12-15-2019

Exploring Information Disclosure in Location-based Services: U.S. vs. German Populations

Dana Naous

Christine Legner

Exploring Information Disclosure in Location-based Services: U.S. vs. German Populations

Completed Research Paper

Dana Naous
Faculty of Business and Economics (HEC), University of Lausanne
1015 Lausanne, Switzerland
dana.naous@unil.ch

Christine Legner
Faculty of Business and Economics (HEC), University of Lausanne
1015 Lausanne, Switzerland
christine.legner@unil.ch

Abstract

Location-based services (LBSs) have enabled users to obtain context-specific and personalized services owing to advances in mobile technologies and location analytics. Since location data are classified as personally identifiable, the sharing of locations on LBSs has privacy implications. We employ a privacy calculus lens to study users' attitudes toward location-information sharing. We explore the role of cultural and institutional environments in users' disclosure behaviors in two populations: the U.S. and Germany. Our results show similarities between the two samples, despite differences in cultural backgrounds and regulations. Contextualization is a highly valued benefit for LBS users, while monetary rewards are not yet foreseen as potential benefits. Location-information disclosure is not uniform; it varies depending on the sharing parties and the information extent or sensitivity. LBS users have high privacy risk perceptions and low trust in service providers and government regulations to protect their privacy and location-information from misuse.

Keywords: Location-information disclosure, location-based services, privacy calculus, risk-benefit tradeoffs.

Introduction

Advances in mobile technologies equipped with location tracking functionalities have resulted in a new category of services that enables users to explore their surroundings. These location-based services (LBSs) span several domains, from navigation, advertising, recommender systems, to social networks. LBSs operate using positioning technologies such as the Global Positioning System (GPS), WiFi connections, IPs, and the triangulation of cellular network information (Cheng et al. 2006; Farkas et al. 2016). With advanced technologies, including Internet of Things (IoT) and analytics, data are easy to collect, analyze, and use by different entities. This has given rise to the emerging field of location analytics (Pick et al. 2017), which uses specialized spatial analysis techniques to understand geographical patterns and relationships, including hotspot areas, spatial clusters, buffers, and proximity polygons (Farkas et al. 2015). Location analytics has generated strong interest from the advertising industry, tourism and destination managers, and security agencies, since they enable micro-targeting people and provide context-specific, personalized services. They can also help improve public services, i.e., to trace criminal records, ease cities' traffic flows (Rudgard 2018), and as the foundation for urban planning and smart cities (Miah et al. 2019). However, since location data act as a bridge of users' offline and online lives, sharing location information on LBSs has privacy implications (Krumm 2007). In fact, location data combined with location analytics serves as a diagnostic representation of sensitive demographic attributes

such as religious and political affiliation, sexual orientation, financial status, and health status (Gambs et al. 2011).

Existing research has mostly focused on privacy-preserving algorithms or techniques such as encryption or access control (Zhu and Cao 2011). At the same time, there has been very little empirical research into user preferences for location-information disclosure. While early studies revealed that people cared little about privacy (Krumm 2007), a handful of studies have investigated users' motivations to share location data through a privacy calculus lens (Sun et al. 2015; Zhou 2011; Xu et al. 2009; Dinev and Hart 2006). These studies treated location-information disclosure as a result of a tradeoff analysis between expected benefits and perceived privacy risks. As LBSs are penetrating our daily lives, and regulations (such as EU-GDPR) impose higher privacy standards, users' attitudes are likely to change. To explore these implications, we ask: What are users' attitudes on location-information disclosure in LBSs and the roles of cultural and institutional environments on the uses of such services?

Our study is based on an extended privacy calculus model that reflects a more realistic and holistic picture of location-information disclosure than previous studies (Naous et al. 2019). We consider location-information sharing not as a uniform user behavior, but as a multi-dimensional construct that reflects tradeoffs between benefits from sharing location data and the related intrinsic and extrinsic privacy risks (Morlok 2016; Olteanu et al. 2017). Based on data collected from 1,055 respondents in Germany and the U.S., we study the dynamics behind users' risk-benefit tradeoffs in location-information disclosure. We assess the impact of privacy regulations on disclosure behaviors, taking an intercultural lens, as suggested by Krasnova et al. (2012) and Krasnova and Veltri (2010) for user self-disclosure in the context of social networks.

Interestingly, both samples share more similarities than differences, despite their specific cultural and institutional environments. The average user is willing to share location-information for contextualized services, but avoids continuous tracking of mobility traces or the sharing of sensitive information. Further, users preferred sharing only with service providers, with no further access to their data by third parties. Our results provide relevant insights into adoption patterns and users' attitudes for researchers, policymakers, and LBS providers.

The remainder of this paper is structured as follows: We first discuss prior research on privacy in the context of LBSs, presenting our conceptual model for location-information disclosure. Next, we present our research design. We then analyze the results along our research model's constructs. Finally, we discuss the findings and conclude with cultural implications on disclosure behaviors.

Theoretical Background

Prior research

In LBSs, users share their locations to achieve certain goals, such as finding nearby locations, navigation, and social networking. While location sharing is important to achieve accurate results and reliable recommendations in LBSs, there are privacy threats associated to them, given that they allow open access to personal data derived from user location-information via location analytics. Location privacy has mostly been treated by the computer science community through designing location privacy models and privacy-preserving algorithms or techniques (Krumm 2007). These techniques, such as cloaking, allow users to mask their location traces before sharing them on LBSs in lower resolution in terms of time and space, thereby achieving anonymity for users (Cheng et al. 2006; Zhu and Cao 2011). While this provides flexibility and control for users, allowing them to use LBS securely, it creates more challenges for service design, since the quality of the provided location traces can be affected, which – in turn – affects these services' performance and outcomes.

Compared to the number of publications on location privacy, there is very little empirical research into users' location-information disclosure preferences. In the IS literature, location-information sharing is a form of self-disclosure, where users communicate their locations to the LBS providers and possibly to other service members. The research into location information disclosure in IS has mainly employed the privacy calculus and supporting theories to study risk-benefit tradeoffs. Among these studies, Xu et al. (2009) developed a framework to link three privacy assurance mechanisms with location information disclosure: technology control, industry self-regulation, and government legislation. They studied these

mechanisms' effects in context-specific scenarios with two LBS application types, including safety and advertising, as well as location-based social networks. Similarly, Sun et al. (2014, 2015) studied location information disclosure in social networks, considering the benefit structure ruling of this disclosure as well as gender differences. Other privacy calculus-based contributions, including Keith et al. (2013), have studied practical information disclosure based on realistic risk perceptions, and have proposed a pragmatic experimental methodology to capture true privacy risk perceptions' effects on information disclosure decisions.

Conceptual Model for Location-Information Disclosure

The privacy calculus lens provides an understanding of the motivations and rationales behind information sharing, considering the costs and benefits associated with sharing behaviors. However, the existing studies have applied a very simplistic conceptualization that does not reflect the realities of information disclosure in LBSs. We extended constructs from previous studies to represent disclosure on multiple dimensions that relate to the realistic settings and nature of location information. Our high-level conceptual model with its multi-dimensional constructs appears in Figure 1.

Foremost, location-information sharing is not a uniform user behavior. In fact, we suggest considering three relevant dimensions that surround disclosure behaviors with certain conditions: (1) extent, (2) sensitivity, and (3) sharing parties. Extent relates to *how much* location information is disclosed, which reflects information breadth (Wheeless and Grotz 1976). It can be classified as continuous disclosure on applications that require uninterrupted tracking of user locations or trajectory tracing (normally via uninterrupted GPS access), or sporadic disclosure via discrete sharing of location points for a specific use (e.g., finding a nearby shop). Location sensitivity relates to which location information *type* is disclosed by a user, corresponding to the information's depth or intimacy (Wheeless and Grotz 1976). It comprises sensitive, personally identifiable information such as financial status, political affiliation, and religious affiliation, which can be revealed using simple heuristics (Gambs et al. 2011). Finally, sharing parties describe *to whom* information is disclosed, also contributing to the depth aspect. This involves service providers via direct application usage and can also entail service members or users who belong to the platform community, as well as third parties through proxy services or governments through urban planninginitiatives.

One major benefit of LBSs is contextualization. Xu et al. (2009) suggested three context variables (time-dependent, position-dependent, and user-dependent) for using LBSs, resulting in two anticipated benefits: (1) locatability, as the ability to access needed information in context at the right time and in the right place, and (2) personalization, as obtaining targeted recommendations and getting relevant content depending on a user's context. Further, studies on information disclosure have highlighted the importance of symbolic or hedonic benefits. Associated to the enjoyment factor (Krasnova et al. 2010), LBS users can disclose so as to project a social image, for instance, being present in certain places and/or with influential people. Finally, incentives, in the form of insurance premiums, discounts, or monetary rewards can positively affect location-information disclosure and can even outweigh risk perceptions.

Location-information can be used to uncover users' identities, classify consumers, and track their behaviors based on their mobility patterns (Xu et al. 2009). Thus, LBSs hold privacy risks relating to malicious or improper access to and usage of user data and privacy invasions. These risks extend beyond personal privacy and include extrinsic ones. With the introduction of location context into social networks, users not only share their personal location-information, but also disclose information about their friends and family in their network. Interdependent location disclosure leads to revealing the colocation information of others, compromising their privacy (Morlok 2016). Privacy risk perceptions can be moderated via two main constructs: trust and privacy control settings (Xu et al. 2009; Krasnova et al. 2010). We built on Dinev and Hart's (2006) definition of trust as an individual's belief that a counter-party involved in an interaction has characteristics that prevent them from utilizing opportunistic behaviors. Three parties are generally engaged in LBS usage contexts: service providers (based on their treatment of data), service members (based on their LBS behaviors), and governments (based on their privacy regulations). Privacy control settings are a key measure for achieving information privacy (Malhotra et al. 2004). People feel more comfortable in using an application if they have the option to allow data sharing or the choice to opt out. This is normally achieved via effective and transparent privacy policies and regulations (Betzing et al. 2019) that enforce data governance on users' information and

describe how service providers and third parties may use this information. Practically, mobile users should be able to limit the amount of location information collected by service providers via privacy control mechanisms that support notice, consent, proximity, and locality (Anuket 2003).

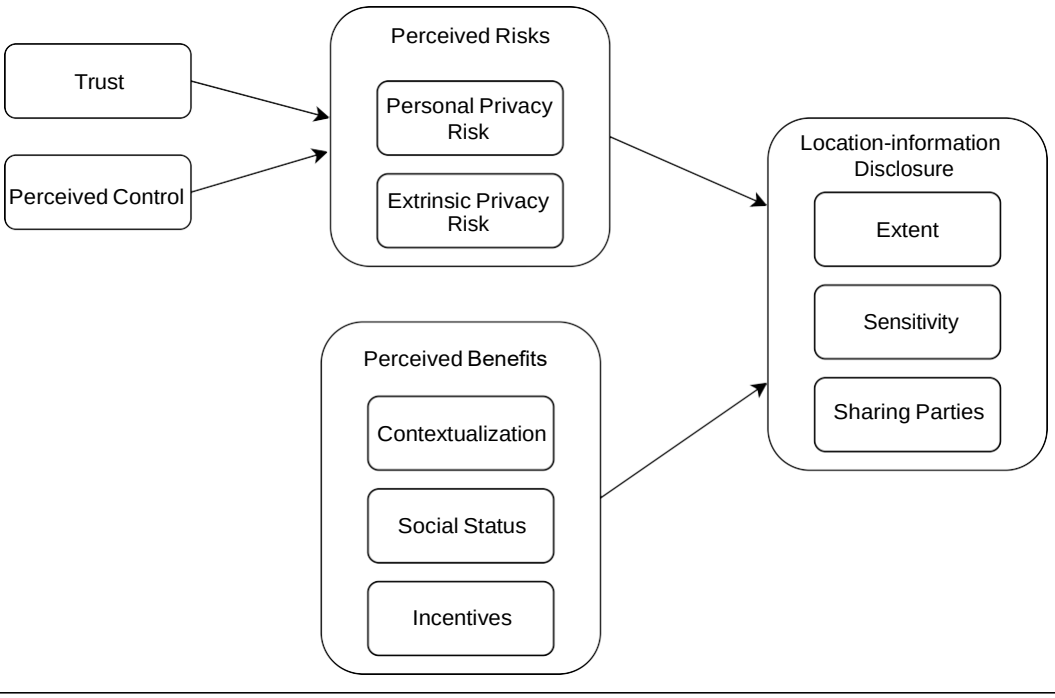

Figure 1. Conceptual model for location-information disclosure

Culture and Institutional Environment's Impact on Location-information Disclosure

Cultural and institutional environment factors have gained importance in studying adoption behaviors in IS research (Jiang and Ji 2009). Institutional environment factors differ between countries, which can also impact on LBSs. For instance, after Edward Snowden's revelations, the applicability of privacy laws in the U.S. has been questioned, although the U.S. constitution prohibits the unreasonable search and seizure of personal information. This implies that privacy protection in the U.S. still relies mainly on industry self-regulation (Bellman et al. 2004). The European Union (EU), seeking to strengthen data protection and privacy for their citizens, has implemented the General Data Protection Regulation (GDPR), which prescribes requirements for the collection, storage, processing, and management of personal data (Pankowska 2018). The GDPR has acknowledged the criticality of location-information as personally identifiable by making it part of its definition of *personal data*. The public discussion and legislation change users' perceptions toward LBS usages and can affect their adoption.

Concerning cultural factors, Krasnova et al. (2012) revealed that culture influences the risk-benefit tradeoffs for information disclosure on social networking sites. Based on these findings and previous studies on e-commerce, it can be argued that cultural characteristics contribute to individuals' risk and benefit perceptions, which – in turn – influence their decisions to use LBSs and to disclose location information. Most studies on cultural differences have relied on Hofstede's (2001) typology of culture and five dimensions: (1) power distance index (PDI), corresponding to the degree of hierarchy established and executed in society, (2) individualism (IDV), corresponding to the extent to which a society is integrated into groups, (3) masculinity (MAS), corresponding to a distribution of roles between men and women, (4) uncertainty avoidance (UAI), corresponding to a society's tolerance of ambiguity or unexpected and unknown events, and (5) long-term orientation (LTO), corresponding to the extent to which a society is focused on the future. An additional dimension was later added: (6) indulgence (IND), as the extent of freedom in fulfilling human desires restrained by social norms (Hofstede et al. 2005).

While these cultural dimensions can be used to explain behaviors in society, online privacy studies have mostly focused on three dimensions: PDI, IDV, and UAI (Milberg et al. 2000; Shin et al. 2007; Jiang and Ji 2009). Societies with low PDI have fewer privacy concerns and are more at ease with disclosing information owing to beliefs of equality (Jiang and Ji 2009). Further, highly individualistic societies are more likely to disclose for the expected personal benefits of their behaviors, disregarding the impacts on or consequences for other members of society (Krasnova et al. 2010; 2013). Also, societies with high UAI have a risk-averse attitude (Hofstede 2001); thus, they have higher risk perceptions concerning information disclosure (Krasnova et al. 2013). Concerning masculinity, Milberg et al. (2000) argued that societies with high MAS indices are more concerned about the consequences of information disclosure. This can be explained by their competitiveness and by others' misuses of the disclosed information (Krasnova et al. 2010). Also, Acquisti (2004) showed that societies with low LTO have preferences for immediate benefits, which affects their disclosure behaviors.

Research Approach

In this study, we explore users' attitudes and motivations behind location- information disclosure for user populations with different cultural and institutional environment backgrounds along our conceptual model. We provide insights through comparing users' perception for the suggested constructs. Empirical testing of the model lies beyond this paper's scope (cf. Naous et al. 2019).

To collect data, we did a survey with users from two countries: the U.S. and Germany, two countries with different cultural and institutional backgrounds (Table 1). Based on Hofstede's cultural dimensions, the U.S and Germany have two distinct cultures characterized by low PDI scores (Germany 35, U.S. 40) and high MAS scores (Germany 66, U.S. 62). Although both had high IDV scores, the U.S. (91) had a more individualistic culture than Germany (67). Concerning UAI, Germany (65) is thought to have a more risk-averse culture than the U.S. (46). Concerning LTO, Germany (83) followed a pragmatic approach for future planning, while the U.S. (26) had a focus on immediate gratification. This is also reflected in the IND dimension, where the U.S. (68) had a higher score than Germany (40). While the U.S. mainly relies on industry self-regulation, as part of the EU, Germany applies the GDPR in all organizations (in its territory and abroad) that treat German citizens' data.

For both countries, we hired participants via Qualtrics online panels that provide access to nationally representative samples around the world, with an audience mix to help find the right insights (qualtrics.com). We did a survey with 1,050 participants with an equal U.S./Germany split and compensated the respondents with the average rate for a 10-minute survey suggested by Qualtrics team to obtain quality responses ($4 per respondent for the U.S. sample and €4 for the German one). To ensure experience with LBSs, the participants were screened and selected based on several criteria such as their smartphone usage patterns (only smartphone users with experience of social networking websites were recruited) and reliance on LBSs (reflected by the number of LBS used). Further, to get adequate variances in the model variables, we selected participants based on their LBS application usage diversity. This can lead to risk-benefit evaluations based on different services and can potentially reduce any inherent biases.

Table 1. Cultural and Institutional Differences between Germany and the U.S.

		Germany	**U.S.**
Cultural environment	Power Distance Index (PDI)	low	low
	Individualism (IND)	high	high
	Masculanity (MAS)	high	high
	Uncertainty Avoidance (UAI)	high	low
	Long-term Orientation (LTO)	high	low
	Indulgence (IND)	low	high
Institutional environment	Privacy regulations applying to location information	GDPR - mobility traces qualify as personal data	none, mainly industry self-regulation

The survey contained questions on users' backgrounds, experience with LBS, and previous privacy experience. We then reflectively measured the constructs along a seven-point Likert scale (between 1 = *strongly disagree* and 7 = *strongly agree*) for all the items. To operationalize the constructs, we relied on

pre-tested and valid scales from prior research. Perceived personal and extrinsic privacy risks, perceived benefits of contextualization, and trust in government regulations constructs were based on items from Xu et al. (2009). For perceived privacy control and other trust items, we used items from Krasnova et al.'s (2010) study on social networks. We developed new scales for the remaining constructs and performed a pre-test survey with 18 LBS users to test the new items' content validity. All the items resulted in satisfactory inter-item correlations and were used in the study. For the data analysis in the next section, we ran t-tests to study the mean differences between the two samples. Significant differences (*) between the two samples are registered for results with p-values ≤ 0.05.

Results

Samples from the U.S. and Germany

We obtained equal samples (525 respondents each from the U.S. and Germany). There was an approximately equal gender split. The participants were mainly young: 41.82% (U.S.) and 49.33% (Germany) were under 35. For both samples, more than 40% of the respondents had three or more LBSs installed on their smartphones, and more than 60% had a minimal understanding of the privacy implications and the potential misuses of users' digital information. The two samples had similar percentages for the LBS types used, including navigation and social networking, with a notable difference for ridesharing applications (U.S. 38.48%, Germany 17.33%). This can be mainly explained by the different implementations and usages of the public transportation systems in the two countries. Detailed statistics on the samples appear in Table 2.

Table 2. Sample Background

Variable	Level	US (in %)	Germany (in %)
Gender	Male	49.81	50.10
	Female	50.19	49.90
Age	18-24	13.75	19.43
	25-34	28.07	29.90
	35-44	30.48	19.43
	45-54	14.13	16.19
	55-64	10.04	11.24
	65 or above	3.53	3.81
Number of LBS	1-3	53.33	52.00
	4-7	29.71	30.29
	8-10	7.24	7.43
	>10	6.10	6.48
	Don't know	3.62	3.81
Type of LBS	Navigation	80.00	84.00
	Ride-sharing	38.48	17.33
	Point of interest	25.14	30.48
	Social networking	84.19	84.95
	Other (e.g., weather, dating, etc.)	20.76	21.33
Privacy Consciousness	Not informed	29.71	32.19
	Moderately informed	44.57	42.67
	Well informed	25.71	25.14

Location-information Disclosure

Both populations generally reported fairly similar attitudes, with means between 3.4 and 4.6 for the different dimensions of location-information disclosure and only a few significant differences (Table 3). The general attitude toward location-information sharing is slightly positive, but the highest percentage of respondents (around 25%) is neutral toward sharing. However, the sharing behaviors vary with respect to the different disclosure dimensions. For sharing extent, both samples are more likely to sporadically share

their locations (i.e., only when needed), with means of 4.71 for Germany and 4.90 for the U.S., and they are less likely to share continuously with GPS functionalities *always-on* in their mobile phones. However, the U.S. show a higher acceptance of such practice (43.87% agreed on different levels: slightly agree, agree, and strongly agree, compared to 37.90% for Germany). Although a high UAI implies avoidance of risky situations, the advantage of real-time updates in case of continuous disclosure is a main reason for this attitude. Further, the adoption of navigation and tracking services worldwide contributes to these results. Concerning the shared location-information type, both samples are unlikely to share what they consider sensitive location-information and are neutral to sharing public locations (mean: Germany 4.16, U.S. 4.18). By *sensitive location-information*, we refer to locations that can reveal sensitive demographic information, such as religious, political, and sexual orientations. Both countries have high MAS and IDV scores, which indicate competitive populations who are concerned about their self-image and about the misuse of such information. Revealing sensitive information can affect their social positions in some situations.

Table 3. Location-Information Disclosure

Items	**Germany**	**US**
	Mean	Mean
General		
I am likely to share my location on LBS.	4.19	4.26
Extent		
Continuous sharing: I am likely to keep my GPS switched on at all times to provide my real-time location to LBS.*	3.88	4.08
Sporadic sharing: I am likely to switch on my GPS only when I need to use LBS.	4.71	4.90
Sensitivity		
Sensitive information sharing: I am likely to share my private/sensitive locations on LBS.	3.88	3.71
Non-sensitive information sharing: I am likely to check-in at public places on LBS.	4.16	4.18
Sharing Parties		
Service provider only: I am likely to share my location-information on LBS given that my data is not shared with any other entity.*	4.34	4.6
Service members: I am likely to share my location-information on LBS given that the service members can view it.	3.98	4.13
3rd Parties: I am likely to share my location-information with LBS even if they sell my data to third-party providers such as data brokers or advertisers.	3.61	3.42
Government: I am likely to share my location-information on LBS knowing that government organizations can access it.	3.89	3.92

Concerning sharing parties, our results show that U.S. users are much more likely to share with service providers only if the latter do not share the information with any other entity. Both Germans and Americans disagree or are neutral toward sharing location-information with other sharing parties, including third-party companies that use location data for commercial purposes, service members, and the government. This can be explained by both countries' high UAI and IDV scores, since they are normally characterized as concerned with privacy and would not want their data to be used without their approval. Further, recent privacy breaches (especially in the U.S.) have contributed to this attitude, with users becoming aware of the lack of privacy-protecting regulations concerning the use of their data by third parties or access by government. This situation may be different in Germany, given the implementation of the GDPR, which can influence disclosure behaviors if properly followed by LBS providers worldwide. Notably, individuals in both countries are reluctant to share with the government, despite the high LTO score for Germany. In fact, cultures with high LTO may see disclosure and use of their data for governmental/country initiatives as a step forward toward better future planning in transportation, communications, or urban planning. This was not the case in our sample, which may be further explained by benefit and risk perceptions, which we will now discuss.

Perceived Benefits

Concerning benefits, location-information disclosure may lead to hedonic benefits (i.e., contextualization and social status) as well as utilitarian benefits (i.e., monetization). Both populations clearly value the benefit of contextualization in terms of locatability and personalization provided by LBSs and agree that sharing their location allows them to have relevant and timely information as well as personalized context. While individualistic cultures generally value immediate benefits, the significant differences between the two samples can be further explained by the high IDN and low LTO scores for the U.S., which drove their attitude toward immediate gain. Compared to contextualization, both populations are more neutral regarding the social status benefit, which can be explained by the low PDI scores in both cultures. A low PDI score indicates that individuals in a community believe in equal power distribution among societal levels, which rejects the assumption that presence in certain locations can boost social image in this cultural setting.

Concerning incentives (as utilitarian benefit), the most respondents from both samples are neutral in their perceptions with means close to 4, except for the second item (Table 4). This may be influenced by current practices. In fact, 59% of Germans and 64% of Americans agreed (on different levels) on the benefit of discounts or deals as a representation of incentives rather than on monetary gains, which they are not currently aware of. Even with the emergence of crypto-currencies and the monetization of personal data, users still do not foresee this opportunity for monetary gain when sharing their location-information.

Table 4. Perceived Benefits

Items	**Germany**	**US**
	Mean	Mean
Contextualization		
1. With LBS I am able to get up to date information/services whenever I need to (e.g. regular updates with latest events, new restaurants).*	4.59	4.82
2. I am able to access the relevant information/services wherever I want to with LBS.*	4.47	4.72
3. With LBS, I am able to access the relevant information/services at the right place.*	4.56	4.83
4. LBS provide me with personalized services tailored to my activity context.*	4.38	4.64
5. LBS provide me with more relevant information tailored to my preferences or personal interests.*	4.42	4.65
6. LBS provide me with the kind of information or service that I might like.*	4.44	4.65
Social Status		
1. I am likely to share my location along with certain other people on LBS (e.g., via check-ins or posting photographs on Facebook or Instagram) to boost my social image.	3.96	3.82
2. I am likely to post a picture at a social event along with certain people to improve my social image on platforms such as Facebook or Instagram.	3.96	3.92
3. I am likely to share my location or post pictures at certain locations to boost my social image on various LBS (e.g., Facebook, Instagram).	3.9	3.81
Incentives		
1. Sharing my location-information will result in monetary gains (e.g., reduction in my car insurance premiums).	3.91	3.89
2. LBS can help me to discover discounts or deals at shops, restaurants or bars.	4.68	4.82
3. LBS associated with data brokers can provide me with monetary benefits.	4.05	3.99

Perceived Privacy Risks

Regarding privacy risks, both populations agree on the privacy risks associated with location-information disclosure, on the personal level and the interdependent level (means: Germany 4.22 to 4.43, U.S. 4.32 to 4.69). However, the Americans seem more risk-averse (although the Germans have a higher UAI), which is mainly significant in the personal privacy risk items (Table 5). Americans (12% to 14%) agree to strongly

agree that sharing location-information may cause potential losses and is risky, compared to 5% of the Germans. Overall, around 42% of the Germans generally agree, while approximately 55% of the Americans agree, on the privacy risks. However, these rates are lower for extrinsic privacy rates, as almost 30% of respondents from both countries are neutral toward the risks to others when they share interdependent location-information, for instance via Facebook posts of photos or location tags with friends. Given that both cultures are considered individualistic, the extrinsic privacy risk may not be seen as critical to individuals who are not concerned with group or community relationships. However, the social nature of LBSs similar to Facebook and Instagram pose questions on the effects of individualism and collectivism on sharing behaviors, since these require sharing in a community of users. Thus, we believe that the perceptions of privacy are somehow uniform between the two cultures and that community is a key factor in sharing.

Table 5. Perceived Risks

Items	Germany	US
	Mean	Mean
Personal Privacy Risk		
1. Disclosing my location to location-based service providers (e.g., Uber or Facebook) could involve many unexpected problems.*	4.39	4.65
2. Disclosing my location-information to the service provider will bring potential losses (e.g., data breaches, information leakages).*	4.22	4.59
3. Disclosing my location-information to the service provider is risky.*	4.43	4.89
Extrinsic Privacy Risks		
1. Tagging my friends on LBS platforms will bring unpredictable problems to them.	4.26	4.32
2. Checking-in with my friends on LBS could be risky to them.	4.39	4.48
3. Tagging my friends on LBS may bring potential losses to them (e.g. data breaches, information leakage).	4.29	4.42

Privacy-Control Settings and Trust

Users generally agree that privacy settings in LBSs allow them to control the shared location-information. This may be the result of advances in privacy-preserving technologies that allow users to specify what information they would like to publicly share, or the granularity of the location-information stored on LBSs. Although they agree that privacy settings can be effective, they do not feel sufficiently in control of who can view their information on LBSs (lower means for item 3 in Table 6). This is also confirmed by the neutral attitude toward all the trust items.

Table 6. Risk Antecedents

Items	Germany	US
	Mean	Mean
Perceived Control		
1. I feel in control over the location-information I provide to LBS (e.g., location granularity on Google maps).	4.26	4.18
2. Privacy settings present in LBS (e.g., Tinder or Facebook) allow me to have control over the location information I provide.*	4.3	4.58
3. I feel in control of who can view my location-information provided on LBS.	4.1	4.09
Trust in government regulations		
1. Government regulations protect my location-information provided to LBS.	4.02	3.83
2. Government regulations protect me from any misuse of my location-information by LBS providers.	3.94	3.82
3. Government regulations protect me from unauthorized use of my personal-location data disclosed on LBS.	4.1	4.09

Trust in service providers		
1. LBS providers are trustworthy and will not misuse any of my location information.	3.92	3.81
2. LBS providers are honest in their dealings with me.	3.98	4.02
3. LBS providers are interested in the well being of their members.	4.1	4
Trust in service members		
1. Users of LBS I use are trustworthy and would not attempt to harm me.	4.12	3.99
2. Users of LBS I use are helpful and receptive to the needs of other users.	4.37	4.45
3. Users of LBS I use are honest in dealing with each other.	4.09	4.04

Although Germany has a more risk-averse culture, we observe similarities between the two countries regarding trust as risk antecedent. The history of privacy leaks as well as the current practice by LBS providers of selling user data to third parties for commercial purposes have shaped this user perception. The effective implementation of privacy protecting regulations (e.g., GDPR in the EU) and the application of privacy as a design principle by LBS providers for the transparent treatment of location data can help to change this perception in the future. Notably, both samples agree that LBS members are helpful and receptive to the needs of others. We believe that this is a trait specific to LBSs in the category of sharing economy such as ridesharing (e.g. Uber) and lodging (e.g. Airbnb). These service types require a community of users who provide services in specific locations, and the members' aforementioned characteristics are necessary in this context. Although both cultures are individualistic and are not concerned with community goals and relationships, our results mostly suggest that LBS users share a collectivist approach to their uses of similar LBS types.

Conclusions

Our study provide insights into users' attitudes toward location-information disclosure for two populations with different cultural backgrounds and institutional environments. Interestingly, we observe more commonalities than differences between them. However, we also observe that the sharing behavior depends on the sharing context. Most importantly, the amount of location-information shared and who has access to it are concerns for users. Users are more likely to share sporadically and would prefer that their location traces not be continuously tracked. Further, they are willing to disclose their location-information on LBSs if this is not shared with any other entity. They are less likely to share sensitive location-information, given the privacy consequences this may have on their lives.

Concerning the rationales behind location-information disclosure, our results reveal a high perceived importance of the contextualization benefit of LBS – users mostly appreciate locatability and personalization over other benefits. This explains the widespread worldwide use of navigation services, such as Google Maps or Waze. The results also show that monetary rewards are not properly seen as a potential benefit for location-information disclosure. Despite the emerging data economy, users seem unwilling to trade their privacy for monetary benefits.

In line with previous studies, we observe that privacy risks are highly relevant to LBS users, but more on the personal level than regarding extrinsic privacy. Users should know that their disclosure of interdependent location-information without their consent could have consequences on others' privacy, since LBS providers or third parties can access this information and can use it for commercial purposes. Both populations value privacy-preserving mechanisms and privacy settings on LBSs so as to maintain control of their information. However, users lack trust in LBS providers and service members experience a lack of control of their information. In fact, current practices of LBS providers as well as privacy awareness play key roles in shaping users' perceptions of control. Further, users believe that government regulations should be more strict, and that they should enact laws that protect user data from risk-associated behaviors, especially concerning access to and treatment of users' information.

References

Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the 5th ACM Conference on Electronic Commerce*, ACM, pp. 21–29.

Anuket, B. 2003. "User Controlled Privacy Protection in Location-Based Services," *Unpublished Master's Thesis, University of Maine, Orono, ME*.

Betzing, J. H., Tietz, M., vom Brocke, J., and Becker, J. 2019. "The Impact of Transparency on Mobile Privacy Decision Making," *Electronic Markets*.

Cheng, R., Zhang, Y., Bertino, E., and Prabhakar, S. 2006. "Preserving User Location Privacy in Mobile Data Management Infrastructures," in *International Workshop on Privacy Enhancing Technologies*, Springer, pp. 393–412.

Farkas, D., Hilton, B., Pick, J., Ramakrishna, H., Sarkar, A., and Shin, N. 2016. "A Tutorial on Geographic Information Systems: A Ten-Year Update," *Communications of the Association for Information Systems* (38:1), p. 9.

Gambs, S., Heen, O., and Potin, C. 2011. "A Comparative Privacy Analysis of Geosocial Networks," in *4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, ACM, pp. 33–40.

Hofstede, G. 2001. *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*, Sage publications.

Hofstede, G., Hofstede, G. J., and Minkov, M. 2005. *Cultures and Organizations: Software of the Mind*, (Vol. 2), Citeseer.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior," *International Journal of Human-Computer Studies* (71:12), pp. 1163–1173.

Krasnova, H., and Veltri, N. F. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA," in *43rd Hawaii International Conference on System Sciences*, IEEE, pp. 1–10.

Krasnova, H., Veltri, N. F., and Günther, O. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering* (4:3), pp. 127–135.

Krumm, J. 2007. "Inference Attacks on Location Tracks," in *International Conference on Pervasive Computing*, Springer, pp. 127–143.

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

Miah, S. J., Vu, H., and Gammack, J. 2019. "A Big-Data Analytics Method for Capturing Visitor Activities and Flows: The Case of an Island Country," *Information Technology and Management*, pp. 1–19.

Milberg, S. J., Smith, H. J., and Burke, S. J. 2000. "Information Privacy: Corporate Management and National Regulation," *Organization Science* (11:1), pp. 35–57.

Morlok, T. 2016. "Sharing Is (Not) Caring-the Role of External Privacy in Users' Information Disclosure Behaviors on Social Network Sites.," in *PACIS*, p. 75.

Naous, D., Kulkarni, V., Legner, C., and Garbinato, B. 2019. "Information Disclosure in Location-based Services: An Extended Privacy Calculus Model," in *ICIS*.

Olteanu, A.-M., Huguenin, K., Shokri, R., Humbert, M., and Hubaux, J.-P. 2017. "Quantifying Interdependent Privacy Risks with Location Data," *IEEE Transactions on Mobile Computing* (16:3), pp. 829–842.

Pankowska, M. 2018. *Privacy Awareness in the GDPR Implementation Circumstances*.

Pick, J. B., Turetken, O., Deokar, A., and Sarkar, A. 2017. "Location Analytics and Decision Support: Reflections on Recent Avancementa, a Research Framework and the Path Ahead," *Decision Support Systems* (99).

Rudgard, O. 2018. "Drivers' Mobile Phone Data to Help Beat Traffic Jams," *The Telegraph*. (https://www.telegraph.co.uk/news/2018/04/18/york-track-mobile-phone-data-traffic-pilot/, accessed September 6, 2019).

Shin, S. K., Ishman, M., and Sanders, G. L. 2007. "An Empirical Investigation of Socio-Cultural Factors of Information Sharing in China," *Information & Management* (44:2), pp. 165–174.

Sun, Y., Wang, N., and Shen, X.-L. 2014. "Perceived Benefits, Privacy Risks, and Perceived Justice in Location Information Disclosure: A Moderated Mediation Analysis.," in *PACIS*, p. 135.

Sun, Y., Wang, N., Shen, X.-L., and Zhang, J. X. 2015. "Location Information Disclosure in Location-Based Social Network Services: Privacy Calculus, Benefit Structure, and Gender Differences," *Computers in Human Behavior* (52), pp. 278–292.

Wheeless, L. R., and Grotz, J. 1976. "Conceptualization and Measurement of Reported Self-Disclosure," *Human Communication Research* (2:4), pp. 338–346.

Xu, H., Teo, H.-H., Tan, B. C., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135–174.

Zhou, T. 2011. "The impact of privacy concern on user adoption of location-based services," I*ndustrial Management & Data Systems* (111:2), pp. 212-226.

Zhu, Z., and Cao, G. 2011. "Applaus: A Privacy-Preserving Location Proof Updating System for Location-Based Services," in *IEEE INFOCOM*, IEEE, pp. 1889–1897.