Transportation Research Part A 171 (2023) 103659

Contents lists available at ScienceDirect

Transportation Research Part A

journal homepage: www.elsevier.com/locate/tra

Perceived benefits as a driver and necessary condition for the willingness of air passengers to provide personal data for non-mandatory digital services at airports

Deodat Mwesiumo [a,e,*], Nigel Halpern [b], Svein Bråthen [a], Thomas Budd [c], Pere Suau-Sanchez [c,d]

[a] Faculty of Logistics, Molde University College – Specialized University in Logistics, Post Box 2110, 6402, Molde, Norway
[b] Department of Marketing, Kristiania University College, Post Box 1190 Sentrum, 0107, Oslo, Norway
[c] Centre for Air Transport Management, Cranfield University, MK43 0TR, Bedfordshire, United Kingdom
[d] Faculty of Business and Economics, Universitat Oberta de Calunya, Rambla del Poblenou 156, 08018 Barcelona, Spain
[e] Møreforsking AS, Britvegen 4, 6410 Molde, Norway

ARTICLE INFO

Keywords:
Digital services at airports
Perceived benefits
Privacy concerns
Privacy calculus
Willingness to provide personal data

ABSTRACT

The willingness of individuals to provide personal data is of interest to policymakers and practitioners seeking to develop more intelligent transportation systems that create value for passengers using technologies, as well as to leverage the use of data more generally to accelerate digital transformation. This study examines the role of perceived benefits as a driver and necessary condition for the willingness of air passengers to provide personal data for non-mandatory digital services at airports. These are services that are not essential for the operation of the airport or for the safety and security of passengers but can enhance the passenger experience or generate additional revenue for the airport. Examples include receiving notifications to a mobile device about their journey and related products and services, accessing customer services online, joining and receiving electronic information from an airport loyalty programme, and making payments for products and services online or via a mobile application. The analysis is based on two samples of 235 and 218 respondents to an online survey where the second sample is used for the purpose of replication. Responses were analysed using a recently developed complementary approach that combines partial least squares structural equation modeling and necessary condition analysis. The findings confirm that perceived benefits are a significant driver and necessary condition for passengers' willingness to provide personal data. More so, perceived benefits significantly attenuate the negative effect that privacy concerns have on passengers' willingness to provide personal data. The findings offer theoretical and methodological contributions, as well as implications for policy and practice.

1. Introduction

According to SITA, 2021, global airport expenditure on technology was US$10 billion in 2018, representing 6.1 % of total revenue. This was up from US$7 billion in 2016 (2.7 % of total revenue). Expenditure declined to US$4 billion by 2020 following the

* Corresponding author.
E-mail address: Deodat.E.Mwesiumo@himolde.no (D. Mwesiumo).

https://doi.org/10.1016/j.tra.2023.103659
Received 19 May 2022; Received in revised form 30 January 2023; Accepted 15 March 2023
Available online 28 March 2023
0965-8564/© 2023 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

coronavirus pandemic. However, due to a sharp drop in revenues during this time, expenditure as a proportion of total revenue increased to 6.3 %, suggesting that airports were still determined to invest in technologies during the pandemic, and this is expected to continue as the industry recovers. SITA, 2021 found that over half of all airports expected to increase expenditure on technology by the end of 2022 compared with previous years, while almost a third expected to spend the same. By comparison, less than one fifth of airports expected to spend less on technology than previous years.

Based on a global survey of airports, conducted at the end of 2019, right before the outbreak of the coronavirus pandemic, Halpern et al. (2020) found that enhancing the passenger experience was the leading driver of investment in technology, and this is also expected to be a key driver as the industry recovers (SITA, 2021). However, personal data is often needed when seeking to create value for passengers using technologies at airports (ACI Europe, 2018; Halpern et al., 2021a; 2021b), as well as for users of other modes of transportation (e.g., see Cottrill, 2020). This is also recognized more generally. For instance, Line et al. (2020) suggest that personal data can help companies identify the most valuable customers and decide how to engage them more effectively, while Anshari et al. (2019) suggest that personal data can facilitate personalization and customization of sales and customer services. Besides enhancing the passenger experience, the processing of passenger data can also be crucial for ensuring the safety and security of transportation systems (McCarthy et al., 2016; Patil et al., 2016), and there has been much debate about the use of biometric technology as a way of verifying the identity of passengers at airports (e.g., see Kasim et al., 2021; Khan & Efthymiou, 2021). This can help to enhance the passenger experience by offering a more seamless journey through airports and improve security checks at airports. Similarly, the processing of passenger data can be crucial for the deployment of contactless technologies used in response to health risks associated with the coronavirus pandemic (e.g., see Serrano & Kazda, 2020).

While personal data can help businesses create more value for customers, there are also growing concerns about data privacy. One example would be location-based mobile applications that use information obtained from a users' smart devices. These potentially enable airports to track passenger movements (e.g., for flow and throughput management purposes) and to offer passengers personalized and customized notifications about their journey and related products and services that are available. However, as noted by Rodríguez-Priego et al. (2022), the implementation and execution of such solutions may raise userś privacy concerns related to sensitive information being handled. Indeed, Meehan (2019) notes that data privacy would be one of the most critical issues in this decade. The rise of privacy concerns is conceivable because, with growing digitalization, more information is collected from individuals (Belanger & Crossler, 2019), making them vulnerable to potential misuse of their personal data (Véliz, 2021). As a result, privacy concerns are regarded as the biggest intrinsic obstacle for the acceptance of new technologies (Tran & Nguyen, 2021), and pose a major challenge for policymakers and practitioners seeking to develop more intelligent transportation systems (e.g., see Fries et al., 2012) and to leverage the use of data more generally to accelerate digital transformation (e.g., see Halpern et al., 2021a; 2021b). There is already evidence of privacy concerns as an obstacle to acceptance in an airport context. For instance, IATA global passenger survey 2018 (IATA, 2018) found that the key reason for preferring paper passports to technology-based alternatives among air travelers was a fear for the security and confidentiality of their personal data. Similarly, Halpern et al. (2021c) found that privacy concerns were significantly higher among passengers preferring to use manual versus technology-based processes at airports. . These observations are consistent with Kasim et al. (2021) and Khan and Efthymiou (2021) who recognize privacy concerns among passengers as a key challenge for the deployment of biometric technologies at airports.

Interestingly, extant literature has recognized the presence of a privacy paradox, that is, a willingness to provide personal data despite reporting high levels of concern about privacy (e.g., see Ioannou et al., 2020a; 2020b; Morosan, 2018). Gerber et al. (2018) argue this can be explained by privacy calculus, which implies that decisions to disclose personal data are contingent upon the potential benefits of doing so. Nevertheless, Lutz and Newlands (2021) note that empirical findings regarding this are inconclusive. As a result, this study addresses three research questions: (1) Do perceived benefits significantly drive passengers' willingness to provide personal data for non-mandatory digital services at airports? (2) Can perceived benefits significantly attenuate the negative effect that privacy concerns have on passengers' willingness to provide personal data for non-mandatory digital services at airports? (3) Are perceived benefits a necessary condition for passengers' willingness to provide personal data for non-mandatory digital services at airports? This study defines non-mandatory digital services as services that are not essential for the operation of the airport or for the safety and security of passengers but can enhance the overall experience or generate additional revenue for the airport. Such services might include receiving notifications about their journey (e.g., flight status, queue times) and related products and services (e.g., public transport, car parking,click and collect shopping, food and drink, lounge or fast-track security access); accessing customer services online; joining and receiving electronic information from an airport loyalty programme; and making payments for products and services online or via a mobile application. The reason for focusing on non-mandatory digital services at airports is because personal data is often processed at airports as a legal and regulatory requirement when passengers carry out mandatory processes such as to check-in, drop baggage, enter the security checkpoint, clear passport control, and enter the boarding gate. Passengers therefore need to provide personal data to obtain these services. The provision of personal data to access non-mandatory digital services (e.g., for commercial or other solutions at airports) is voluntary and passengers therefore have a choice over whether to disclose personal data for such services.

Following Sukhov et al. (2022), this study answers the three research questions by applying a recently developed complementary approach that combines partial least squares structural equation modeling (PLS-SEM) and necessary condition analysis (NCA). The findings are based on an online survey of air travelers in Norway. As will be explained in the methodology section, this study follows a differentiated replication logic. A total of 453 completed responses were included in the analysis, 235 for the main study and 218 for the replication study. The study contributes in three ways. Firstly, while previous studies have focused on examining perceived benefit as a driver for the willingness to provide personal data for digital services in general, this study focuses on non-mandatory digital services which ideally should be more difficult to obtain consent for. Although this study is focused on airports, its insights can inform

scholars and managers interested in other modes of transportation, and those working in other fields such as marketing and consumer behavior, and information systems management. Secondly, it is one of the first studies to examine the necessity of perceived benefits in inducing service users to share their personal data. While previous studies have focused on examining perceived benefit as a driver of willingness to provide personal data, this study goes a step further to examine whether it is also a necessary condition. When a factor representing a necessary condition is absent, it means that the desired effect cannot be achieved. In practice this means that acting on other aspects than the necessary condition will not create the desired effect and would be a waste of effort (Dul, 2016). Thirdly, the study contributes by examining the incidence of privacy calculus by using a contingency approach. Previous studies have examined this mainly by observing a significant positive relationship between perceived benefits and willingness to provide data, and a significant negative relationship between privacy concerns and willingness to provide data. Unlike previous studies, this one examines the interaction effect between perceived benefits and privacy concerns, in addition to examining their main effects. Applying this approach contributes to the development of theory behind privacy calculus logic because, as noted by Dawson and Richter (2006), a contingency approach can significantly contribute to theoretical advancement.

In terms of the structure to this paper, the next section provides a review of literature on the willingness to provide personal data and the need for applying a contingency logic when examining privacy calculus. It also provides rationale for hypotheses that are tested by this study. The methodology section provides details regarding research design, data collection, sample size, operationalization of constructs, potential alternative explanations, and the analytical approach taken by this study. The analysis and findings present the results of the study. The discussion further explores the results, taking theoretical and methodological contributions and implications for policy and practice into consideration. Key findings and related arguments, as well as opportunities for future research, are summarized in the conclusion.

2. Literature review and hypotheses

2.1. Willingness to provide personal data and privacy concerns

In line with Article 4 of the European Union's General Data Protection Regulation (GDPR), this study defines personal data as "any piece of information related to an identified or identifiable person, including name, identification number, location data and an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person". Therefore, the willingness to provide personal data is defined in this paper as the readiness of an individual to offer any piece of information specified in Article 4 of the GDPR. The willingness of individuals to provide personal data has attracted attention from previous studies. Most of them have focused on determining driving factors such as the perceived benefits (Kim et al., 2019; Ioannou et al., 2020a), extrinsic rewards (Yeh et al., 2018), trust in the service provider (Ioannou et al., 2020b), perceptions of security (Morosan, 2018), attitudes and subjective norms (Kasim et al., 2021), and privacy social norms and awareness (Zlatolas et al., 2015). This is understandable because determining drivers provides a basis for guiding business managers seeking to implement measures to increase willingness to provide personal data. Such measures are crucial considering that willingness has tended to decline over time (Goldfarb & Tucker, 2012).

Among the drivers of willingness to provide personal data, the role of privacy concerns has received considerable scholarly attention. Privacy concerns can be defined as an individual's concerns about their ability to control when, how, and to what extent their personal data is used (Ioannou et al., 2020a). Interestingly, while several studies suggest a significant negative association between privacy concerns and willingness to provide personal data, some studies such as Yeh et al. (2018) and Oghazi et al. (2020) have found that there is no significant relationship between the two variables. Remarkably, Ioannou et al. (2020a) found a positive relationship between privacy concerns and the willingness to share personal data. They contended that the positive effect was perhaps due to the privacy paradox, that is, individuals decide to share personal data despite privacy concerns because the benefits outweigh the risks of doing so. Another possible explanation is that since previous studies on the link between privacy concerns and willingness to provide personal data were conducted in different contexts, inadequate measurement approach could be the source of contradicting results (Mwesiumo et al., 2021). In other words, the relationship between privacy concerns and the willingness to share personal data might be contingent on the context in which the data are collected.

Considering the increasing number of contexts in which individuals are asked to provide personal data, privacy concerns will most likely keep growing, including in different contexts within transportation. Examples include privacy concerns related to autonomous vehicles (e.g., Fagnant & Kockelman, 2015), electric scooter sharing services (e.g., Li et al., 2021), airports (e.g., Halpern et al., 2021c), and Mobility as a Service (e.g., Huang, 2022). Over two decades ago, Glancy (1995) argued that "respecting privacy will be important, as advanced technologies improve highways and other surface transportation systems", and "figuring out how to structure transportation applications of advanced computer, communications and other technologies so that the technological infrastructure respects individual privacy will be among the most challenging legal and social issues". Authorities around the world have started to respond to the need for protecting privacy in the transportation sector. For instance, the USA and South Korea have enacted legislations on data privacy that applies to all vehicles, including autonomous vehicles (Taeihagh & Lim, 2019). The SPY Car Act (Congress, 2019) protects the use of (and access to) driving data in all vehicles manufactured for sale in the USA, and likewise, the South Korean Vehicle Management Act (The Government of South Korea, 2017) established conditions for the issuance of temporary licences to test autonomous vehicles and states requirements on data collection for all vehicles. These regulations ensure that personal data related to transportation services are collected following consent of the data subject. In other words, users of the transportation services must be willing to provide their personal data before such data is collected.

2.2. Hypotheses

Overall, most of the previous studies have shown that privacy concerns tend to engender negative attitudes towards providing personal data to service providers. Accordingly, this study argues that as privacy concerns among passengers at airports increases, the more skeptical they will become about providing personal data, and the more likely they will be to refrain from providing it, unless it is mandatory. Consequently, this will result in lower willingness to provide personal data for non-mandatory digital services at airports. However, the notion of privacy calculus implies that individuals act rationally when making privacy-related decisions by weighing the anticipated risks of providing personal data against the potential benefits. Examples of studies that have shown perceived benefits as a driver of the willingness to provide personal data include Trepte et al. (2017) who found that the subjective importance of social gratifications has a positive association with the willingness to have an open profile/to upload pictures accessible to all network friends. Likewise, in the context of mobile applications, Wang et al. (2016) observed that perceived benefits has a significant positive effect on the intention to disclose personal data.

Based on the extant literature discussed in Section 2.1, we argue that perceived benefits should be important when passengers decide to provide personal data for non-mandatory digital services at airports. Furthermore, we argue that perceived benefits constitute a necessary condition for providing personal data. As Dul (2016) explains, a necessary condition allows an outcome to occur such that without it the outcome will not exist. In other words, a necessary condition is a bottleneck that must be managed. In contrast, a driver is a factor that contributes to the occurrence of an outcome, but the outcome may occur despite its absence. Accordingly, this study contends that some form of incentive must be present to motivate passengers to provide personal data for non-mandatory digital services; therefore, perceived benefits should be critical for passengers' willingness to provide personal data. Considering the above reasoning, the following hypotheses are proposed:

H1: Perceived benefits are positively associated with passengers' willingness to provide personal data for non-mandatory digital services at airports.

H2: Perceived benefits are a necessary condition for passengers' willingness to provide personal data for non-mandatory digital services at airports.

Furthermore, based on privacy calculus logic, we argue that perceived benefits should compensate for the perceived risks of sharing personal data, and subsequently weaken the negative effect of privacy concerns on passengers' willingness to provide personal data for non-mandatory digital services at airports. Although the privacy calculus logic is so widely accepted that existing research on information privacy has mostly relied on it (Kehr et al., 2015), previous studies have not examined it explicitly. These studies (e.g., Al-Jabri et al., 2020; Jozani et al., 2020; Trepte et al., 2020) tend to implicitly assume an interaction between perceived benefits and privacy concerns but the interaction between these two factors is neither acknowledged nor tested. Accordingly, the present study contends that a contingency approach is needed when testing privacy calculus. It should involve examining the interaction effect between privacy concerns and the benefits of sharing personal data. Therefore, this study explicitly recognizes the contingency effect embodied by privacy calculus logic and argues that if the decision to share personal data involves a tradeoff of costs and benefits, then perceived benefits should weaken the effect that privacy concerns have on the passengers' willingness to provide personal data. Accordingly, the following hypothesis is proposed:

H3: Perceived benefits weaken the effect that privacy concerns have on the passengers' willingness to provide personal data for non-mandatory digital services at airports.

3. Methodology

3.1. Research design

To test the hypotheses, this study employed a survey method, including replication. We chose to conduct a replication in order to strengthen the basis for empirical generalizations (Iso-Ahola, 2020). According to Uncles and Kwok (2013), replication can take three forms. The first form is exact replication where a study is repeated while keeping the conceptual, methodological, and substantive domains of research intact. The second is close replication where a slight variation is permitted in the conceptual, methodological, or substantive domains of the study. The third is differentiated replication where variation in the conceptual, methodological, or substantive domains is deliberate or purposeful. The present research implemented a differentiated replication that involved a deliberate variation in the methodological domain by measuring privacy concerns in two different ways, using a multi-item scale (main study) versus a global/generalized indicator which semantically addresses the target construct (replication study). Rather than applying other forms of replication, a differentiated replication was chosen to determine whether the findings of the main study are robust and not simply an artifact of the specific measurement used (Uncles & Kwok, 2013).

3.2. Data collection

Data were collected using a self-administered survey consisting of questions that represent the focal constructs and other variables of interest. The survey was implemented using an online panel provided by Qualtrics. Lowry et al. (2016) suggest that researchers can obtain high quality data from online panels by making proper data collection choices and engaging in appropriate practices. This study ensured quality by following the latest procedures recommended when collecting data via online panels. These include providing strong pre-screeners for the target respondents, verifying their IP addresses, checking for possible duplicates, and assessing rushed responses.

Screening of respondents was done based on four criteria: age, residency, gender, and the number of flights taken. Thus, eligible respondents were individuals who had taken at least one return flight during the last 24 months (24 months was used instead of a shorter period of say 12 months due to reduced travel during the coronavirus pandemic in the 12 months before conducting the survey at the end of 2020). Regarding age and residency, respondents had to be at least 18 years old, and reside in Norway – the country in which funding was received to conduct the study. As for gender, Qualtrics was instructed to balance gender representation.

Respondents were asked to consider personal data requested for non-mandatory digital services at airports. The surveys were written in Norwegian. To ensure accuracy, the surveys were pre-tested, and later piloted with 50 panel respondents before being approved for distribution. The demographics of the respondents in the main study are presented in Table 1.

3.3. Sample size and addressing potential common method variance

To determine an appropriate sample size for this study, the inverse square root method proposed by Kock and Hadaya (2018) was applied. Using data from the pilot study (50 observations), this involved regressing the willingness to provide data on privacy concerns and perceived benefits. The path coefficients of privacy concerns and perceived benefits were −0.246 and 0.628 respectively. Following the inverse square root method, the path with the smallest absolute value (0.246) was used to compute a minimum sample size required to achieve an 80 % statistical power. The result showed that a minimum sample size of 102 was required. Eventually, Qualtrics was instructed to launch the main data collection. After eliminating rushed responses (any response completed faster than the 25 % trimmed mean of the completion time), a total of 235 observations were used for the analysis. Potential common method variance was addressed by using ex-ante strategies related to the design of the survey. First, questions were presented clearly to ensure respondents did not face ambiguity in interpreting them. Second, items of some constructs were mixed to reduce the likelihood of respondents deducing the intended constructs. Third, the estimated model, including a higher-order measurement and an interaction effect made it relatively difficult for an average respondent to infer the intended conceptual model.

3.4. Operationalization of constructs

The focal constructs in this study are the willingness to provide personal data, privacy concerns and perceived benefits of providing personal data. These constructs were operationalized as reflective latent variables using items based on previous studies. Although these items have been used mainly in other contexts, the pilot study confirmed that they are relevant to the airport context. Based on Hong and Thong (2013), privacy concerns were operationalized as a third-order construct consisting of two second-order factors: interaction management (INTM) and information management (INFM), and one first-order factor: awareness (AW). As for the second-order factors, INTM consists of three first-order factors: collection (CO), secondary usage (SU) and control (CR), while INFM consists of two first-order factors: improper access (IA) and errors (ER). Perceived benefits (PB) were measured using three items, based on Al-Jabri et al. (2020). Finally, we considered the willingness to provide personal data to be a concrete attribute, which according to Bergkvist (2016), can adequately be measured by a single item. Therefore, respondents were asked to indicate the extent to which they would be willing to provide personal data for non-mandatory digital services at airports. A 7-point Likert scale was applied for all measures. The choice of this scale as opposed to a 5-point scale was because we wanted to increase measurement precision as a 7-point scale provides more options for respondents to choose from, which allows for more nuanced measurement. Table 2 presents the focal constructs and the items used.

3.5. Potential alternative explanations

Besides the focal constructs, this study includes three variables that could potentially serve as alternative explanations for variations in the willingness to provide personal data. The variables include age, education level, and gender. These variables were included in line with Becker et al. (2016) who recommend the use of control variables which are conceptually meaningful and can potentially

Table 1
Variables representing potential alternative explanations – main study.

Variable	Response	N	%
Gender[a]	Male	119	50.6
	Female	116	49.4
Age	18–24	11	4.7
	25–34	30	12.8
	35–44	41	17.4
	45–54	60	25.5
	55–64	54	23.0
	65+	39	16.6
Highest completed education	No completed education	3	1.3
	Primary/secondary school	82	34.9
	Further education	13	5.5
	Undergraduate degree	83	35.3
	Postgraduate degree	54	23.0

[a] No responses were received for binary or other.

Table 2
The focal constructs and items.

Construct	Items
Privacy concerns (PC)	
Collection (CO)	CO1. It would bother me when I am asked for personal data
	CO2. I would think carefully before providing personal data
	CO3. I am concerned that too much personal data is collected
Secondary usage (SU)	SU1. I would be concerned that personal data I give for a specific purpose, might be used for other purposes
	SU2. I would be concerned that personal data I give might be shared with others without my authorisation
	SU3. I would be concerned that personal data I give might be sold to others without my authorisation
Errors (ER)	ER1. I would be concerned that personal data about me might be inaccurate
	ER2. I would be concerned that procedures to correct errors in my personal data are inadequate
	ER3. I would be concerned that too little time and effort is given to verify the accuracy of my personal data
Improper access (IA)	IA1. I would be concerned that my personal data is not sufficiently protected from unauthorised access
	IA2. I would be concerned that too little time and effort is given to prevent unauthorised access to my personal data
	IA3. I would be concerned that too few steps are taken to make sure that unauthorised people cannot access my personal data
Control (CR)	CR1. I would be concerned that I do not have control over what personal data I need to provide
	CR2. I would be concerned that I do not have control over how my personal data is collected, used and shared
	CR3. I would be concerned that my personal data might be altered or lost without me knowing about it
Awareness (AW)	AW1. I would be concerned when a clear privacy policy is not given when providing personal data
	AW2. I would be concerned when I am not aware of how my personal data will be used
	AW3. I would be concerned when a clear explanation is not given about how my personal data is collected, processed, and used
Benefits of disclosure (BD)	
	BD1. Providing personal data would help airports to serve me better
	BD2. Providing personal data would improve my experience with digital services at airports
	BD3. Overall, I feel that providing personal data would be beneficial for passengers
Willingness to provide personal data (WD)	
	In general, I would be willing to provide personal data for additional digital services at airports

offer alternative theoretical explanations in the hypothetico-deductive model. As such, age was included based on Goldfarb and Tucker (2012) who found that older people are less likely to provide personal data than younger people. They suggest that a possible explanation could be the more limited experience with using information technology among older people and hence a greater level of concern regarding privacy. The greater level of privacy concern for new technologies among older versus younger people is confirmed in an airport context by Halpern et al. (2020).

We also included education level as a possible explanation for the variation in willingness to provide personal data, in the sense that the level of awareness about privacy concerns is expected to increase with education. Finally, gender is included because providing personal data to a service provider involves taking some risk, and several studies suggest that men and women differ significantly in terms of risk-taking, whereby women tend to be more risk averse (e.g. Charness & Gneezy, 2012; Xie et al., 2017). In addition, women have been found to have greater levels of privacy concern regarding transport technology solutions by Zhang et al. (2020). As such, it is assumed that male passengers will be more willing to provide personal data. The potential alternative explanations (AE) are summarized as follows:

AE1: Age is negatively associated with the passengers' willingness to provide personal data for non-mandatory digital services at airports.
AE2: Educational level is negatively associated with the passengers' willingness to provide personal data for non-mandatory digital services at airports.
AE3: Male passengers are more willing provide personal data for non-mandatory digital services at airports than female passengers.

The three variables were operationalized as follows: gender (male, female, non-binary or other), age (18–24, 25–34, 35–44, 45–54, 55–64, 65+), and education level (no completed education, primary/secondary school education, further education, undergraduate degree, postgraduate degree) (Table 1).

3.6. Analytical approach

The analysis was performed using PLS-SEM, a method that is increasingly applied in various research fields, including transportation (e.g. Mandhani et al., 2020; Zhang et al., 2019). Applying PLS-SEM is appropriate because the focal constructs are composite, that is, their empirical essence is represented by the items used to create them (Richter et al., 2016). Besides, modeling privacy concerns as a third-order construct and testing privacy calculus using a contingency approach makes the estimated model rather complex. According to Benitez et al. (2020), PLS-SEM is suitable for estimating such complex models. Finally, Hair et al. (2019) recommends that studies that require latent variable scores for follow-up analyses, such as necessary condition analysis, should use PLS-SEM.

4. Analysis and findings

4.1. Evaluation of the measurement model

The analysis of data began by assessing the measurement model. This assessment is essential for ensuring validity of the results (Henseler et al., 2016). Since constructs in this study were measured using a reflective model, the assessment should involve checking for internal consistency reliability, convergent validity, and discriminant validity. Internal consistency reliability was assessed using ρA (rho_A) proposed by Dijkstra and Henseler (2015). Currently, this is the only consistent reliability coefficient for PLS-SEM construct scores (Benitez et al., 2020). Convergent validity was assessed based on the value of the average variance extracted (AVE). As presented in Table 3, the values of ρA and AVE for all first-order constructs are above the recommended thresholds of 0.7 and 0.5 respectively. Additionally, the loadings of the measurement model meet Hair et al. (2022)'s recommendation that the loading of each item should be higher than 0.7. The discriminant validity of the focal constructs was assessed to ensure that each construct is empirically different from other constructs included in the model. As shown in Table 4, the discriminant validity of the focal constructs is established as the values of the heterotrait-monotrait (HTMT) ratio are well below the maximum threshold of 0.85 recommended by latest guidelines (e.g., Hair et al., 2022).

4.2. Estimating the structural model

The hypotheses were tested through estimation of the path model (Fig. 1) following Hair et al. (2022)'s guidelines. Thus, the analysis was conducted using 10,000 bootstrap samples, and a two-stage approach was applied to test the interaction effect. Values of the path coefficients, effect sizes, and R^2 were checked to assess adequacy of the structural model, while the in-sample predictive power of the model was determined by assessing the value of Stone–Gaisser's Q^2. As recommended by Hair et al. (2022), the main effects were interpreted according to Cohen (1988) [0.02 to 0.14 = small; 0.15 to 0.34 = medium; 0.35 or more = large], while the size of the interaction term was interpreted according to Kenny (2018) [0.005 to 0.009 = small; 0.010 to 0.024 = medium; 0.025 or more = large]. Table 5 reports results of the path model estimation.

As reported in Table 5, the values of R^2 and adjusted R^2 suggest that the independent variables adequately explain the variation in willingness to provide personal data. Likewise, since Q^2 is sufficiently above zero, the in-sample predictive power of the model is established. Since all variance inflation factors (VIF) are below 3, the estimation does not seem to suffer from the problem of multicollinearity. The main effects of privacy concerns and perceived benefits on the willingness to provide personal data are significantly negative (path coefficient = -0.262; $p < 0.001$) and positive (path coefficient = 0.690; $p < 0.001$) respectively. Intriguingly, the effect

Table 3
Results of the measurement model assessment – main study.

Construct and its indicators	Loading	Mean	Standard Deviation	Rho_A	AVE
Collection (CO)[1]				0.869	0.777
CO1	0.843	4.374	1.633		
CO2	0.896	5.183	1.534		
CO3	0.904	5.136	1.603		
Secondary Usage (SU)[1]				0.947	0.903
SU1	0.951	5.396	1.544		
SU2	0.960	5.468	1.539		
SU3	0.939	5.409	1.604		
Control (CR)[1]				0.890	0.808
CR1	0.862	4.791	1.656		
CR2	0.935	5.251	1.574		
CR3	0.898	5.055	1.671		
Awareness (AW)				0.907	0.839
AW1	0.881	5.540	1.447		
AW2	0.934	5.719	1.314		
AW3	0.931	5.651	1.449		
Improper Access (IA)[2]				0.934	0.884
IA1	0.938	5.191	1.539		
IA2	0.928	5.102	1.478		
IA3	0.954	5.140	1.558		
Errors (ER)[2]				0.874	0.797
ER1	0.877	4.336	1.598		
ER2	0.923	4.668	1.476		
ER3	0.878	4.681	1.448		
Benefits of disclosure (BD)				0.932	0.877
BD1	0.950	3.970	1.787		
BD2	0.951	3.774	1.747		
BD3	0.908	4.009	1.810		
Willingness to provide personal data (WD)					
WD	1.000[3]	3.838	1.748	1.000[3]	1.000[3]

[1] Constitutes interaction management; [2]Constitutes information management; [3]Single item.

Table 4
Heterotrait-monotrait (HTMT) ratio values – main study.

	AW	BD	CO	CR	ER	IA	SU
BD	0.316						
CO	0.624	0.568					
CR	0.751	0.377	0.762				
ER	0.555	0.241	0.536	0.748			
IA	0.765	0.391	0.697	0.898	0.768		
SU	0.722	0.391	0.798	0.823	0.655	0.777	
WD	0.398	0.819	0.685	0.499	0.303	0.469	0.476

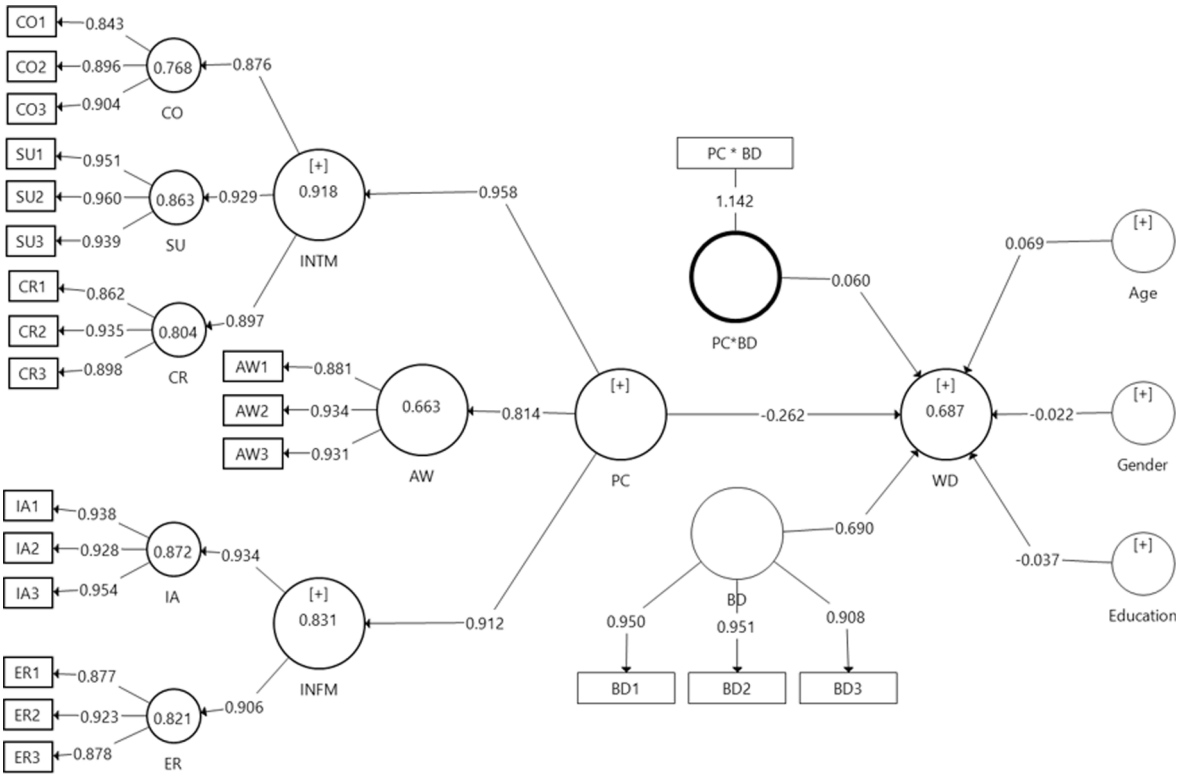

Fig. 1. Path model estimation – main study.

Table 5
Results of path model estimation – main study.

	Effect on WD				
	Path coefficient	p-value	f^2	VIF	Significant
PC	−0.262	0.000[a]	0.168 [M]	1.308	Yes
BD	0.690	0.000[a]	1.116[L]	1.364	Yes
PC*BD	0.060	0.045[b]	0.013[M]	1.121	Yes
Age	0.069	0.090[c]	0.015[N]	1.058	No
Gender	−0.022	0.537[ns]	0.004[N]	1.022	No
Education	−0.037	0.301[ns]	0.002[N]	1.005	No
R^2	0.687				
Adjusted R^2	0.679				
Q^2	0.663				

Significance: [a]significant at $p < 0.01$; [b]significant at $p < 0.05$; [c]significant at $p < 0.1$; [ns]not significant.
Effect size: [L]large; [M]medium; [N]none.

size of perceived benefits is larger ($f^2 = 1.116$) than that of privacy concerns ($f^2 = 0.168$). Of particular interest in this study is the interaction effect of privacy concerns and perceived benefits. The results show that it is significant (path coefficient = 0.060; $p = 0.045$), with a medium effect size ($f^2 = 0.013$), indicating that perceived benefits significantly attenuate the negative effect that privacy concerns have on the willingness to provide personal data. As for the potential alternative explanations, none of them are significant at $p < 0.05$. Although age has a significant path coefficient at $p < 0.1$, looking at the corresponding f^2 value, the magnitude of its effect is negligible.

4.3. Necessary condition analysis (NCA) – Main study

The PLS-SEM results showed that perceived benefits significantly affect passengers' willingness to provide personal data, but a key question for this study is whether perceived benefits constitute a necessary condition for the willingness to provide personal data. Dul et al. (2020) recommends that at least three conditions are met to declare a necessary condition. These include a plausible theoretical justification, considerable effect size ($d > 0$), and a small p value. Like Sukhov et al. (2022), the NCA in this study was conducted according to the general guidelines provided by Dul (2021) and specific guidelines for the combined use of PLS-SEM and NCA (Richter et al., 2020). The analysis was performed in R, an environment for statistical analysis (version 4.0.5), using NCA R package version 3.1.1 (Dul, 2021). The results (Table 6) show that the effect size of perceived benefits is 0.151 ($p < 0.001$), indicating that they constitute a necessary condition for passengers' willingness to provide personal data.

Considering the results of PLS-SEM and NCA, the conclusion is twofold. First, on average, an increase in the perceived benefits significantly leads to an increase in passengers' willingness to provide personal data. Second, as shown by NCA results in Table 6, a certain level of perceived benefits is necessary to trigger the willingness to provide personal data. The results show that up to level 40 of the willingness to provide personal data, perceived benefits are not necessary (NN). However, for level 50 or higher, perceived benefits are necessary.

4.4. Replication study

As noted in Section 3.1, this study involved a differentiated replication where we deliberately changed the methodological domain by measuring privacy concerns using a global/generalized indicator that semantically addresses the target construct. This means the context and conceptual domains were kept the same while the measurement model was changed by deploying a single-item scale for measuring privacy concerns. Thus, we collected a replication dataset using a new survey whereby instead of asking the respondents to rate their perception of different aspects that reflect privacy concerns, we asked one concrete question regarding their level of concern for privacy when using non-mandatory digital services at airports. In other words, the replication study measured privacy concerns using a single item as opposed to multiple items used in the main study. The rationale for using a single item is that privacy related to digital services has been an important social-cultural issue for several years now and has drawn the attention of most people. Thus, privacy concerns can be considered to be a concrete aspect that, according to Bergkvist (2015, 2016), can be measured using a single item.

4.4.1. Sample size and checking the validity of the single-item measurement

After eliminating potential rushed responses, a total of 218 usable responses were obtained. Although single-item scales tend to have lower predictive power, this sample size is well above 102 observations suggested by the results of the inverse square root (Section 3.3). Before testing the hypotheses, we conducted a nomological validity test to check whether the single-item measurement adequately captured the intended construct. In addition to the variables of interest, the survey included questions that measured disposition to privacy and previous exposure to privacy invasion (Table 7). Disposition to privacy refers to a person's general desire or need for privacy across contexts (Li, 2014).

Previous studies found that disposition to privacy and previous exposure to privacy invasion are positively related to privacy concerns. The effect of disposition to privacy is supported by Li (2014) while the effect of previous exposure is supported by Yeh et al. (2018) and Ioannou et al. (2020a). Thus, to test a nomological validity of privacy concerns, we regressed it on previous exposure and disposition to privacy. As shown in Fig. 2, both factors have significant associations with privacy concerns ($p < 0.01$), consistent with the findings of the previous studies. Thus, the single item measurement seems to adequately capture privacy concerns and using it for further analysis is justifiable.

When conducting a replication study, a critical methodological question is whether the studies are comparable considering the potential sampling error due to differences between samples (Altman & Bland, 2014). Thus, comparability of results from two different

Table 6
NCA results – main study.

	Effect size	Bottleneck										
BD	0.151***	NN	NN	NN	NN	NN	2.6	10.0	17.4	24.8	32.2	50.0
Y	–	0	10	20	30	40	50	60	70	80	90	100

Note: The effect size is based on the ceiling envelopment–free disposal hull ceiling (ce-fdh). Significance testing was performed with 10,000 permutations (***Significant at $p < 0.01$); NN stands for not necessary.

Table 7
Operationalizing disposition to privacy, previous exposure, and privacy concerns – replication study.

Construct	Items
Previous exposure to privacy invasion (PE) Rho_A = 0.740 AVE = 0.633	PE1. I believe my personal data (e.g., name, personal number, address, telephone number or payment details) have been monitored, searched, recorded, or stored at least once without my permission PE2. I have had bad experiences with regards to the privacy of my personal data when using services online PE3. I have been a victim of privacy invasion at least once in the past as a result of using services online
Disposition to privacy (DP) Rho_A = 0.810 AVE = 0.687	DP1. Compared to others, I am more sensitive about the privacy of my personal data when using services online DP2. Compared to others, I prefer to keep my personal data private when using services online DP3. Compared to others, I tend to be more concerned about threats to the privacy of my personal data when using services online
Privacy concerns (PC) Rho_A = 1.000[a] AVE = 1.000[a]	Generally, I would be concerned about the privacy of my personal data when using additional digital services at airports

[a] Single item.

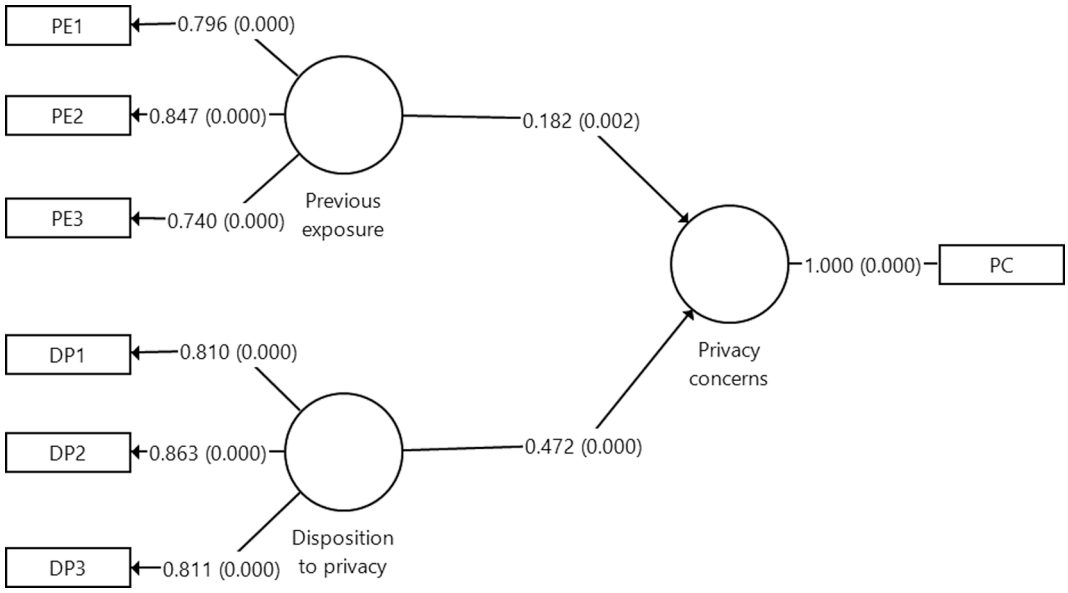

Fig. 2. Testing the nomological validity of privacy concerns measured by a single item.

samples depends on several factors, including the similarity of the samples, the methods used to collect and analyze data, and the specific research question being addressed. To ensure comparability, we instructed Qualtrics to collect responses from a sample that closely resembles the sample in the main study in terms of demographics, sampling method, and sample size. Table 8 (in comparison with Table 1) shows that the sample used in the replication study is comparable to the sample used in the main study in terms of age,

Table 8
Variables representing potential alternative explanations – replication study.

Variable	Response	N	%
Gender[a]	Male	111	50.9
	Female	107	49.1
Age	18–24	15	6.9
	25–34	28	12.8
	35–44	26	11.9
	45–54	51	23.4
	55–64	30	13.8
	65+	68	32.2
Highest completed education	No completed education	3	1.4
	Primary/secondary school	82	37.6
	Further education	6	2.8
	Undergraduate degree	84	38.5
	Postgraduate degree	43	19.7

[a] No responses were received for binary or other.

gender, and education.

4.4.2. Estimating the focal conceptual model

Having confirmed the nomological validity of the single item measurement of privacy concerns, the analysis proceeded to estimate the focal conceptual model that includes perceived benefits and privacy concerns as predictors of passengers' willingness to provide personal data, the interaction effect, and potential alternative explanations. The loadings for perceived benefits were above the recommended threshold of 0.7 (Fig. 2). The internal consistency reliability and convergency validity for the construct were also established as the values of Rho_A and AVE were 0.903 and 0.829 respectively. The discriminant validity for the focal variables was established as all the HTMT values were below the threshold of 0.85 (BD – PC = 0.279; BD – WD = 0.786; PC – WD = 0.363). Fig. 3 presents the estimated model.

Fig. 3 shows the explanatory power of the model is slightly lower ($R^2 = 0.605$) compared with the model based on multi-item measurement of privacy concerns in Fig. 1 ($R^2 = 0.687$). This was expected due to the lower predictive power of the single item measurement. Nevertheless, the model adequately and consistently explains the variation in the willingness to provide personal data. Subsequently, the analysis was conducted using 10,000 bootstrap samples, and a two-stage approach was applied to test the interaction effect. As shown in Table 9, the results of the analysis are consistent with those found in the main study. The main effects of privacy concerns and perceived benefits on the willingness to provide personal data are significantly negative (path coefficient = -0.183; $p < 0.001$) and positive (path coefficient = 0.674; $p < 0.001$), respectively. The effect size of perceived benefits is larger ($f^2 = 1.017$) than that of privacy concerns ($f^2 = 0.076$). The interaction effect of privacy concerns and perceived benefits is significant (path coefficient = 0.105; $p = 0.047$), with a large effect size ($f^2 = 0.032$), indicating that perceived benefits significantly attenuate the effect of privacy concerns on the passengers' willingness to provide personal data. As for the potential alternative explanations, all of them are not significant (at $p < 0.05$) and their effect sizes are negligible. In sum, the results of the differentiated replication are consistent with the findings of the main study. The results therefore provide evidence in support of the three hypotheses in Section 2.2.

4.4.3. NCA – Differentiated replication

Subsequently, NCA was conducted to determine whether perceived benefits constitute a necessary condition for the willingness to provide personal data. The results (Table 10) show that the effect size of perceived benefits is 0.120 ($p < 0.001$), indicating that they constitute a necessary condition for the willingness to provide personal data. As shown in Table 10, up to level 60 of the willingness to provide personal data, perceived benefits are not necessary (NN). However, for level 70 or higher, perceived benefits are necessary. Hence, the NCA results of the replication study are consistent with the NCA results of the main study, providing support that perceived benefits are a necessary condition for the willingness to provide personal data.

5. Discussion

The findings of this study offer theoretical and methodological contributions, as well as implications for policy and practice. In

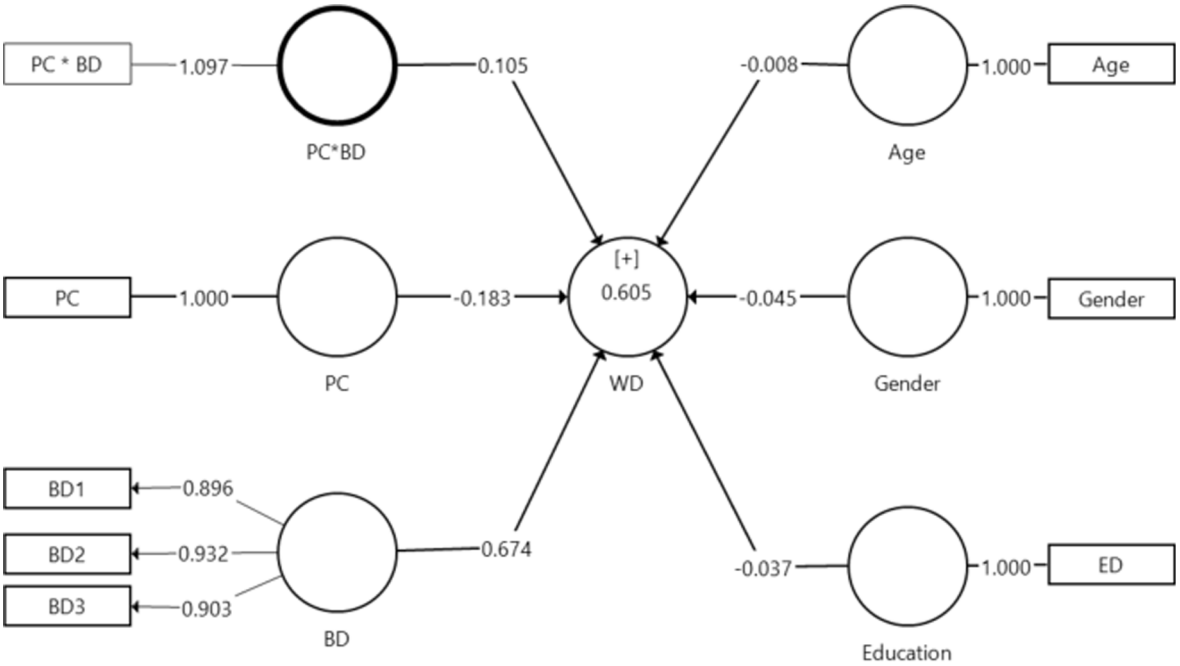

Fig. 3. Path model estimation – replication study.

Table 9
Results of path model estimation – replication study.

	Effect on WD				
	Path coefficient	p-value	f^2	VIF	Significant
PC	−0.183	0.000^{a}	0.076^{S}	1.118	Yes
BD	0.674	0.000^{a}	1.017^{L}	1.130	Yes
PC*BD	0.105	0.047^{b}	0.032^{L}	1.028	Yes
Age	−0.008	0.882	0.000^{N}	1.033	No
Gender	−0.045	0.274^{ns}	0.005^{N}	1.043	No
Education	−0.037	0.438^{ns}	0.003^{N}	1.073	No
R^2	0.605				
Adjusted R^2	0.593				
Q^2	0.582				

Significance: [a]significant at $p < 0.01$; [b]significant at $p < 0.05$; [ns]not significant.
Effect size: [L]large; [M]medium; [S]small; [N]none.

Table 10
NCA results – replication study.

	Effect size	Bottleneck										
BD	0.120***	NN	NN	NN	NN	NN	NN	NN	16.1	16.1	55.7	55.7
Y	–	0	10	20	30	40	50	60	70	80	90	100

Note: The effect size is based on the ceiling envelopment–free disposal hull ceiling (ce-fdh). Significance testing was performed with 10,000 permutations (***Significant at $p < 0.01$); NN stands for not necessary.

terms of theoretical contributions, it confirms the incidence of privacy calculus logic in the context of airports. Unlike previous studies (e.g., Jozani et al. 2020; Trepte et al., 2020), this one explicitly deploys a contingent approach to examine it. Considering that privacy concerns may vary by context (Mwesiumo et al., 2021), our findings provide evidence of the privacy calculus logic in a new context, hence suggesting its broad applicability. This is valuable because manifestation in a wide range of contexts is an important quality of a good theory.

Furthermore, while previous studies mostly examined perceived benefits as a driver for the willingness to provide personal data, this one takes an extra step to examine whether it is a necessary condition for the willingness to provide personal data. The NCA results confirm that it is. This means that in the absence of perceived benefits, passengers will not provide personal data for non-mandatory digital services at airports. Therefore, acting on other aspects than increasing perceived benefits will not guarantee increased willingness to provide personal data and would be a waste of resources. As Bokrantz and Dul (2022) note, the presence of necessary conditions does not guarantee success, but their absence guarantees failure and cannot be compensated by changing the level of other factors. Although necessity causality exists in virtually all research areas, necessity statements are usually not part of the theories (Dul, 2016). Thus, NCA conducted in this study provides an opportunity to test and confirm necessity theory related to the link between perceived benefits and passengers' willingness to provide personal data. Regarding the mechanism that makes perceived benefits a necessary condition, we argue that since personal data in question are requested for services that passengers can live without, and considering that privacy concerns are widespread, to make some passengers share their personal data would certainly require providing considerable incentives. Plausibly, perceived benefits provide such an incentive.

As the willingness of passengers to provide personal data is crucial, especially in the face of data protection regulations and laws, such as the GDPR in the European Union, and the California Consumer Privacy Act and New York Privacy Act in the USA, the findings of this study provide relevant insights for airports. UNCTAD (2021) indicated that 137 out of 194 countries (71 %) had put in place legislation to secure the protection of data and privacy. These regulations include privacy requirements that impact different organizations, including airports. Our findings imply that airports must explore different forms of potential benefits that can entice passengers to provide personal data for non-mandatory digital services. Besides incentives such as discounts on airport products and services, airports can also increase transparency and security measures around data usage and storage to build trust with passengers. Clear and easy-to-understand explanations of how the data will be used and protected can also help to increase the likelihood of passengers providing their personal information. Indeed, these implications are also relevant in other transportation contexts such as autonomous vehicles (Fagnant & Kockelman, 2015), Mobility as a Service (Huang, 2022), and electric scooter sharing (Li et al. 2021) where privacy concerns are critical.

Furthermore, a clear and transparent communication in connection with data use and protection may affect the perceived costs of revealing personal data and hence reduce the need for perceived benefits. One should bear in mind that this is likely to be a matter of confidence-building. Therefore, systematic communication between the stakeholders on the supply and demand side should be developed and designed to run in both directions where applicable. Transparent procedures for storage time and purging of personal data should be a part of the communication strategy. In addition, the nature and content of the benefits for passengers and other users must be clearly communicated. When doing this, one should be aware of both short and long run benefits and to what extent disclosure of personal data could accumulate and increase the amount and quality of passenger services. These recommendations could be relevant for other transport modes as well. For instance, Mobility as a Service (MaaS) with the prospective future of autonomous

vehicles will probably have similar needs for private data exchange.

Interestingly, contrary to our expectations, both studies showed that age, gender, and education do not have significant effects on the passenger's willingness to provide personal data for non-mandatory digital services. One possible explanation is that the effects of these factors perhaps depend on the population, context, or research question under investigation. Indeed, the role of context is crucial when it comes to issues related to privacy in digital services (Smith et al., 2011; Mwesiumo et al. 2021). Norway is one of the countries whose residents have high digital literacy. As of January 2022, Norway's internet penetration rate stood at 99 % of the total population (Kemp, 2022). As most people are used to using digital technology solutions, one can argue that, on average, their attitude towards providing personal data would be accounted for by other factors than demographics.

In terms of its methodological contribution, the differentiated replication study used a single item to measure privacy concerns instead of the normal approach taken by studies (as well as in the main study in this paper) of asking respondents to rate their perception of different aspects that reflect privacy concerns. Despite having somewhat lower predictive power, the single item measurement adequately captured privacy concerns in the replication study. This adds support to the notion that privacy is a well-established social-cultural issue. More importantly, it means that privacy concerns are a concrete aspect that can be measured using a single item. This supports the use of a single item measurement of privacy concerns in future studies, for instance, as an alternative to the 18 items used to measure privacy concerns in the main study – potentially allowing researchers to significantly reduce the length of their surveys.

Privacy concerns have potential implications for government and public agencies that are looking to develop policy and standards to protect the privacy of passengers using airports and other transportation systems, but also for practitioners seeking to encourage a broad acceptance of technology-based solutions in transportation. The results of this study therefore offer actionable insights for policy and practice. In particular, the findings suggest that although privacy concerns are significant determinants of passengers' willingness to provide personal data, perceived benefits have a larger effect. In addition, perceived benefits significantly help to lessen the negative effect of privacy concerns and are in fact a condition for the willingness to provide personal data. Based on the findings of this study, benefits associated with technological investments in transportation need to be effectively communicated to passengers. Otherwise, such investments may not deliver the desired outcomes if a significant proportion of passengers refrain from accepting them.

Of course, not all technological solutions are desired by all passengers. For instance, there might be less interest in downloading an airport mobile application and consenting to receive notifications from it among foreign or infrequent travelers that are less willing to part with personal data for an application they will rarely use. Furthermore, while effective communication of perceived benefits and data handling can lessen privacy concerns, and therefore encourage passengers to part with personal data, the service provider then needs to deliver actual benefits that meet passenger expectations. Also, in addition to effective communications and meeting passenger expectations, there still needs to be sufficient policy and standards in place to protect passengers, as well as effective privacy management practices, for instance among airport operators and third parties that process personal data at airports. Indeed, from a practitioner's perspective, leveraging personal data and effective privacy management is recognized as being critical for digital transformation in transportation (e.g., see ACI, 2017 regarding airports). This can be a challenge given the amount of data exchange that potentially takes place between different stakeholders within a transportation system, for instance, at airports, this typically includes airport operators, airlines, ground handling companies, security companies, government and public agencies, concessionaires, and passengers (ACI Europe, 2018). Determining optimal privacy control for data exchange within the airport and with other transportation systems will play a key role here (e.g. see He & Chow, 2020).

6. Conclusion

To conclude, this study set out to investigate the role of perceived benefits as a driver and necessary condition for passengers' willingness to provide personal data for non-mandatory digital services at airports. It does so by applying a complementary approach that combines PLS-SEM and NCA on responses to an online survey of air travelers in Norway. Results support all three hypotheses that were proposed in the study: (1) that perceived benefits are positively associated with passengers' willingness to disclose personal data; (2) that perceived benefits are a necessary condition for passengers' willingness; (3) that perceived benefits weaken the effect that privacy concerns have on passengers' willingness. The findings suggest that benefits related to non-mandatory digital services should be communicated effectively to passengers. Future research can go one step further by investigating how to frame messages effectively. There has been some research in this area, for instance, Shore (2022) investigates how messaging influences privacy concerns regarding the use of biometrics. However, that study was focused on the influence of news media messaging versus messaging from policymakers and practitioners responsible for authorizing and/or deploying the technologies. Comparative studies of managerial procedures and practices applied within other parts of the transport sector could inform 'best practices' for dealing with data sharing and privacy protection. Several potential alternative explanations were included in the analysis for this study: age, education, and gender. Although they were expected to have a significant effect on the willingness to provide personal data, they turned out to be insignificant. Since the notion of privacy is context-dependent (Smith et al., 2011), future research may investigate if the relevance of demographics in driving the willingness to provide personal data varies across contexts. For instance, future studies may consider replicating this study in a country with lower access to digital services.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgement

This paper is part of a project funded by the Research Council of Norway on digital capabilities at airports, project number 283349. It is an international collaboration between Kristiania University College and Molde University College in Norway, and Cranfield University in the United Kingdom. Avinor who operate 44 airports in Norway is an industry partner to the project.

References

ACI, 2017. Airport Digital Transformation: Best Practice. ACI, Montreal.
ACI Europe, 2018. Guidelines for Passenger Services at Airports: The Passenger at the Heart of the Airport Business. ACI Europe, Brussels.
Al-Jabri, I.M., Eid, M.I., Abed, A., 2020. The willingness to disclose personal information: trade-off between privacy concerns and benefits. Information and Computer Security 28 (2), 161–181. https://doi.org/10.1108/ICS-01-2018-0012.
Altman, D.G., Bland, J.M., 2014. Uncertainty and sampling error. BMJ 349. https://doi.org/10.1136/BMJ.G7064.
Anshari, M., Almunawar, M.N., Lim, S.A., Al-Mudimigh, A., 2019. Customer relationship management and big data enabled: personalization & customization of services. Appl. Comput. Informatics 15 (2), 94–101. https://doi.org/10.1016/J.ACI.2018.05.004.
Becker, T.E., Atinc, G., Breaugh, J.A., Carlson, K.D., Edwards, J.R., Spector, P.E., 2016. Statistical control in correlational studies: 10 essential recommendations for organizational researchers. J. Organ. Behav. 37 (2), 157–167. https://doi.org/10.1002/JOB.2053.
Belanger, F., Crossler, R.E., 2019. Dealing with digital traces: understanding protective behaviors on mobile devices. J. Strateg. Inf. Syst. 28 (1), 34–49. https://doi.org/10.1016/J.JSIS.2018.11.002.
Benitez, J., Henseler, J., Castillo, A., Schuberth, F., 2020. How to perform and report an impactful analysis using partial least squares: guidelines for confirmatory and explanatory IS research. Inf. Manag. 57 (2), 103168 https://doi.org/10.1016/j.im.2019.05.003.
Bergkvist, L., 2015. Appropriate use of single-item measures is here to stay. Mark. Lett. 26 (3), 245–255. https://doi.org/10.1007/s11002-014-9325-y.
Bergkvist, L., 2016. The nature of doubly concrete constructs and how to identify them. J. Bus. Res. 69 (9), 3427–3429. https://doi.org/10.1016/j.jbusres.2016.02.001.
Bokrantz, J., Dul, J., 2022. Building and testing necessity theories in supply chain management. J. Supply Chain Manag. 59 (1), 48–65. https://doi.org/10.1111/JSCM.12287.
Charness, G., Gneezy, U., 2012. Strong evidence for gender differences in risk taking. J. Econ. Behav. Organ. 83 (1), 50–58. https://doi.org/10.1016/J.JEBO.2011.06.007.
Cohen, J., 1988. Statistical Power Analysis for the Behavioral Sciences, 2nd ed. Routledge, New York.
Congress,, 2019. Security and Privacy in Your Car Act of 2019 or the SPY Car Act of 2019. Available at: https://www.congress.gov/bill/116th-congress/senate-bill/2182.
Cottrill, C.D., 2020. MaaS surveillance: privacy considerations in mobility as a service. Transp. Res. A Policy Pract. 131, 50–57. https://doi.org/10.1016/J.TRA.2019.09.026.
Dawson, J.F., Richter, A.W., 2006. Probing three-way interactions in moderated multiple regression: development and application of a slope difference test. J. Appl. Psychol. 91 (4), 917–926. https://doi.org/10.1037/0021-9010.91.4.917.
Dijkstra, T.K., Henseler, J., 2015. Consistent partial least squares path modeling. MIS Quarterly: Management Information Systems 39 (2), 297–316. https://doi.org/10.25300/MISQ/2015/39.2.02.
Dul, J., 2016. Necessary Condition Analysis (NCA): Logic and methodology of "necessary but not sufficient" causality. Organ. Res. Methods 19 (1), 10–52. https://doi.org/10.1177/1094428115584005.
Dul, J., van der Laan, E., Kuik, R., 2020. A statistical significance test for Necessary Condition Analysis. Organ. Res. Methods 23 (2), 385–395. https://doi.org/10.1177/1094428118795272.
Dul, J. (2021). *Necessary Condition Analysis. R Package.* (3.1.1). URL: https://cran.r-project.org/web/packages/NCA/.
Fagnant, D.J., Kockelman, K., 2015. Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. Transp. Res. A Policy Pract. 77, 167–181. https://doi.org/10.1016/J.TRA.2015.04.003.
Fries, R.N., Gahrooei, M.R., Chowdhury, M., Conway, A.J., 2012. Meeting privacy challenges while advancing intelligent transportation systems. Trans. Res. Part C: Emerging Technologies 25, 34–45. https://doi.org/10.1016/j.trc.2012.04.002.
Gerber, N., Gerber, P. & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. In *Computers and Security* (Vol. 77, pp. 226–261). Elsevier Ltd. https://doi.org/10.1016/j.cose.2018.04.002.
Glancy, D., 1995. Privacy and Intelligent Transportation Tech-nology. Santa Clara Computer & High Tech Law Journal 11, 151–203.
Goldfarb, A., Tucker, C., 2012. Shifts in privacy concerns. Am. Econ. Rev. 102 (3), 349–353. https://doi.org/10.1257/aer.102.3.349.
Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., 2022. A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publications, Thousand Oaks, CA.
Halpern, N., Budd, T., Suau-Sanchez, P., Bråthen, S., Mwesiumo, D., 2020. Survey on Airport Digital Maturity and Transformation. Kristiania University College, Oslo.
Halpern, N., Budd, T., Suau-Sanchez, P., Bråthen, S., Mwesiumo, D., 2021a. Conceptualising airport digital maturity and dimensions of technological and organisational transformation. J. Airport Manage. 15 (2), 182–203.
Halpern, N., Mwesiumo, D., Suau-Sanchez, P., Budd, T., Bråthen, S., 2021b. Ready for digital transformation? The effect of organisational readiness, innovation, airport size and ownership on digital change at airports. J. Air Transp. Manag. 90, 101949 https://doi.org/10.1016/j.jairtraman.2020.101949.
Halpern, N., Mwesiumo, D., Budd, T., Suau-Sanchez, P., Bråthen, S., 2021c. Segmentation of passenger preferences for using digital technologies at airports in Norway. J. Air Transp. Manag. 91, 102005 https://doi.org/10.1016/J.JAIRTRAMAN.2020.102005.
He, B.Y., Chow, J.Y.J., 2020. Optimal privacy control for transport network data sharing. Trans. Res. Part C: Emerging Technologies 113, 370–387. https://doi.org/10.1016/j.trc.2019.07.010.
Henseler, J., Hubona, G., Ray, P.A., 2016. Using PLS path modeling in new technology research: updated guidelines. Ind. Manag. Data Syst. 116 (1), 2–20. https://doi.org/10.1108/IMDS-09-2015-0382.
Hong, W. & Thong, J.Y.L. 2013. Internet privacy concerns: An integrated conceptualization and four empirical studies. In *MIS Quarterly* (Vol. 37, pp. 275–298). Management Information Systems Research Center, University of Minnesota. https://doi.org/10.2307/43825946.
Huang, S., 2022. Listening to users' personal privacy concerns. The implication of trust and privacy concerns on the user's adoption of a MaaS-pilot. Case Studies on. Transp. Policy 10 (4), 2153–2164. https://doi.org/10.1016/j.cstp.2022.09.012.
IATA, 2018. Global Passenger Survey. IATA, Montreal.
Ioannou, A., Tussyadiah, I., Lu, Y., 2020a. Privacy concerns and disclosure of biometric and behavioral data for travel. Int. J. Inf. Manag. 54, 102122 https://doi.org/10.1016/j.ijinfomgt.2020.102122.
Ioannou, A., Tussyadiah, I., Miller, G., 2020b. That's private! Understanding travelers' privacy concerns and online data disclosure. J. Travel Res. 60 (7), 1510–1526. https://doi.org/10.1177/0047287520951642.

Iso-Ahola, S.E., 2020. Replication and the establishment of scientific truth. Front. Psychol. 2183. https://doi.org/10.3389/FPSYG.2020.02183.
Jozani, M., Ayaburi, E., Ko, M., Choo, K.K.R., 2020. Privacy concerns and benefits of engagement with social media-enabled apps: a privacy calculus perspective. Comput. Hum. Behav. 107, 106260 https://doi.org/10.1016/j.chb.2020.106260.
Kasim, K.O., Winter, S.R., Liu, D., Keebler, J.R., Spence, T.B., 2021. Passengers' perceptions on the use of biometrics at airports: a statistical model of the extended theory of planned behavior. Technol. Soc. 67, 101806 https://doi.org/10.1016/j.techsoc.2021.101806.
Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Inf. Syst. J. 25 (6), 607–635. https://doi.org/10.1111/ISJ.12062.
Kemp, S. (2022). Digital 2022: Norway. Available at: https://datareportal.com/reports/digital-2022-norway (Last acceessed on 14.01.2023).
Kenny, D. A. (2018). Moderation. URL: http://davidakenny.net/cm/moderation.htm.
Khan, N., Efthymiou, M., 2021. The use of biometric technology at airports: the case of customs and border protections. Int. J. Information Manage. Data Insights 1 (2), 100049. https://doi.org/10.1016/j.jjimei.2021.100049.
Kim, D., Park, K., Park, Y., Ahn, J.H., 2019. Willingness to provide personal information: perspective of privacy calculus in IoT services. Comput. Hum. Behav. 92, 273–281. https://doi.org/10.1016/J.CHB.2018.11.022.
Kock, N., Hadaya, P., 2018. Minimum sample size estimation in PLS-SEM: the inverse square root and gamma-exponential methods. Inf. Syst. J. 28 (1), 227–261. https://doi.org/10.1111/ISJ.12131.
Li, Y., 2014. The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. Decis. Support Syst. 57 (1), 343–354. https://doi.org/10.1016/j.dss.2013.09.018.
Li, L., Lee, K.Y., Chang, Y., Yang, S., Park, P., 2021. IT-enabled sustainable development in electric scooter sharing platforms: focusing on the privacy concerns for traceable information. Inf. Technol. Dev. 27 (4), 736–759. https://doi.org/10.1080/02681102.2021.1882366.
Line, N.D., Dogru, T., El-Manstrly, D., Buoye, A., Malthouse, E., Kandampully, J., 2020. Control, use and ownership of big data: a reciprocal view of customer big data value in the hospitality and tourism industry. Tour. Manag. 80, 104106 https://doi.org/10.1016/J.TOURMAN.2020.104106.
Lowry, P.B., D'Arcy, J., Hammer, B., Moody, G.D., 2016. "Cargo Cult" science in traditional organization and information systems survey research: a case for using nontraditional methods of data collection, including Mechanical Turk and online panels. J. Strateg. Inf. Syst. 25 (3), 232–240. https://doi.org/10.1016/J.JSIS.2016.06.002.
Lutz, C., Newlands, G., 2021. Privacy and smart speakers: a multi-dimensional approach. Information Society 37 (3), 147–162. https://doi.org/10.1080/01972243.2021.1897914.
Mandhani, J., Nayak, J.K., Parida, M., 2020. Interrelationships among service quality factors of Metro Rail Transit System: an integrated Bayesian networks and PLS-SEM approach. Transp. Res. A Policy Pract. 140, 320–336. https://doi.org/10.1016/J.TRA.2020.08.014.
McCarthy, O.T., Caulfield, B., ÓMahony, M., 2016. Technology engagement and privacy: a cluster analysis of reported social network use among transport survey respondents. Trans. Res. Part C: Emerging Technol. 62, 195–206.
Meehan, M., 2019. Data Privacy Will Be The Most Important Issue In The Next Decade. Forbes. https://www.forbes.com/sites/marymeehan/2019/11/26/data-privacy-will-be-the-most-important-issue-in-the-next-decade/#3694c28f1882.
Morosan, C., 2018. Information disclosure to biometric e-gates: The roles of perceived security, benefits, and emotions. J. Travel Res. 57 (5), 644–657. https://doi.org/10.1177/0047287517711256.
Mwesiumo, D., Halpern, N., Budd, T., Suau-Sanchez, P., Bråthen, S., 2021. An exploratory and confirmatory composite analysis of a scale for measuring privacy concerns. J. Bus. Res. 136, 63–75. https://doi.org/10.1016/J.JBUSRES.2021.07.027.
Oghazi, P., Schultheiss, R., Chirumalla, K., Kalmer, N.P., Rad, F.F., 2020. User self-disclosure on social network sites: a cross-cultural study on Facebook's privacy concepts. J. Bus. Res. 112, 531–540. https://doi.org/10.1016/j.jbusres.2019.12.006.
Patil, S., Patruni, B., Potoglou, D., Robinson, N., 2016. Public preference for data privacy – A pan-European study on metro/train surveillance. Transp. Res. A Policy Pract. 92 (October), 145–161. https://doi.org/10.1016/J.TRA.2016.08.004.
Richter, N.F., Cepeda, G., Roldán, J.L., Ringle, C.M., 2016. European management research using partial least squares structural equation modeling (PLS-SEM). Eur. Manag. J. 34 (6), 589–597. https://doi.org/10.1016/j.emj.2016.08.001.
Richter, N.F., Schubring, S., Hauff, S., Ringle, C.M., Sarstedt, M., 2020. When predictors of outcomes are necessary: guidelines for the combined use of PLS-SEM and NCA. Ind. Manag. Data Syst. 120 (12), 2243–2267. https://doi.org/10.1108/IMDS-11-2019-0638/FULL/PDF.
Rodríguez-Priego, N., Porcu, L., Kitchen, P.J., 2022. Sharing but caring: Location based mobile applications (LBMA) and privacy protection motivation. J. Bus. Res. 140, 546–555. https://doi.org/10.1016/j.jbusres.2021.11.022.
Serrano, F., Kazda, A., 2020. The future of airports post COVID-19. J. Air Transp. Manag. 89, 101900 https://doi.org/10.1016/j.jairtraman.2020.101900.
Shore, A., 2022. Talking about facial recognition technology: How framing and context influence privacy concerns and support for prohibitive policy. Telematics Inform. 70, 101815 https://doi.org/10.1016/j.tele.2022.101815.
SITA, 2021. Air Transport IT Insights. SITA, Brussels.
Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: An interdisciplinary review. In: MIS Quarterly: Management Information Systems, Vol. 35(4. Management Information Systems Research Center, University of Minnesota, pp. 989–1015. https://doi.org/10.2307/41409970.
Sukhov, A., Olsson, L.E., Friman, M., 2022. Necessary and sufficient conditions for attractive public Transport: Combined use of PLS-SEM and NCA. Transp. Res. A Policy Pract. 158, 239–250. https://doi.org/10.1016/J.TRA.2022.03.012.
Taeihagh, A., Lim, H.S.M., 2019. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transp. Rev. 39 (1), 103–128. https://doi.org/10.1080/01441647.2018.1494640.
The Government of South Korea (2017). Motor vehicle management act. Act No. 14546, Jan. 17, 2017. Available at: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42015&lang=ENG.
Tran, C.D., Nguyen, T.T., 2021. Health vs. privacy? The risk-risk tradeoff in using COVID-19 contact-tracing apps. Technol. Soc. 67, 101755 https://doi.org/10.1016/J.TECHSOC.2021.101755.
Trepte, S., Reinecke, L., Ellison, N.B., Quiring, O., Yao, M.Z. & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus: *Social Media + Society*, 3(1). https://doi.org/10.1177/2056305116688035.
Trepte, S., Scharkow, M., Dienlin, T., 2020. The privacy calculus contextualized: The influence of affordances. Computers in Human Behavior 104, 106115. https://doi.org/10.1016/J.CHB.2019.08.022.
Uncles, M.D., Kwok, S., 2013. Designing research with in-built differentiated replication. J. Bus. Res. 66 (9), 1398–1405. https://doi.org/10.1016/j.jbusres.2012.05.005.
Unctad, 2021. Data protection and privacy legislation worldwide. Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
Véliz, C., 2021. Privacy and digital ethics after the pandemic. Nat. Electron. 4 (1), 10–11. https://doi.org/10.1038/s41928-020-00536-y.
Wang, T., Duong, T.D., Chen, C.C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. Int. J. Inf. Manag. 36 (4), 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003.
Xie, Z., Page, L., Hardy, B., 2017. Investigating gender differences under time pressure in financial risk taking. Front. Behav. Neurosci. 246. https://doi.org/10.3389/FNBEH.2017.00246.
Yeh, C.H., Wang, Y.S., Lin, S.J., Tseng, T.H., Lin, H.H., Shih, Y.W., Lai, Y.H., 2018. What drives internet users' willingness to provide personal information? Online Inf. Rev. 42 (6), 923–939. https://doi.org/10.1108/OIR-09-2016-0264.

Zhang, C., Liu, Y., Lu, W., Xiao, G., 2019. Evaluating passenger satisfaction index based on PLS-SEM model: Evidence from Chinese public transport service. Transp. Res. A Policy Pract. 120, 149–164. https://doi.org/10.1016/J.TRA.2018.12.013.

Zhang, M., Zhao, P., Qiao, S., 2020. Smartness-induced transport inequality: Privacy concern, lacking knowledge of smartphone use and unequal access to transport information. Transp. Policy 99, 175–185. https://doi.org/10.1016/j.tranpol.2020.08.016.

Zlatolas, L.N., Welzer, T., Heričko, M., Hölbl, M., 2015. Privacy antecedents for SNS self-disclosure: The case of Facebook. Comput. Hum. Behav. 45, 158–167. https://doi.org/10.1016/j.chb.2014.12.012.

https://dspace.org/

Perceived benefits as a driver and necessary condition for the willingness of air passengers to provide personal data for non-mandatory digital services at airports

Mwesiumo, Deodat; Halpern, Nigel; Bråthen, Svein; Budd, Thomas; Suau-Sanchez, Pere

2023-05-01
Elsevier
https://doi.org/10.1016/j.tra.2023.103659
Mwesiumo D, Halpern N, Bråthen S, et al., (2023) Perceived benefits as a driver and necessary condition for the willingness of air passengers to provide personal data for non-mandatory digital services at airports. Transportation Research Part A: Policy and Practice, Volume 171, May 2023, Article number 103659

Downloaded from a DSpace repository. https://dspace.org/