Yang Lu
University of Kent

Athina Ioannou
University of Surrey

Iis Tussyadiah
University of Surrey

Shujun Li
University of Kent

Segmenting Travelers Based on Responses to Nudging for Information Disclosure

Digital technologies shape travel environments. Noticing online privacy issues, consumers can hold distinct attitudes towards disclosing personal information to service providers. We conducted a panel survey to gauge travelers' willingness to share personal information with service providers, provided with different types of nudges. Based on the results of clustering analysis, two segments were identified: travelers who are reasonably willing to share (*Privacy Rationalists*) and those who are reluctant to share (*Privacy Pessimists*). This study provides empirical evidence of privacy segmentations in the travel context, which has not been reported before and thus deserves more attention from both researchers and practitioners.

Key words: travel, privacy, information disclosure, incentive, nudge, segmentation, profiling

Yang Lu
School of Computing
University of Kent
Canterbury CT2 7NZ
UK
Email: y.lu@kent.ac.uk

Athina Ioannou
School of Hospitality and Tourism Management
University of Surrey
Guildford GU2 7XH
UK
Email: a.ioannou@surrey.ac.uk

Iis Tussyadiah
School of Hospitality and Tourism Management
University of Surrey
Guildford GU2 7XH
UK
Email: i.tussyadiah@surrey.ac.uk

Shujun Li
School of Computing

University of Kent
Canterbury CT2 7NF
UK
Email: s.j.li@kent.ac.uk

Yang Lu is a Postdoctoral Research Associate at University of Kent. Working in the EPSRC funded project "PriVELT" (PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers), her research is mainly about privacy assessment frameworks, privacy-enhancing solutions with technologies of privacy computing, semantic web and artificial intelligence.

Athina Ioannou is a Research Fellow at University of Surrey. She is working in the EPSRC funded project "PriVELT" (PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers). Her research is primarily around privacy and data management as well as in technology adoption and diffusion focusing on the implications of technology use in individual, organizational and social contexts.

Iis Tussyadiah is Professor of Intelligent Systems in Service and Head of Department of Hospitality in School of Hospitality and Tourism Management at University of Surrey. Her research interests lie in the intersection of information systems and consumer behavior.

Shujun Li is Professor of Cyber Security at School of Computing, University of Kent. He is directing Kent Interdisciplinary Research Centre in Cyber Security (KirCCS), an UK government recognized Academic Centre of Excellence in Cyber Security Research (ACE-CSR). His research interests are mostly around interdisciplinary topics covering cyber security and privacy, digital forensics and cybercrime, human factors, and multimedia computing.

Introduction

The emergence of new digital technologies has brought considerable benefits into our everyday lives. However, the incurred data disclosures have raised consumers' concerns over their privacy. While using various digital services and products, consumers are requested to make privacy decisions, such as configuring settings to allow/disallow data access by mobile apps and sharing certain personal information in exchange for services or benefits (e.g., cash returns, discounts, and coupons). According to Acquisti et al. (2017), various human factors (e.g., heuristics, mental shortcuts, feelings and emotions, cognitive or behavioral biases) can affect individuals' privacy decision making processes and behaviors, which can result in less efficient or even regrettable choices. Therefore, there is an emergent need to focus on interventions to assist consumers in making privacy decisions.

Many studies on human behavior in different disciplines, including behavioral economics and computer science, have suggested using soft paternalistic interventions (i.e., nudges) to guide people into making their decisions. As defined in (Thaler & Sunstein 2003; Thaler & Sunstein 2009), a nudge is "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives". Nudging can affect individuals' decision-making processes without forcing them to take a particular course of action, thus safeguarding their freedom of choice and improving their well-being. There has been a growing body of research investigating the use of digital nudging in the context of individual privacy-related behavior and decisions. Digital nudging refers to the use of computer user interface elements in digital choice environments, aiming to guide users as they are required to make judgements and decisions (Ridley-Siegert, 2015). Researchers have studied a wide range of digital nudging strategies to affect information disclosure, including nudging with presentation and design concepts such as privacy notices and warnings, nudging with information by providing education and

feedback to users such as notifications and privacy notices, nudging with the provision of incentives, and nudging with default options such as opt-in and opt-out options (Acquisti et al., 2017). Although a growing number of empirical studies has focused on the effects of nudging on privacy decisions (Junger, Montoya & Overink, 2017; Lu, Ou & Angelopoulos, 2018), it is largely unknown how nudging types affect travelers' information disclosures. Therefore, further research is essential to gain a better understanding into the potential effectiveness of the different nudging strategies and how they can be used in various contexts in order to achieve optimum results for users.

Privacy means differently to different people. Westin, Louis & Associates (1991) suggested grouping people into *Fundamentalists*, *Unconcerned* and *Pragmatists*, based on their privacy concerns, attitudes, and trust in existing laws and organizations using their personal data. Based on Westin's Index and its applications, researchers have developed privacy metrics for different purposes (Kumaraguru & Cranor, 2005). By examining users' privacy concerns in 15 different situations, the group *pragmatists* were further divided into sub-groups based on their concerns on identifiable information collection and usage (Sheehan, 2002). Besides, segmenting people's privacy behaviors can help system developers to better understand online users and provide privacy protection accordingly (Woodruff et al., 2014). For instance, Poikela et al. (2014) proposed to segment users based on the frequency and the level of accuracy of sharing real-time locations with location-based apps. Through inviting participants to rank privacy behaviors while using a technology service, a five-group segmentation was proposed to identify users' information-seeking preferences and inform the construction of default privacy personas (Morton & Sasse, 2014). Based on the self-reported privacy behaviors on Facebook, Wisniewski, Knijnenburg & Lipford (2017) identified six privacy management strategies to personalize social network service (SNS) privacy and optimize the privacy features.

To deliver effective privacy-enhancing strategies and to reduce the chance of privacy breaches occurring in online environments (Tussyadiah, Li & Miller, 2019), it is essential to understand travelers' privacy profiles and potential influences of other attributes. To the best of our knowledge, this has not been studied before in the context of online travel environments. To fill this gap, our study examines how different information sharing incentives (as nudging strategies) from service providers impact travelers' privacy decisions, especially their willingness to disclose personal information online.

Methodology

To capture a set of individual factors related to privacy as well as travelers' willingness towards information disclosure, an online questionnaire was distributed to a panel of UK residents by a professional survey company in May 2019, as a part of PriVELT[1], an interdisciplinary research project investigating online privacy solutions for travelers. The survey included a set of screening questions in order ensure that participants were travelers who have used travel websites in the last six months. All items were presented with a 5-point Likert scale: 1 = 'strongly disagree', 2 = 'disagree', 3 = 'neither disagree or agree', 4 = 'agree', and 5 = 'strongly agree'. Measurement items for the construct of privacy knowledge was adapted to the research context based on the measurement scale from (Youn, 2009). Items relating to privacy awareness and experience were adopted from (Xu et al., 2011) and (Li, 2014), respectively. Participants were requested to state the sensitivity and degrees of willingness to share different types of personal information. Meanwhile, three nudging strategies were tested: (1) monetary incentives (e.g., cash), (2) non-monetary incentives (e.g., discounts), and (3) privacy assurances (e.g., privacy policies provided by organizations). Example questions are shown in Table 1.

Table 1. Items capturing willingness to disclose personal information

---

[1] PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers PriVELT. https://www.privelt.ac.uk/

Variable	Item
No Nudge (Control)	'How willing are you to share personal information with online travel providers?'
Monetary Incentives	'Should you receive monetary incentives (i.e. cash), how willing are you to share personal information with online travel providers?'
Non-Monetary Incentives	'Should you receive non-cash incentives (i.e. discounts), how willing are you to share personal information with online travel providers?'
Privacy Assurances	'If the online company is providing privacy assurances (such as an easy to read privacy policy) about the protection of your personal data, how willing are you to share personal information with online travel companies?'

Results and Discussion

A total of 836 responses were collected from the panel. After excluding unqualified responses, the usable sample size was 685. There was a relatively balanced distribution in gender with 47.2% being male, while the majority were young travelers, being in the age range of 26 to 45 years old (45%), and having finished high school (38.8%). Aiming to learn the privacy profiles of travelers, a clustering analysis, one-way analysis of variance (ANOVA), and Pearson χ^2 tests were conducted.

Segmenting Travelers based on Willingness towards Information Disclosure

Aiming to understand whether travelers can be grouped into meaningful segments, we conducted the TwoStep cluster analysis (Şchiopu, 2010) by using IBM SPSS version 25 to classify our samples and to identify the optimal number of clusters. Specifically, the TwoStep cluster analysis starts by constructing a modified cluster feature (CF) tree in the pre-clustering step (Zhang, Ramakrishnan & Livny, 1996). In the clustering stage, all the sub-clusters resulting from the pre-clustering step are recursively merged following an agglomerative hierarchical clustering process. In this study, traveler segments were determined based on self-reported levels of willingness to share personal data with the three binary (with and without) nudging variables: monetary incentives, non-monetary incentives, and privacy assurances. In addition, online privacy concerns, willingness to share data when

no incentives were provided, and privacy awareness were used as evaluation variables for the resulting clusters.
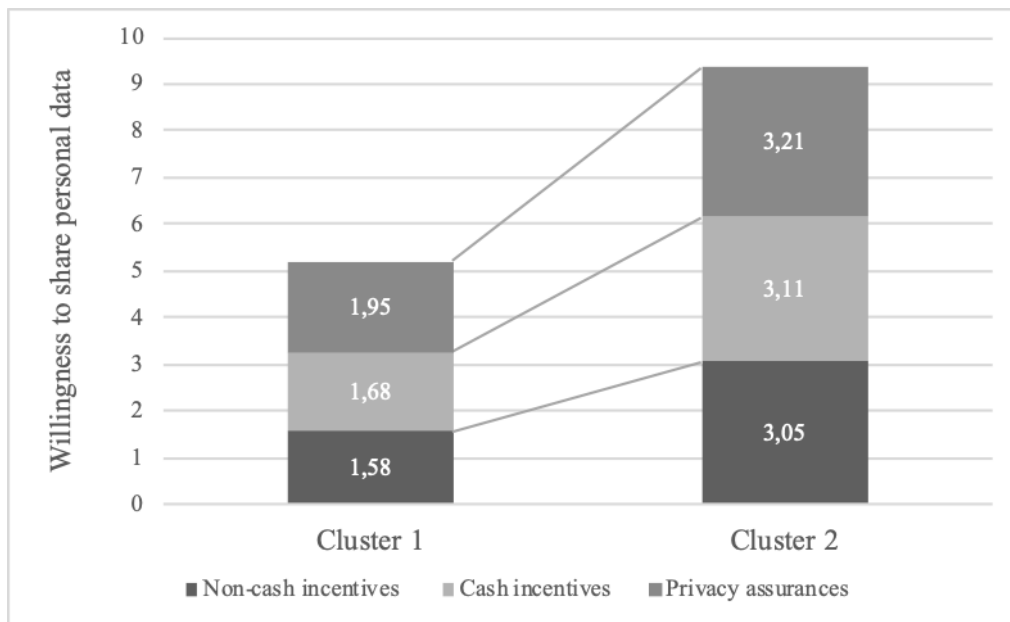

Figure 1 Average willingness to share information with nudging provided

Table 2. Segment Characteristics

	Cluster 1	Cluster 2
No Nudge	2.13	3.04
Privacy Concerns	3.85	3.53
Privacy Awareness	3.81	3.70

According to the model summary statistics in the SPSS viewer, the two-cluster solution was deemed as "good" (average Silhouette Index = 0.6) and selected to represent traveler segments. As shown in Figure 1 and Table 2, Cluster 1 is characterized by individuals who are less willing to share their personal information regardless of the provision of any types of incentives. What is more surprising, they became even less willing to share their personal data when any types of incentives were provided (Average levels were 1.58, 1.68, and 1.95, respectively, reduced from 2.13 when no incentive was provided). By contrast, Cluster 2 is characterized by individuals who are more likely to share their personal information` for certain benefits. As they reacted positively to incentives and monetization of

their personal data, it can be suggested that they are open to share or 'sell' their personal data to receive certain benefits in return. Compared to Cluster 1, this group showed a (slightly) lower level of privacy concerns and awareness on privacy-related issues (see Table 2).

Overall, the cluster analysis revealed that the provision of incentives can impact travelers' willingness to share personal information. Participants who are highly aware of (concerned about) privacy issues tend to be more reluctant to share personal information, and providing incentives may discourage them more from sharing personal information with online travel service providers. Indeed, as reported in the literature, a higher level of privacy awareness can increase concerns over privacy (Benamati, Ozdemir & Smith, 2017). Individuals with a higher level of privacy concerns tend to protect their personal information and engage in similar behaviors, thus being less willing to disclosure any personal information (Wozniak et al., 2018). Therefore, one possible reason to explain the behavior of travelers in Cluster 1 is that the received incentives triggered privacy awareness, which then lowered the willingness to sharing personal information with online travel service providers.

Travelers in Cluster 2 are more likely to share data when incentives were provided. Regarding the effects of nudging strategies, the results demonstrate that nudging with privacy assurances was most effective in motivating Cluster 2 travelers to disclose personal information (3.21), while monetary (3.11) and non-monetary (3.05) incentives were less influential. In the same vein, when non-monetary incentives were offered, Cluster 1 travelers became reluctant to share personal data (1.58), but relatively less so when privacy assurances were provided (1.95). Our findings are in agreement with previous studies suggesting that the provision of privacy assurances in websites could motivate users to provide more personal information and that privacy assurances are more effective than monetary rewards (Gabisch & Milne, 2013; Hui & Lee, 2017).

A one-way analysis of variance test (ANOVA) was performed in order to detect significant differences between the clusters regarding the three nudging strategies. Results showed significant differences among the clusters in terms of nudging preferences of the cluster members: non-monetary [$F(1, 683) = 1143.9$, $p < 0.001$], monetary [$F(1, 683) = 927.6$, $p < 0.001$], and privacy assurances [$F(1, 683) = 774.4$, $p < 0.001$]. Moreover, further ANOVA analysis was conducted in order to identify significant differences in terms of individual factors of the cluster members, revealing significant differences between both clusters in terms of privacy concerns [$F(1,683) = 48.673$, $p < 0.001$], willingness to share information without nudging [$F(1,683) = 279.43$, $p < 0.001$], and privacy awareness [$F(1,683) = 4.048$, $p = 0.045$].

Traveler profiling

To further uncover group profiles, Pearson χ^2 tests were conducted to evaluate whether demographic differences exist among cluster members. As shown in Table 3, two groups are significantly different across age and online shopping experience, while almost no difference was found across gender ($\chi^2 = 4.788$, $p = 0.091$), education ($\chi^2 = 1.272$, $p = 0.938$), travel frequency ($\chi^2 = 1.915$, $p = 0.384$), internet experience ($\chi^2 = 3.755$, $p = 0.289$) or employment status ($\chi^2 = 7.564$, $p = 0.182$). As shown in Table 3, Cluster 1 is characterized by mostly older travelers (63% are 46 or older) with moderate online shopping experiences (76% several times a month or less), while Cluster 2 includes more travelers in younger age groups (45.4% in 18-46 range) who usually shop online more often (78% several times a month and more often).

Based on the cluster size and demographic characteristics, it can be inferred that Cluster 2 travelers are aware of privacy related matters through the media or by previous experiences and thus are more open to the idea of sharing personal information in exchange for incentives. However, Cluster 1 likely represents a customer group that are older

individuals, with less online shopping experience, thus more likely prefer making purchases physically rather than online. This consumer group is less willing to accept incentives in exchange for sharing personal information with online travel service providers.

Table 3. Demographic Profiles

Characteristics	Cluster 1	Cluster 2	χ^2	p
Age			18.89	0.002
<25	2.5%	7.3%		
26-35	21.3%	26.8%		
36-45	13.2%	11.3%		
46-55	16.5%	18%		
56-65	22.4%	22%		
over 65	24.1%	14.6%		
Online shopping experience			18.808	0.001
Daily	8.1%	11.6%		
Several times a week	16.5%	26%		
Several times a month	42%	41%		
Roughly once a month	28%	19%		
Almost Never	6%	3%		

Conclusions and Future Work

This research contributes both to the privacy and tourism literatures by offering a more nuanced understanding of travelers' responses to a number of nudging strategies which are reflected in their willingness to disclose personal information when in online environments. Aiming to uncover the different privacy profiles of travelers, two segments were identified through a clustering analysis*: similar to the Fundamentalists, travelers in Cluster 1 (Privacy Pessimists*) consider themselves very private and resist to share personal information regardless of the benefits they may receive in return; Cluster 2 (*Privacy Rationalists*) shares the characteristics of the *Pragmatists,* who are confident to share personal information and willing to exchange it for benefits. Interestingly, we found that *Privacy Pessimists* are even less willing to share personal data when they are offered any type of incentives (nudges).

Since the majority of studies have been implemented in general consumption contexts, the current study adds value to the extant research and practice by focusing on nudging strategies that can be used by service providers in the travel and tourism industry to assist consumers in making better and more informed decisions when sharing personal information online. By revealing the privacy profiles of today's travelers, online travel agencies can better understand their customer base in terms of privacy concerns, responses to nudging, and intention to disclose personal information. Online travel service providers will be able to offer better, more tailored solutions to customers in order to enhance customer experience, increase revenues, and thus overall success. Moreover, our results offer a better understanding of user privacy profiles so that practitioners can develop better privacy protection tools for consumers.

Our findings come with limitations. First, the study was conducted in a single point in time as a cross sectional study in a specific country (UK) thus causal inferences should be made with caution. Longitudinal studies should be designed to assess perceptions to various nudging strategies and privacy concerns over a period of time. Also, binary measures (present or absent) are used to capture travelers' responses to nudging. Future experiments should measure responses to incentives in real consumption settings to make more rigorous causal inferences. Moreover, the present study examined the impacts of nudging strategies on the willingness to share information. Future experiments should be designed to monitor and analyze travelers' actual behaviors to test the effectiveness of various nudging strategies. According to previous studies on privacy segmentation in general contexts, the majority of consumers are *Pragmatists,* while a smaller percentage of people are *Fundamentalists* and *Unconcerned* (Harris Interactive, 2003; Ridley-Siegert, 2015). However, our results showed the *Pessimists* and *Rationalists* are similar in size. This may be explained by the different focus on travelers and the online environments. To further validate and generalize these

findings, it is essential to investigate personal and organizational factors in various contexts beyond travel, such as trust in banks, reputation of hospitals, and informativeness of product description.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, 50(3).

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents - Privacy Concerns - Outcomes model. *Journal of Information Science*, 43(5), 583–600.

Gabisch, J. A., & Milne, G. R. (2013). Self-disclosure on the web: Rewards, safety cues, and the moderating role of regulatory focus. *Journal of Research in Interactive Marketing*, 7(2), 140–158.

Harris Interactive. *Most people are privacy pragmatists who, while concerned about privacy, will sometimes trade it off for other benefits*. 2003.

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly: Management Information Systems*, 31(1), 19–33.

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, 66, 75–87.

Kumaraguru, P., & Cranor, L. (2005). Privacy indexes: A survey of westin's studies. School of Computer Science, Carnegie Mellon University.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, 57(1), 343–354.

Lu, Y., Ou, C., & Angelopoulos, S. (2018). Exploring the effect of monetary incentives on user behavior in online sharing platforms. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, 3437–3444.

Morton, A., & Sasse, M. A. (2014). Desperately seeking assurances: Segmenting users by their information-seeking preferences a q methodology study of users' ranking of privacy, security & trust cues. In *Twelfth Annual International Conference on Privacy, Security and Trust IEEE*, 102–111.

Poikela, M., Schmidt, R., Wechsung, I., & Möller, S. (2014). Locate!-When do users disclose location? In *Tenth Symposium On Usable Privacy and Security (SOUPS)*. Menlo Park, CA. 2014.

Ridley-Siegert, T. (2015). Data privacy: What the consumer really thinks. *Journal of Direct, Data and Digital Marketing Practice*, 17(1), 30–35.

Sheehan, K. B. (2002). Toward a typology of internet users and online privacy concerns. *Information Society*, 18(1), 21–32.

Șchiopu, D. (2010). Applying TwoStep cluster analysis for identifying bank customers' profile. *Buletinul*, 62, 66-75.

Thaler, R. H., & Sunstein, C. R. (2003). Libertarian paternalism. *American Economic Review,* 93(2), 175–179.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin.

Tussyadiah, I., Li, S., & Miller, G. (2019). Privacy protection in tourism: Where we are and where we should be heading For. In *Information and Communication Technologies in Tourism 2019*. Springer, Cham, 278-290.

Westin, A., Louis, H., and Associates (1991). Harris-equifax consumer privacy survey.

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human Computer Studies*, 98, 95–108.

Woodruff, A., Pihur, V., Consolvo, S., Brandimarte, L., & Acquisti, A. (2014). Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In *USENIX Association Tenth Symposium On Usable Privacy and Security*.

Wozniak, T., Schaffner, D., Stanoevska-Slabeva, K., & Lenz-Kesekamp, V. (2018). Psychological antecedents of mobile consumer behaviour and implications for customer journeys in tourism. *Information Technology and Tourism*, 18(1–4), 85–112.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association of Information Systems*, 12(12), 798–824.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy. *The Journal of Consumer Affairs*, 43(3), 389–418.

Zhang, T., Ramakrishnan, R., & Livny, M. (1996, June). BIRCH: an efficient data clustering method for very large databases. *ACM Sigmod Record*, 25(2), 103-114.