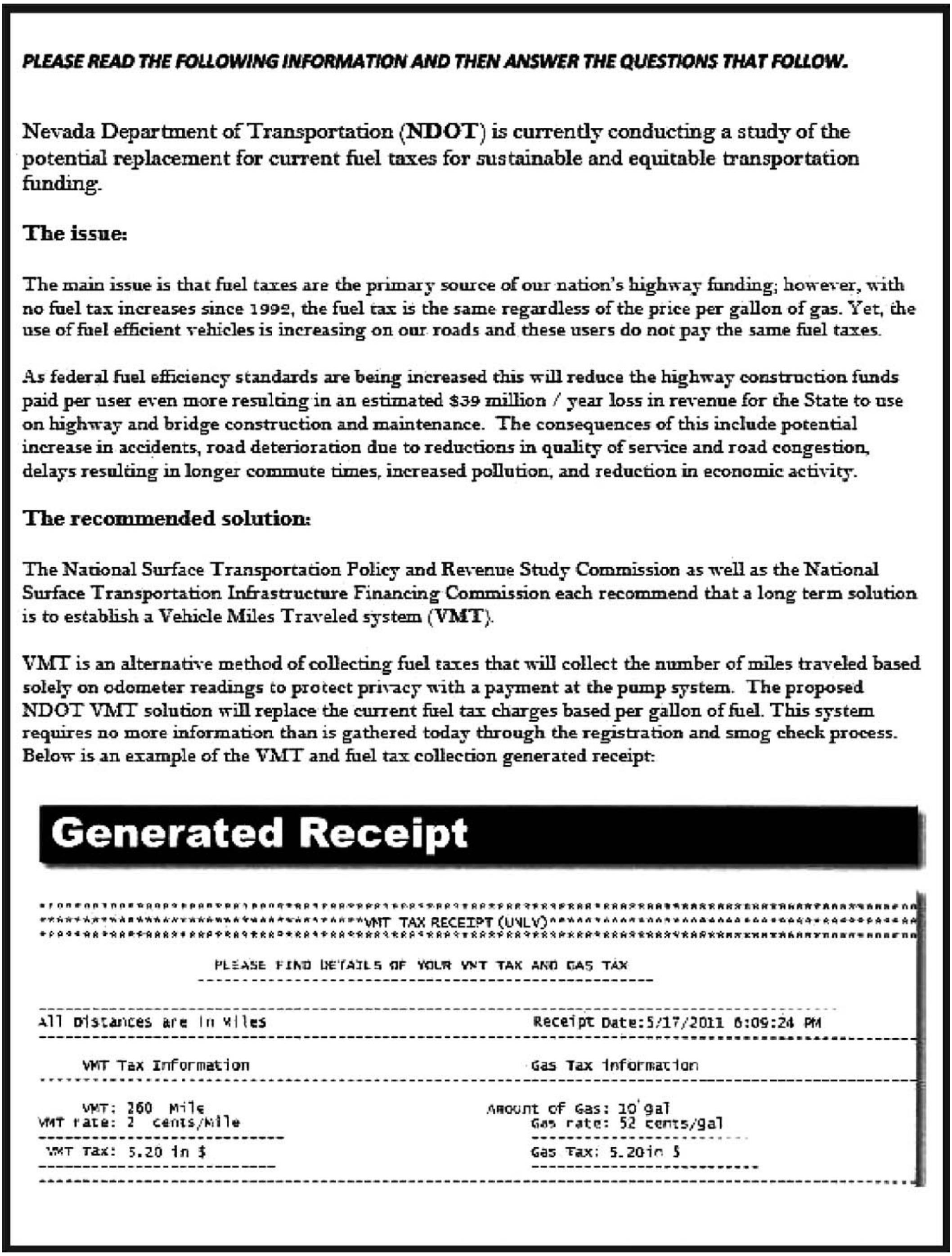
Weidenmier, M. L., and S. Ramamoorti. 2006. Research opportunities in information technology and internal auditing. *Journal of Information Systems* 20 (1): 205–219.

Xu, H., H. H. Teo, B. C. Y. Tan, and R. Agarwal. 2009. The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems* 26 (3): 135–173.

Xu, H., R. E. Crossler, and F. Bélanger. 2012. A value sensitive design investigation of privacy enhancing tools in web browsers. *Decision Support Systems* 54 (1): 424–433.

APPENDIX A

Study Context



PLEASE READ THE FOLLOWING INFORMATION AND THEN ANSWER THE QUESTIONS THAT FOLLOW.

Nevada Department of Transportation (**NDOT**) is currently conducting a study of the potential replacement for current fuel taxes for sustainable and equitable transportation funding.

The issue:

The main issue is that fuel taxes are the primary source of our nation's highway funding; however, with no fuel tax increases since 1992, the fuel tax is the same regardless of the price per gallon of gas. Yet, the use of fuel efficient vehicles is increasing on our roads and these users do not pay the same fuel taxes.

As federal fuel efficiency standards are being increased this will reduce the highway construction funds paid per user even more resulting in an estimated $39 million / year loss in revenue for the State to use on highway and bridge construction and maintenance. The consequences of this include potential increase in accidents, road deterioration due to reductions in quality of service and road congestion, delays resulting in longer commute times, increased pollution, and reduction in economic activity.

The recommended solution:

The National Surface Transportation Policy and Revenue Study Commission as well as the National Surface Transportation Infrastructure Financing Commission each recommend that a long term solution is to establish a Vehicle Miles Traveled system (VMT).

VMT is an alternative method of collecting fuel taxes that will collect the number of miles traveled based solely on odometer readings to protect privacy with a payment at the pump system. The proposed NDOT VMT solution will replace the current fuel tax charges based per gallon of fuel. This system requires no more information than is gathered today through the registration and smog check process. Below is an example of the VMT and fuel tax collection generated receipt:

Generated Receipt

```
**********************************************************************************************
*****************************************VMT TAX RECEIPT (UNLV)*******************************
**********************************************************************************************

                     PLEASE FIND DETAILS OF YOUR VMT TAX AND GAS TAX
                   ----------------------------------------------------

-------------------------------------------------------------------------------------------
All Distances are in Miles                               Receipt Date:5/17/2011 6:09:24 PM
----------------------------------------------------------------------------------------------

     VMT Tax Information                                 Gas Tax information
----------------------------------------------------------------------------------------------

     VMT: 260  Mile                                  Amount of Gas: 10 gal
VMT rate: 2  cents/Mile                                  Gas rate: 52 cents/gal
-----------------------------                            -------------------------
 VMT Tax: 5.20 in $                                      Gas Tax: 5.20in $
-----------------------------                            --------------------------
----------------------------------------------------------------------------------------------
```

Copyright of Journal of Information Systems is the property of American Accounting Association and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.