Iis Tussyadiah, Shujun Li and Graham Miller, "Privacy protection in tourism: Where we are and where we should be heading for," in I*nformation and Communication Technologies in Tourism 2019: Proceedings of the International Conference in Nicosia, Cyprus, January 30–February 1, 2019*, pp. 278-290, 2019, https://doi.org/10.1007/978-3-030-05940-8_22

Privacy protection in tourism: Where we are and where we should be heading for*

Iis Tussyadiah[a], Shujun Li[b], and Graham Miller[a]

[a]School of Hospitality and Tourism Management
University of Surrey, United Kingdom
{i.tussyadiah; g.miller}@surrey.ac.uk

[b]Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)
and School of Computing
University of Kent, United Kingdom
s.j.li@kent.ac.uk

Abstract

The link between information privacy concerns and privacy behaviours has been a focus of extensive investigation in various disciplines. However, little attention has been devoted to this issue in the tourism literature. Spurred by technological development and shaped by tourism-related environments, emerging privacy issues call for comprehensive yet context-specific studies to ensure tourists are making beneficial privacy choices. This paper first presents a comprehensive review of state-of-the-art research on privacy concerns and behaviours. Then, it suggests a list of overarching research priorities, merging social and technical aspects of privacy protection approaches as they apply to tourism. The priorities include research to measure tourists' privacy concerns, explore specific biases in tourists' privacy decisions, experiment with privacy nudges, and explore how to integrate privacy nudges in system design. Thus, this paper contributes to guiding the direction of future research on privacy protection in tourism.

Keywords: privacy concern; personal data; information disclosure; privacy paradox; nudges.

1 Emerging Issues

Tourism is information intensive [1, 2]. Tourists need to process a significant amount of information to make various decisions along their journey from pre-trip planning to in-destination experiences to post-trip evaluation and experience sharing. Correspondingly, tourists are often required to give up personal information in exchange for services to enable (e.g., booking process, visa application) and enhance (e.g., access to discounts) their travel experiences. As an illustration, overwhelmed with the large number and variety of points-of-interest (POIs) in a destination, some tourists will resort to using recommender systems (RSs) to make informed decisions [3]. Various RSs have been developed to suggest POIs, tourist services, user-generated content and social networking services, routes and tours, and personalised multiple-day tour planning [4]. In order to deliver relevant recommendations, these RSs collect and process sensitive data about users, such as their locations, interests, mobility requirements, previous visits, etc., sometimes without tourists being fully aware of it. While getting personalised recommendations is found in prior research to

* Citation: Tussyadiah, I., Li, S., & Miller, G. (2019). Privacy protection in tourism: Where we are and where we should be heading for. *In* Pesonen, J., & Neidhardt, J. (Eds.), Information and Communication Technologies in Tourism 2019. Springer.

lead to positive responses, including higher willingness to disclose personal information, it can also lead to negative responses due to higher level of privacy concerns; generating the so-called personalisation–privacy paradox [5].

Indeed, the link between privacy concerns and disclosure of personal information has been a focus of investigation in various disciplines [6, 7, 8]. Its application in the tourism context requires a critical perspective due to several existing and emerging issues that may contribute to less awareness of privacy threats and greater vulnerability to violations [9, 10]. *First*, information technologies develop fast and travel and tourism tend to be among the first industries to embrace them [2]. While tourists have an option to skip the use of emerging technologies such as mobile payment while travelling, some other technologies are much harder or impossible to avoid. An example is the use of automated check-in kiosks collecting biometric information at an airport gate. Additionally, destinations increasingly use real-time surveillance system for safety and security purposes, to protect tourists and residents from crimes. Tourists may not be aware of the range of privacy and security threats that come with these technologies. Furthermore, recent breakthroughs in Artificial Intelligence (AI) have allowed tourists to rely on automated systems such as an intelligent personal assistant, a system that is capable of learning the interests and behaviour of the user and respond accordingly [11]. This potentially raises new layers of privacy concerns.

Second, being in an unfamiliar environment, tourists may be easily persuaded to disclose personal information due to an inflated sense of urgency to obtain information and/or services [9]. This applies when information is considered time-critical, as tourists try to maximise activities within the limited length of stay. For the same reason, tourists may feel more at ease when sharing information with organisations or individuals they do not expect to interact extensively (or at all) anymore after the trip. *Third*, tourists' relationships with service providers and thus services rendered/used are typically short-lived and variety-seeking tourists are seldom loyal customers [10]. This will limit trust building, which may affect privacy decisions. *Fourth*, due to the prevalence of online social networks (OSNs) among Internet users, many travellers would like to share their travel experience including pictures and videos with friends and the public, both during and after the trip. Many of them consider this an important part of their overall travel experience, so have a tendency to overshare. Note that such information sharing activities often involve sharing information of other people (e.g., family members and friends travelling together or being visited). *Last*, with the prevalent use of peer-to-peer (P2P) platforms such as Airbnb and Uber where trust mechanism is built upon reciprocal reviews, sensitive personal information revealed privately during offline guest–host interactions may reach the public sphere or a scope wider than expected by way of online reviews. This implies the risks from compounded physical and informational privacy [12].

These emerging issues call for comprehensive studies to better understand the ever more complex information privacy decision making for tourists. Importantly, as privacy failures can impact not only the travel industry and tourism destinations, but also a wider society, efforts to bring about desired privacy behaviours from tourists are critical. To that end, this paper aims to review the state-of-the-art research on the

topic of information privacy from various disciplinary perspectives and, based on emerging issues in tourism, recommend areas of research priorities to ensure tourists are making more informed choices when it comes to disclosing personal information related to their travels.

2 State-of-the-Art

Westin [13] defined privacy as "…the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p.7). Subsequent research conceptualised privacy as a right or an ability to control how information about self is collected, retained and/or maintained, used and communicated, disclosed or shared [14]. More specifically, the definitional approach is classified to privacy into value-based (privacy as a human right integral to society's moral value system) or cognate-based (privacy is related to individual's mind, perceptions, and cognition rather than to an absolute moral value) [15]. The first approach defined privacy as a right and as a commodity (economic subject), while the latter defined privacy as a state (of limited access to information) and as (ability to) control information [15]. These definitions influence how privacy is measured in empirical research.

While research on information privacy in the context of tourism is extremely limited, the topic, especially pertaining to behaviour in online environments, has been extensively investigated in behaviour economics, decision science, and information systems disciplines. As suggested in a number of systematic review and meta-analytic studies [6, 7, 8, 15, 16, 17, 18], research on privacy has focused on individuals' privacy behaviours, specifically investigating perceived privacy concerns and its antecedents and consequences, cognitive and behavioural biases influencing privacy decisions, including the concept of privacy paradox, and nudge strategies for positive behaviour intervention.

2.1 Perceived Privacy Concerns

Privacy concerns, which refer to individuals' beliefs about the risks and potential negative consequences associated with disclosing personal information [6, 19], are considered a measurable proxy for privacy [15]. In essence, consumers who are worried about information privacy would take protective actions to reduce these perceived risks, which will generate significant impacts on service providers. Therefore, studies have been dedicated to theorising privacy concerns and finding empirical support for behavioural models linking privacy concerns and privacy management [8, 18], also termed the macro model of APCO (Antecedents → Privacy Concerns → Outcomes) to assess privacy at an individual level [15].

Theories of Privacy Concerns. Li [18] presents a comprehensive analysis of the theoretical landscape underlying information privacy concerns. To explain what leads to privacy concerns, research refers to Agency Theory [20] and Social Contract Theory [21], which elucidate how privacy concerns exist due to incomplete information and providers' opportunistic behaviour regarding customer information. The consequences of privacy concerns are generally explained with Theory of Reasoned Action (TRA) [22] and Theory of Planned Behaviour (TPB) [23], which

describe how privacy concerns can manifest in attitude toward privacy, intention, and information disclosure behaviour. Other systematic reviews have also been devoted to the relationship between different consequences of privacy concerns [7, 17], specifically on the (information) Privacy Paradox [24, 25, 26], which refers to the dichotomy of privacy attitude and actual behaviour.

The Privacy Calculus Theory [27, 28] plays a central role in explicating the trade-offs (benefits vs. risks) consumers consider when deciding to disclose personal information. Three various forms of privacy calculus were also considered in previous research: Utility Maximisation Theory [29], Expectancy Theory of Motivation [30], and Expectancy-Value Theory [22]. The discussions regarding risks and benefits of information disclosure also dominated the literature on Privacy Paradox [7, 17], with a multitude of theories used to elucidate risk–benefit calculation in privacy decisions as guided by rationality (e.g., Rational Choice Theory of Human Behaviour [31], Resource Exchange Theory [32, 33]), biases in risk–benefit assessment (e.g., Theory of Bounded Rationality [34], Uses and Gratification Theory [35, 36], Prospect Theory [37]), and failure to perceive risks associated with privacy decisions (e.g., Theory of Incomplete Information [38]). Biases associated with privacy decisions, including heuristics, will be discussed in the next section.

Finally, to explain factors influencing privacy concerns, such as institutional and individual factors, different theories were used in previous research, including Procedural Fairness Theory (27), Protection Motivation Theory [39], and Social Cognitive Theory [40, 41]. Li [18] suggests the mediating role of protection-motivation in the impacts of institutional and individual factors on perceived privacy concerns and proposes a new Risk Calculus Theory, referring to the trade-off between perceived risks and the efficacy to cope with these risks, which together with the privacy calculus form the *Dual-Calculus* model determining individuals' intention to disclose personal information.

Measures of Privacy Concerns. Notable frameworks to assess individuals' concerns for privacy include Global Information Privacy Concerns (GPIC), Concerns for Information Privacy (CFIP) [42], and Internet Users' Information Privacy Concerns (IUIPC) scales [43]. GPIC is a unidimensional scale measuring privacy concerns in general, while CFIP delves into specific dimensions of individual's privacy concerns, mainly focusing on organisations' responsibilities for the proper handling of customer information. CFIP consists of four dimensions: the collection of personal information, unauthorised secondary use of personal information, improper access to personal information, and errors in storing of personal information. The purpose of IUIPC is to reflect internet users' concerns, focusing on perceptions of fairness and justice in the context of information privacy in online environments [43]. It has three factors: collection (whether the exchange of personal information is equitable), control (whether users have control over the data), and awareness (whether users are adequately informed about the use of the data). Various privacy research has adopted the aforementioned scales, adapted them to specific research contexts, or refined the scales with additional dimensions, such as technological, socio-cultural, and legal aspects of privacy concerns [12, 44, 45]. Research calls for refining the privacy concerns construct by incorporating various facets of information privacy and test the construct validity in different contexts [8], including tourism.

Antecedents of Privacy Concerns. In general, individuals' concerns of information privacy depend on a number of factors. Antecedents evaluated in empirical research on privacy are summarised in [8] and [15]. Reviewing privacy research in the marketing domain, [45] categorised these factors into consumer determinants (psychology of privacy), which are affected by privacy in society factors. They include:

- *Individual factors*: demographic differences, personality differences, privacy experiences, privacy awareness and knowledge, psychological and socio-psychological factors (including dispositions to heuristics, which will be discussed in subsequent section), self-efficacy, etc.
- *Social-relational factors:* the influence of important others (social norms/subjective norms).
- *Organisational factors*: awareness of improper handling of personal data by organisations and organisational communication of privacy.
- *Macro-environmental factors*: ethical framework, global variation (cross-cultural preferences, cross-national regulatory variation and effects), and legal and policy implications (privacy failure intervention).
- *Information contingencies*: types and sensitivity of information (personally identifiable information, medical records, financial information, biometric templates, etc.).

Previous research calls for exploration for additional antecedent factors to privacy concerns [8], especially as they relate to risks associated with various contexts.

Outcomes of Privacy Concerns. As an independent variable, privacy concerns are linked to behavioural responses [15]. In marketing research, a range of outcomes at the individual level include purchase intent, willingness to disclose information, click-through (in online environments), falsifying information, negative word-of-mouth, and switching behaviour [45]. In general, consequences of privacy concerns are analysed from TRA and TPB perspectives, which can be categorised into [8]:

- *Personal beliefs*: trusting beliefs, risk and uncertainty beliefs, etc.
- *Attitude*: conceptualised as a direct result of beliefs, it refers to attitude toward information disclosure.
- *Behavioural intention*: intention to share, to adopt, to take protective actions, etc.
- *Actual behaviour*: transactional behaviours (e.g., information disclosure) and protective behaviours (e.g., refusal to provide information, removal of information, negative word-of-mouth, information fabrication) [47, 48].

While the conceptualised link between attitude, intention, and behaviour has been validated, behaviour research also found discrepancies between attitude, intention and actual behaviour [48], as captured in the concept of privacy paradox [7, 17, 26]. This remains an important research area. The following subsection will touch upon the limitations faced by consumers when making decisions to disclose personal information, which provide some explanation to some of the inconsistencies in consumers' privacy behaviour.

2.2 Cognitive and Behavioural Biases in Privacy Decisions

Early research on privacy behaviour based its assumption on rational model of decision-making, assuming that people make rational deliberation comparing risks and benefits of information disclosure [28, 42]. However, privacy behaviours are complex and nuanced; they are also made based on heuristics, affects, and emotions [16, 17]. Based on a comprehensive review of research in behavioural decision research, behavioural economics, and experimental psychology, three hurdles that consumers face when making privacy decisions, preventing them from making rational choices, were suggested [16]. *First*, technologies and threats constantly evolve, so users are left with incomplete and asymmetric information. Data holders (e.g., service providers) usually have more information regarding the purposes and conditions of future use of personal data, compared to consumers. *Second*, consumers have limited mental resources to evaluate all possible consequences of their behaviour (i.e., bounded rationality), leading them to lean on heuristics. *Third*, privacy decisions are prone to be affected by cognitive and behavioural biases.

Some of the psychological biases found in previous research to influence privacy and security decisions are [7, 16, 17]:

- *Anchoring*: consumers may be affected by what others do when deciding to disclose personal information, regardless of the consequences that it may entail.
- *Loss aversion*: people report high privacy concerns about companies gathering their personal information (loss), but refuse to pay for privacy protection.
- *Framing effect*: consumers may find a privacy policy more desirable when framed as more protective compared to a reference point (e.g., a competitor's privacy notice), thus affecting their willingness to share personal information.
- *Hyperbolic discounting* or *immediate gratification bias*: consumers may choose an option with immediate gain in choices involving inter-temporal trade-offs, such as access to desired services (immediate benefit) vs. privacy costs that may be incurred months later (risk diffusion).
- *Optimism bias and overconfidence*: consumers may be overconfident in their assessment of privacy or security risks.
- *Post-completion errors*: consumers omitting secondary tasks (e.g., logging out of a shared computer) after completing a primary task (e.g., booking a tour), leading to privacy and security risks.
- *Status quo bias*: people have an affinity for default choices, such as the default configurations of privacy tools without actually reviewing the settings.
- *Habit*: habitual use of technologies spills over to other consumption situations.
- *Indeterminacy* (from quantum theory): consumers may alter their preferences indeterminately, at the time an actual decision is made.

Users are often unaware of these biases and tend to be influenced by the same biases as they make similar decisions. This signifies the need for behavioural interventions to avoid negative consequences of poor privacy-related decisions.

2.3 Nudges for Privacy

In light of the limitations facing consumers when making privacy decisions, researchers have attempted to identify approaches to balancing information disclosure

and protection of personal data in ways that optimise consumers' overall welfare and minimise losses such as regrettable disclosure. Previous research uses soft paternalistic intervention approaches (or nudges) [49, 50], applying lessons from behavioural research to design policies, systems, and choice architectures to nudge users toward more beneficial choices [16, 51]. Six interrelated nudging dimensions were proposed [16] to mitigate (or exploit) the aforementioned limitations in privacy decisions, which include:

- *Nudging with information*: reducing information asymmetries and providing a realistic perspective of risks via education (prior to decision) and feedback (after decision). For example, presenting privacy settings in a concise and readable manner (e.g., "everyone can see this photo.") will improve user's understanding of privacy risks and result in responsible data sharing behaviour.
- *Nudging with presentation*: providing necessary contextual cues in the user interface to reduce cognitive load and convey the appropriate level of risk through framing and structure (e.g., increasing saliency or exaggerating privacy risk).
- *Nudging with defaults*: reduce user effort by configuring the system according to users' expectations, such as defaults for opting-in or opting-out consent.
- *Nudging with incentives*: motivating users to behave according to their stated preferences through rewards and punishments. These also include non-financial rewards and punishments such as social support and peer pressure. Another example is nudging away from risky behaviour by making it more difficult to share information (e.g., by multiple confirmation).
- *Facilitating reversibility and error resiliency:* limiting the impact of mistakes by designing systems that ease error correction, through forced actions or automated completion and reversibility (e.g., deleting regrettable posts, comments, or tweets that reveal too much information).
- *Timing of nudges*: defining the right moment to nudge.

Further, Acquisti et al. [16] raise a question regarding how far nudging should go in influencing user behaviour, especially in situations where right or wrong decisions are not entirely clear. This calls for further studies pertaining to implementation of nudges, including the ethical and legal aspects of it (i.e., liability issues arising from consumers following nudges that are later proven illegal). Additionally, there may be no one-size-fits-all approach to nudging for privacy. Thus, identifying most effective nudges for different population and privacy contexts is a critical research area.

3 Research Priorities

Extensive research on information privacy has been done in various disciplines. Yet, these call for further studies to continue the research tradition in this area, to refine the measurements of privacy, and to explore the dynamics of individuals' privacy management and behaviours in various contexts. Taking the context of tourism, it is critical that future research will not be a mere attempt to test whether existing theories and models are applicable to tourists and tourism, but instead enrich the literature by refining the conceptualisation of privacy and exploring new factors that contribute to the better understanding of general and situational privacy behaviour. Therefore, a set

of research priorities is presented in the following, taking into consideration emerging issues and the state-of-the-art, to guide future research on this topic (see Fig. 1).

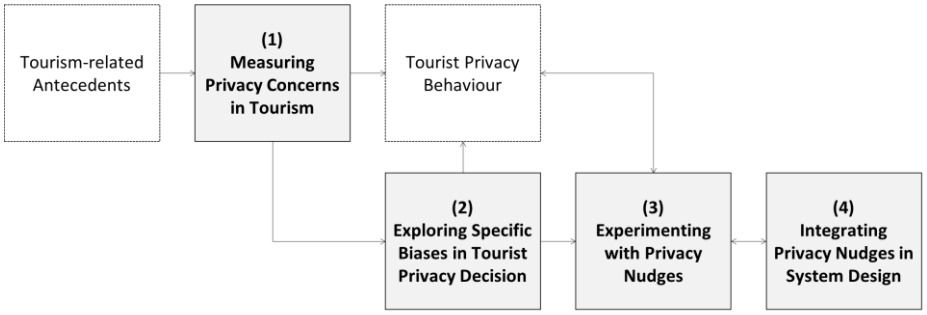

Fig. 1. Privacy Protection in eTourism: Research Priorities

3.1 Measuring Privacy Concerns in Tourism

In order to assess privacy concerns in the context of tourism, it is necessary to refine existing privacy concerns construct by incorporating different facets of information privacy, integrating potential compounding privacy concerns from online and offline (i.e., cyber-physical) environments, and validate the constructs with diverse population of tourists. Furthermore, future research needs to focus on identifying specific antecedents and consequences of tourists' privacy concerns. Specifically, contextual factors will influence information contingencies involved in tourists' disclosure behaviour, such as types and sensitivity of information, as well as organisational and macro-environmental factors. For instance, the influence of cross-national regulatory contexts in international travel will be an important area to explore: as tourists crossed boundaries, they would need to adapt to new regulatory frameworks for privacy protection and (mandatory) information disclosure, which might add to privacy concerns. Additionally, it is necessary to further explore the limited interactions and thus opportunities for trust building between tourists and service providers and their consequences on information disclosure behaviour. Lastly, in terms of behavioural outcomes, future research should be devoted to examine whether tourists employ different disclosure or protective actions while travelling compared to actions in daily life and to what extent the privacy paradox phenomenon (i.e. discrepancy between attitude and behaviour) exists in travel contexts.

3.2 Exploring Specific Biases in Tourists' Privacy Decisions

Tourism is a hedonic experience; leisure tourists typically search for enjoyment from traveling to a destination. This may have an influence on tourists leaning more toward employing affect heuristics when making decisions while travelling. In addition, the fact that tourists will be in unfamiliar environments and have limited access to resources they normally have at home, the problem of incomplete information may be stronger for tourists, which may result in added anxiety. This may also lead to underestimation of risks due to the transient nature of travel activities. Furthermore, tourists may need to use entirely different sets of service providers, adding to information asymmetry issues. Therefore, future research needs to focus on specific

biases that influence tourists' privacy decisions. These may also include a greater potential for hyperbolic discounting due to time-critical services and information in the limited time of traveling and post-completion errors as tourists are driven to complete their primary to-do list in the destination (e.g., forgetting to log out or delete browsing history after using a computer in a hotel's business centre to search for nearby attractions or to check-in for a flight online).

3.3 Experimenting with Nudges

Based on specific hurdles tourists face for their privacy decisions, future research needs to be devoted to evaluation of different nudges and their outcomes. It is important that a range of nudging strategies and specific designs of those strategies are tested to tackle the most prevalent biases that pose greater risk for privacy failures (suboptimal privacy-related decisions) in the travel contexts. From a methodological point of view, behavioural experiments with nudges will yield relevant results to test the effectiveness of nudging strategies and designs. These can be done in a controlled lab setting to quickly assess how people react to various nudging strategies for travellers and in the field, such as places of transit and tourist destinations, to assess the impacts of nudges on actual tourist behaviour in the real world. Importantly, while people might respond positively to education and feedback (i.e., nudging with information) as they complete travel-related tasks in a lab experiment, such as booking accommodation or sharing travel photos with their social network, they might not have the same responses to these strategies while actually traveling. Therefore, a combination of lab-based and field studies will be desirable for more robust results.

3.4 Integrating Privacy Nudges in System Design

As a general principle, Privacy by Design (PbD) including privacy by default has been widely accepted by both designers and end users, and also been included in the latest European data protection law, General Data Protection Regulation (GDPR). However, despite a lot of efforts on privacy enhancing technologies, there have been much less work on applying behavioural nudges in technical solutions of privacy protection. To better incorporate privacy nudges into a tourist-facing privacy protection system, more future research is called to address at least the following aspects: computational ontology for incorporating proven theories in behavioural science into the automated system, environmental and behavioural monitoring for personalising and contextualising nudges, (semi-)automated privacy risk assessment including mathematical models of different parts of the whole process, the use of interactive information visualisation for qualitative presentation of risks and nudges, information fusion of data from multiple sources to cover a more complete picture of users' privacy behaviour and privacy risks, and human-in-the-loop approach to facilitating incremental refinement of automated components.

4 Concluding Remarks

In light of existing and emerging privacy issues in tourism, comprehensive yet context-specific studies are needed to better understand tourists' privacy decision making process in order to ensure they are making informed decisions when it comes

to sharing personal information while traveling. This paper presents a comprehensive review of state-of-the-art research on privacy concerns, cognitive biases in privacy decisions, and nudges for privacy. This review is inclusive of theoretical foundation underpinning the conceptual framework of previous information privacy research in various contexts as well as methodological framework to empirically measure privacy-related concepts, such as privacy concerns and their antecedents and outcomes. Based on this review, this paper provides a set of overarching research priorities, merging the social and technical aspects of privacy protection framework to nudge tourists into making more responsible disclosure decisions. In so doing, this paper contributes to guiding the direction of future research on information privacy in tourism context.

The research priorities are intended to affect various groups of researchers and practitioners in tourism. First, for researchers focusing on tourist behaviour, the theoretical models and methodological frameworks reviewed herein could be applied to explain and measure tourists' privacy concerns, including their antecedents and outcomes, and cognitive biases in tourists' privacy decisions. Second, for researchers focusing on tourism-related policy, travel organisations, and policymakers, the array of nudging strategies explained herein could be implemented to influence tourists' privacy behaviours. Finally, for researchers and practitioners in tourism information systems and technologies, the priorities should entice the design of an effective tourist-facing privacy protection system.

References

1. Gretzel U (2011) Intelligent systems in tourism: A social science perspective. Annals of Tourism Research, 38(3), 757-779.
2. Werthner H, Klein S (1999) Information technology and tourism—A challenging relationship. Springer: Vienna.
3. Drosatos G, Efraimidis PS, Arampatzis A, Stamatelatos G, Athanasiadis IN (2015). Pythia: A Privacy-enhanced Personalized Contextual Suggestion System for Tourism. 2015 IEEE 39th Annual International Computers, Software & Applications Conference. doi: 10.1109/COMPSAC.2015.88
4. Gavalas D, Kasapakis V, Konstantopoulos C, Mastakas K, Pantziou G (2013) A survey on mobile tourism recommender systems. doi: 10.1109/ICCITechnology.2013.6579536
5. Lee CH, Cranage DA (2011) Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel websites. Tourism Management, 32(5), 987-994.
6. Baruh L, Secinti E, Cemalcilar Z (2017) Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, 67(1), 26-53.
7. Barth S, de Jong MDT (2017) The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. Telematics and Informatics, 34(7), 1038-1058.
8. Li Y (2011) Empirical studies on online information privacy concerns: Literature review and an integrative framework. Communications of the Association for Information Systems, 28, 453-496.
9. Anuar F, Gretzel U (2011) Privacy concerns in the context of location based services for tourism. Paper presented at the ENTER 2011 Conference, Innsbruck, Austria, January 26–28, 2011.
10. Gretzel U, Sigala M, Xiang Z, Koo C (2015) Smart tourism: foundations and developments. Electronic Markets, 25(3), 179-188.

11. Manikonda L, Deotale A, Kambhampati S (2017) What's up with privacy?: User preferences and privacy concerns in intelligent personal assistants. https://arxiv.org/abs/1711.07543
12. Lutz C, Hoffmann CP, Bucher E, Fieseler C (2018) The role of privacy concerns in the sharing economy. Information, Communication & Society, 21(10), 1472-1492.
13. Westin AF (1967) Privacy and freedom. Atheneum: New York.
14. Xu H, Teo H-H (2004) Alleviating consumers' privacy concerns in location-based services: A psychological control perspective. ICIS 2004 Proceedings, 64. https://aisel.aisnet.org/icis2004/64
15. Smith HJ, Dinev T, Xu H (2011) Information privacy research: An interdisciplinary review. MIS Quarterly, 35(4), 89-1015.
16. Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, Leon PG, 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), 44.
17. Kokolakis S (2017) Privacy attitudes and privacy behaviour. Computers and Security, 64(C), 122-134.
18. Li Y (2012) Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems, 54(1), 471-481.
19. Zhou T, Li H (2014) Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. Computers in Human Behavior, 37, 283–289.
20. Eisenhardt KM (1989) Agency Theory: An Assessment and Review. The Academy of Management Review, 14(1), 57-74.
21. Milne GR, Gordon ME (1993) Direct mail privacy-efficiency trade-offs within an implied social contract framework. Journal of Public Policy & Marketing, 12(2), 206-215.
22. Ajzen I (1991) The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50, 179-211.
23. Ajzen I, Fishbein M (1980) Understanding attitudes and predicting social behavior. Prentice-Hall, Englewood-Cliffs, NJ.
24. Acquisti A (2004) Privacy in electronic commerce and the economics of immediate gratification. Proceedings of the 5th ACM Conference on Electronic Commerce, 21-29.
25. Barnes SB (2006) A privacy paradox: Social networking in the United States. First Monday, 11. http://dx.doi.org/10.5210/fm.v11i9.1394
26. Norberg PA, Horne DR, Horne DA (2007) The privacy paradox: personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100-126.
27. Culnan MJ, Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science, 10(1), 104-115.
28. Laufer RS, Wolfe, M (1977) Privacy as a concept and a social issue: a multidimensional development theory. Journal of Social Issues, 33(3), 23-42.
29. Awad NF, Krishnan MS (2006) The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly, 30(1), 13-28.
30. Stone EF, Stone DL (1990) Privacy in organizations: theoretical issues, research findings, and protection mechanisms. Research in Personnel and Human Resources Management, 8, 349-411.
31. Simon HA (1955) A behavioral model of rational choice. The Quarterly Journal of Economics, 69(1), 99-118.
32. Donnenwerth GV, Foa UG (1974) Effect of resource class on retaliation to injustice in interpersonal exchange. Journal of Personality and Social Psychology, 29, 785-793.
33. Foa UG (1971) Interpersonal and economic resources. Science, 71, 345-351.
34. Simon HA (1982) Models of Bounded Rationality. Volume 1: Economic Analysis and Public Policy. Volume 2: Behavioural Economics and Business Organization. MIT Press, Cambridge, MA.
35. Blumler JG, Katz E (1974) The Uses of Mass Communication. Sage, Beverly Hills, CA.

36. Katz E, Blumler JG, Gurevitch M (1973) Uses and gratifications research. Public Opinion Quarterly, 37(4), 509-523.
37. Kahneman D, Tversky A (1979) Prospect theory: an analysis of decision under risk. Econometrica, 47(2), 263-291.
38. Harsanyi JC (1967) Games with incomplete information played by "Bayesian" players, I-III. Part I. The basic model. Management Science, 14(3), 159-182.
39. Floyd DL, Prentice-Dunn S, Rogers RW (2000) A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407-429.
40. Bandura A (1986) Social foundations of thought and action: A social cognitive theory. Prentice-Hall, Englewood Cliffs, NJ.
41. Bandura A (2001) Social cognitive theory: an agentic perspective. Annual Review of Psychology, 52, 1-26.
42. Smith HJ, Milberg S, Burke S (1996) Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly, 20(2), 167-196.
43. Malhotra NK, Kim SS, Agarwal J (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355.
44. Buchanan T, Paine C, Joinson AN, Reips UD (2007) Development of measures of online privacy concern and protection for use on the internet. Journal of the American Society for Information Science and Technology, 58(2), 157-165.
45. Martin KD, Murphy PE (2017) The role of data privacy in marketing. Journal of the Academy of Marketing Science 45(2), 135-155.
46. Lwin M, Williams JD, Wirtz J (2007) Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. Journal of the Academy of Marketing Science 35(4), 572-585.
47. Son J-Y, Kim SS (2008) Internet users' information privacy-protective responses: A taxonomy and a nomological model. MIS Quarterly, 32(3), 503-529.
48. Ajzen I, Brown TC, Carvajal F (2004) Explaining the discrepancy between intentions and actions: The case of hypothetical bias in contingent valuation. Personality and Social Psychology Bulletin, 30, 1108-1121.
49. Thaler RH, Sunstein CR (2008) Nudge: Improving decisions about health, wealth, and happiness. Yale University Press, New Haven & London.
50. Hansen PG (2016) The definition of nudge and libertarian paternalism: does the hand fit the glove? European Journal of Risk Regulation, 7(1), 155-174.
51. Acquisti A (2009) Nudging privacy: The behavioral economics of personal information. IEEE Security & Privacy, 7(6), 82-85.
52. Tavani, H. T. 2008. Informational privacy: Concepts, theories, and controversies. In The handbook of information and computer ethics, ed. K. E. Himma and H. T. Tavani, 131–164. Hoboken, NJ: Wiley.

Acknowledgements

This work was part of the "PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers (PriVELT)" Project supported by the UK's Engineering and Physical Sciences Research Council (EPSRC) (EP/R033196/1, EP/R033749/1, and EP/R033609/1).