Journal of Business Research 136 (2021) 63–75

Contents lists available at ScienceDirect

Journal of Business Research

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

An exploratory and confirmatory composite analysis of a scale for measuring privacy concerns

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

[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, Av. Tibidabo, 39-43, 08035 Barcelona, Spain

ARTICLE INFO

Keywords:
Privacy concerns scale
Confirmatory composite analysis
Partial least squares path modelling
Airport management
Online retail

ABSTRACT

This paper reports a confirmatory composite analysis of a scale for measuring privacy concerns, and the effect of privacy concerns on the willingness to provide personal data. The analysis is based on 468 survey responses, divided into two contexts: airport digital services and online retail services. Results from both contexts confirm that privacy concerns consist of a third-order construct comprising two-second order constructs (interaction management and information management) and a first-order construct (awareness). The effect of privacy concerns on the willingness to provide personal data is higher in the airport digital context than in the online retail context. Also, the relevance of the three dimensions varies by context. Thus, researchers must carefully consider their research context and include items for the most relevant dimensions of privacy concerns in measurement models. Likewise, managers must prioritise dimensions of privacy concerns according to their business context.

1. Introduction

Digital services provide opportunities to enhance customer experiences by offering more convenience and greater levels of personalisation. However, the collection of customer data to enable such services has led to increased concerns regarding privacy. Indeed, privacy concerns resulting from the proliferation of digital services have become one of the critical social-cultural issues of our time, and the implications of this from a consumer behaviour perspective have been noted by previous studies. For instance, Miltgen et al. (2016) found that privacy concerns reduce consumers' intention to accept innovations in information technology, while Jozani et al. (2020) found that privacy concerns result in reduced user engagement with social media-enabled applications. Oghazi et al. (2020) argue that as awareness regarding privacy issues increases, customer concerns also rise, and may subsequently result in a greater unwillingness to disclose personal information. Wieringa et al. (2019) note that although data is considered the new oil of the economy, privacy concerns among consumers limit its full potential. Since privacy concerns affect consumer behaviour, businesses must take appropriate measures (Krishen et al., 2017).

As one of the most critical issues in this new decade (Meehan, 2019), privacy concerns will continue to be an essential construct in research across disciplines, providing a basis for the formulation and testing of its probabilistic relations with other theoretical constructs. The validity of evidence obtained from such research will partly depend on the effective operationalisation of privacy concerns into specific, concrete and measurable indicators. Given its importance, there have been several attempts to develop and test scales for the measurement of privacy concerns in different contexts. Although existing studies provide valuable insights, there have been mixed findings. For instance, while some studies have identified privacy concerns as a second-order factor (e.g. Smith et al., 1996; Malhotra et al., 2004), Buchanan et al. (2007) found only one dimension, and Hong and Thong (2013) identified it as a third-order factor.

The inconsistent findings of previous studies warrant further research to guide an effective and efficient measurement of privacy concerns in future studies, and this study contributes in three ways. Firstly, it conducts a differentiated replication of Hong and Thong (2013), which among all previous studies, identifies the largest number of privacy concerns dimensions and is the only one to identify privacy concerns as a third-order factor. By replicating Hong and Thong (2013), this study can also explore the validity of second-order and single-factor modelling if third-order modelling turns out to be invalid. Hence, the study responds to the call for a paradigm shift in business research from

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

https://doi.org/10.1016/j.jbusres.2021.07.027
Received 10 February 2021; Received in revised form 7 July 2021; Accepted 10 July 2021
Available online 23 July 2021

testing for significant differences to testing for significant sameness (Hubbard and Lindsay, 2013). Based on Uncles and Kwok (2013), this study is a differentiated replication because it maintains the conceptual framework used in Hong and Thong (2013) while deliberately changing the methodological approach and context of the study. Thus, like Hong and Thong (2013), six dimensions of privacy concerns are explored and confirmed. Unlike Hong and Thong (2013), a recently developed method, confirmatory composite analysis (CCA) (Hair et al., 2020), is applied to analyse data from 468 respondents in Norway, representing two different contexts: airport digital services and online business-to-consumer (B2C) retail services. As such, this study provides reliable indicators that future research related to privacy concerns can use. Secondly, since CCA requires an assessment of the relationship between the focal construct and a potential antecedent and outcome variable, this study tests the relationship between privacy invasion experience, privacy concerns and willingness to provide data. The results of the tests contribute actionable insights for managers of airport and retail services. Thirdly, since this is among the first studies to apply CCA, it is hoped that it will serve as an essential reference for future studies that intend to confirm other measurement scales. The advantages of conducting CCA, as opposed to traditional factor analysis include: (1) the possibility to retain a higher number of items used to measure the construct, thus improving content coverage and construct validity; (2) the availability of determinant construct scores; (3) the possibility to apply to formative measurement models (Hair et al., 2020). More so, Benitez et al. (2020) report the growing application of PLS-SEM in various fields of business research, thus the choice of conducting CCA using PLS-SEM seems justifiable.

2. Literature and conceptual framework

2.1. Privacy and privacy concerns

Although the concept of privacy and the right to privacy have long been acknowledged (Moor, 1990), there remains no agreed definition. Different disciplines such as management information systems, philosophy, political science, law, psychology, marketing, and economics, define privacy differently. Thus, privacy appears to be a context-dependent, multi-dimensional and dynamic construct that evolves with technological advancements (Jozani et al., 2020). Smith et al. (2011) examine different approaches that have been used to define privacy in various disciplines and broadly classify privacy definitions as being either value-based or cognate-based. The value-based perspective views privacy as a human right integral to society's moral value system. In contrast, the cognate-based perspective views privacy as a construct related to the individual's mind, perceptions, and cognition rather than an absolute moral value/norm.

Given its focus, this study embraces a definition of privacy that has been widely adopted in the context of digital technologies. It refers to privacy as an individual's ability to control when, how, and to what extent their personal information is used (Bélanger and Crossler, 2011; Hong and Thong, 2013; Ioannou et al., 2020). This definition is consistent with the European Union's General Data Protection Regulation (GDPR) that views data privacy as people's ability to control how their data is used and who has access to it. According to GDPR Article 4, personal data refers to 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. The idea that privacy is not simply an absence of information about us in the minds of others, and that privacy is the control we have over information about ourselves, is not new (e.g., see Fried, 1968).

One aspect related to privacy that has attracted significant scholarly attention is individuals' privacy concerns. It refers to individuals' perceptions of how service providers handle personal data, contrary to their expectations of how they should do it (Hong and Thong, 2013). Such perceptions are subsequently related to attitudes and behaviours towards providing personal data to service providers. For instance, Morosan (2018) finds that privacy concerns had a significant adverse effect on travellers' willingness to disclose biometric information at airports. Interestingly, Goldfarb and Tucker (2012) found that refusals to disclose personal data has tended to rise over time, and that older people are less likely to disclose personal data than younger people. They argue that these observations are possibly related to increased experience with information technology (and a greater awareness of potential privacy concerns), as well as a changing online population. They also observed an increase in the number of contexts in which consumers perceive privacy concerns to be relevant.

2.2. Measuring privacy concerns

Privacy concerns constitute a central construct in studies related to privacy, and it has been measured in various ways. Considering the various conceptions attached to privacy, Smith et al. (2011) observe that measuring privacy itself is near impossible. Therefore, it is reasonable to conclude that the different approaches are partly due to the various meanings attached to the concept of privacy. In other words, since privacy is context-dependent, the measurement of it will also depend on the context.

Several studies have attempted to develop a scale for measuring privacy concerns (Table 1). Most of them use multiple dimensions, meaning that they view it as a single theoretical concept comprised of two or more distinct but related dimensions. Examples of dimensions include: (1) how personal information is collected; (2) errors in personal data; (3) unauthorised secondary use of personal data; (4) improper access of personal data by unauthorised people; (5) awareness of privacy practices; (6) control of personal data.

The number of dimensions identified varies by study. For instance, Smith et al. (1996) identify four dimensions, while Malhotra et al. (2004) identify three. Intriguingly, Buchanan et al. (2007) found only one dimension despite including indicators related to various dimensions. Besides, while studies that view privacy concerns as a multi-dimensional construct mostly identify it as a second-order construct (where privacy concerns comprise sub-constructs that are measured by observable indicators), Hong and Thong (2013) identify it as a third-order construct (that comprises second-order constructs that are further composed of sub-constructs measured by observable indicators). Since Hong and Thong (2013) is the latest study to develop a privacy concerns scale, and the only one to identify it as a third-order construct, the approach taken in this study is to conduct a differentiated replication of it.

Importantly, multi-dimensional constructs provide holistic representations of complex phenomena and allow researchers to match broad predictors with broad outcomes (Edwards, 2001). Considering that privacy concerns are based on a complex concept of privacy (Smith et al., 2011), there is a strong case that privacy concerns should always be measured using a multi-dimensional scale. As Polites et al. (2012) suggest, it is critical to properly conceptualise and identify constructs' dimensions because analytical results will be influenced by how a measurement model is operationalised.

Against this backdrop, conducting a confirmatory analysis is justifiable. Previous studies have exclusively established scales for privacy concerns by confirming theoretical structures, particularly measurement models using confirmatory factor analysis (CFA). This process is both qualitative and statistical (Hair et al., 2020). It involves examining the reliability of the individual indicators, construct reliability, face and content validity, convergent and discriminant validity, and Goodness of Fit. The process allows researchers to evaluate multi-item constructs based on common variance, and it is part of covariance-based structural equation modelling (CB-SEM). Unlike the extant studies, this study applies CCA, a recently proposed process for confirming PLS-SEM measurement models. Like CFA, CCA aims to establish a measurement

Table 1
Examples of measurements of privacy concerns.

Authors	Context	Measurement approach
Smith et al. (1996); Stewart and Segars (2002)	Individuals' concerns about organisational information privacy practices	Privacy concern as a second-order factor consisting of 4 first-order factors measured by 15 indicators *The first order factors* • Collection of personal information (four items) • Errors in personal data (four items) • Unauthorised secondary use of personal data (four items) • Improper access to personal data by unauthorised people (three items)
Malhotra et al. (2004)	Internet users' concerns about the privacy of their information	Privacy concern as a second-order factor consisting of 3 first-order factors measured by10 indicators *The first order factors* • Control (three items) • Awareness of privacy practices (three items) • Collection of personal information (four items)
Buchanan et al. (2007)	Internet users' concerns about the privacy of their information	Privacy concern as a first-order factor measured by 16 indicators *Examples of items* • In general, how concerned are you about your privacy while you are using the internet? • Are you concerned about online organisations not being who they claim they are? • Are you concerned that you are asked for too much personal information when you register or make online purchases? • Are you concerned about online identity theft?
Hong and Thong (2013)	Internet users' concerns about the privacy of their information	Privacy concern as a third-order factor consisting of 2 second-order factors and 6 first-order factors. *Second-order factors* • Interaction management • Information management *First-order factors* • Collection • Secondary usage • Errors • Improper access • Control • Awareness

theory. It also begins by presenting theoretical constructs and proceeds to structural modelling after confirming the measurement models. However, there are essential distinctions between CFA and CCA (Hair et al., 2020). CFA is based on common variance only, while CCA is based on total variance. Also, while CFA is confirmatory only, CCA is both exploratory and confirmatory.

2.3. Nomological network

Conducting CCA requires testing a nomological network of the focal variable. It involves formulating a conceptual framework that links the focal construct to its potential antecedent and outcome variables. The framework should be supported with results of previous research (Hair et al., 2020). The nomological network for this study was developed by linking the focal variable (privacy concerns) with previous exposure to privacy invasion (as an antecedent factor) and willingness to provide personal data (as a potential outcome) (Fig. 1).

As shown in Fig. 1, privacy invasion experience leads to increased privacy concerns. The argument for this assertion is that privacy invasion provides knowledge that helps improve the ability to perceive threats in a particular situation and accurately evaluate factors in the environment that might incur a loss of privacy (Masur, 2019). The significance of the positive relationship between privacy invasion experience and privacy concerns is supported by extant empirical research (e.g. Yeh et al., 2018; Ioannou et al., 2020). As for the outcome variable, the framework shows that privacy concerns negatively affect the willingness to provide personal data. The argument is that customers who are concerned about their privacy tend to protect themselves against exposure, among other things, by refraining from sharing personal data with service providers. The negative association between privacy concerns and overall willingness to provide personal data is supported by empirical studies such as Zlatolas et al. (2015) and Morosan (2018).

3. Methodology

3.1. Context and key constructs

The two contexts, digital services at airports and online retail services were used as a basis for the analysis. The goal was to explore the relevance of privacy concerns dimensions in different contexts. For each context, respondents were asked to consider personal data requested for additional digital services versus those that are mandatory. In the case of airports, this might include receiving notifications about the 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; joining and receiving information from a loyalty programme; and making payments for products and services online or via a mobile application. For retail, it might include receiving information on related products and services; tracking a delivery; accessing customer services; joining and receiving information from a loyalty programme; and storing personal and/or payment details for future purchases.

A survey for each context was used to capture the nomological network variables: privacy invasion experience, privacy concerns, and general willingness to provide personal data. Indicators for the three constructs were adopted from previous studies and modified to suit the two contexts: airports and retail. Following Mwesiumo and Halpern (2018), all indicators were measured on a 7-point Likert scale ranging from "strongly disagree" (1) to "strongly agree" (7) apart from the indicator measuring willingness to provide personal data (WD), which was on a scale ranging from "very unwilling" (1) to "very willing" (7). Privacy concerns (PC) was operationalised as the extent to which an individual is worried about various aspects related to privacy. We adopted an exhaustive list of privacy concerns dimensions in the extant literature, as identified by Hong and Thong (2013). The dimensions are data

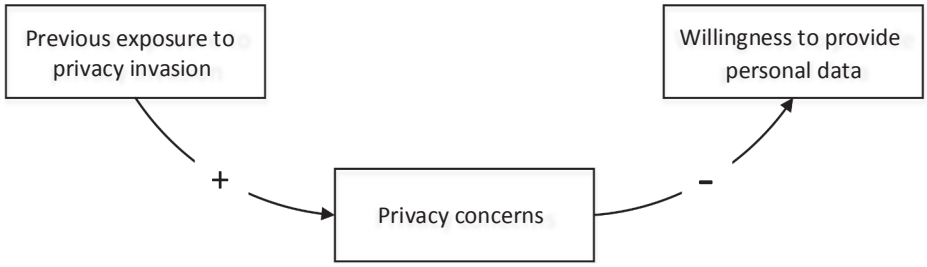

Fig. 1. Nomological network for privacy concerns.

Table 2
Constructs and items.

Constructs	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
Privacy invasion experience (PE)	
	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
Willingness to provide personal data (WD)	
	In general, I would be willing to provide personal data for additional [digital services at airports] [online services with retailers]

collection (CO), secondary usage (SU), errors (ER), improper access (IA), control (CR), and awareness (AW). In addition to Hong and Thong (2013), the phrasing of the indicators was also informed by other studies (e.g. Smith et al., 1996; Malhotra et al., 2004; Ioannou et al., 2020). Privacy invasion experience (PE) was operationalised as the extent to which a respondent perceives their privacy was previously intruded. Its measures are based on Li (2014) and Ioannou et al. (2020). Willingness to provide personal data (WD) was measured using a generalised statement based on Morosan (2018). Since willingness to provide personal data is a concrete attribute, measuring it by a single item is justifiable (Bergkvist, 2016). Each construct (and dimension in the case of PC) and the items used in the survey to create them can be seen in Table 2.

3.2. Data collection

Data were collected using an online panel (see Fan et al., 2020; Kharouf et al., 2020 for recent studies that have also used this approach). Online panels provide fast and convenient access to a large pool of respondents at a relatively low cost (Smith et al., 2016), and can be crowdsourced or commercially maintained. In their analysis that compared data quality between crowdsourced and commercially maintained panels, Smith et al. (2016) conclude that a commercial panel results in better quality data, most likely due to the vendor's strict quality measures. Consequently, data for this study were collected from a commercially maintained panel, which was provided by Qualtrics. Qualtrics was also used as the online survey tool for this study.

Two separate surveys were developed, one for each context. The surveys began with questions used to screen respondents according to three criteria. For the airport context, respondents had to have taken at least one return flight during the last 24 months (24 months was used instead of 12 months because of reduced travel during the coronavirus pandemic in the 12 months prior to conducting the survey). For the retail context, respondents had to have purchased something from an online retailer during the last 12 months. For both contexts, respondents had to be at least 18 years old and resident in Norway.

Representative quotas for Norway were then set according to age (18–24, 25–34, 35–44, 45–54, 55–64, 65+) and gender (male, female, non-binary or other). Text about each context (as explained in Section 3.1) and questions containing the items listed in Table 2 were then included with wording modified according to each context. The surveys were initially written in English and translated to Norwegian. In addition to the authors, five Norwegians took part in a pre-test of each of the surveys. Each survey was then piloted with 50-panel respondents before being approved for distribution. Data collection took place towards the end of 2020. Any responses completed faster than 25% trimmed mean

Table 3
Respondent characteristics.

		Airport context (n = 235)		Retail context (n = 233)	
Variable	Response	N	%	N	%
Gender[a]	Male	119	50.6	116	49.8
	Female	116	49.4	117	50.2
Age	18–24	11	4.7	17	7.3
	25–34	30	12.8	26	11.2
	35–44	41	17.4	38	16.3
	45–54	60	25.5	49	21.0
	55–64	54	23.0	56	24.0
	65+	39	16.6	47	20.2

[a] No respondents selected the non-binary or other option.

completion time were excluded from the analysis to account for respondents who had deliberately rushed or completed the survey too quickly. We chose to use the 25% trimmed mean because it is equivalent to the interquartile mean, a measure of central tendency that shares some properties of both the mean and the median. This ensured that rushed responses were eliminated based on a robust measure of average completion time. Several more lenient thresholds were considered (5%, 10% and 20%), and while they did improve the percentage of variation in the target dependent variable, the direction and significance of the estimated coefficients remained unchanged, so the more robust threshold of 25% was used. The final sample size consisted of 468 observations (235 for the airport context and 233 for the retail context) (Table 3). The number of observations in each context is well above the sample size recommended for a statistical power of 80% in PLS-SEM (Hair et al., 2017).

3.3. Data analysis

This study uses a CCA procedure for reflective measurement models proposed by Hair et al. (2020). The procedure consists of seven steps: (1) estimate loadings and significance; (2) check indicator reliability; (3) check composite reliability of the construct; (4) check convergence validity; (5) check discriminant validity; (6) check nomological validity of the construct; (7) check predictive or concurrent validity of the construct. The first five steps help assess the quality of the measurement model. The last two steps are concerned with the relevance of the structural model. Following Mwesiumo et al. (2019), the steps were carried out using PLS-SEM software SmartPLS 3.

Like Hong and Thong (2013), we modelled privacy concerns as a third-order construct consisting of three dimensions: interaction management (INTM), information management (INFM) and awareness (AW). Further, INTM consists of three first-order constructs: collection (CO), secondary usage (SU) and control (CR), while INFM consists of two first-order constructs: improper access (IA) and errors (ER). Structurally, privacy concerns and its lower-order constructs were conceptualised as a reflective-reflective hierarchical component model. This is appropriate because our goal is to determine the common factor of several related but distinct reflective lower-order constructs (Sarstedt et al., 2019). We applied the repeated indicators approach whereby all lower-order constructs' items are assigned to the higher-order constructs' measurement model. Thus, the items are used to generate primary loadings (for the lower order constructs) and secondary loadings (for the higher-order constructs). We implemented the PLS algorithm and then, following Hair et al. (2017), we executed a bootstrapping procedure with 5000 runs. Results of the analysis for the two contexts are presented in Sections 4 and 5.

4. Results from the airport context (Context A)

In this context, CCA is conducted on the data collected from 235 respondents. Fig. 2 presents the estimated nomological network and its path coefficients. The results of the seven CCA steps follow.

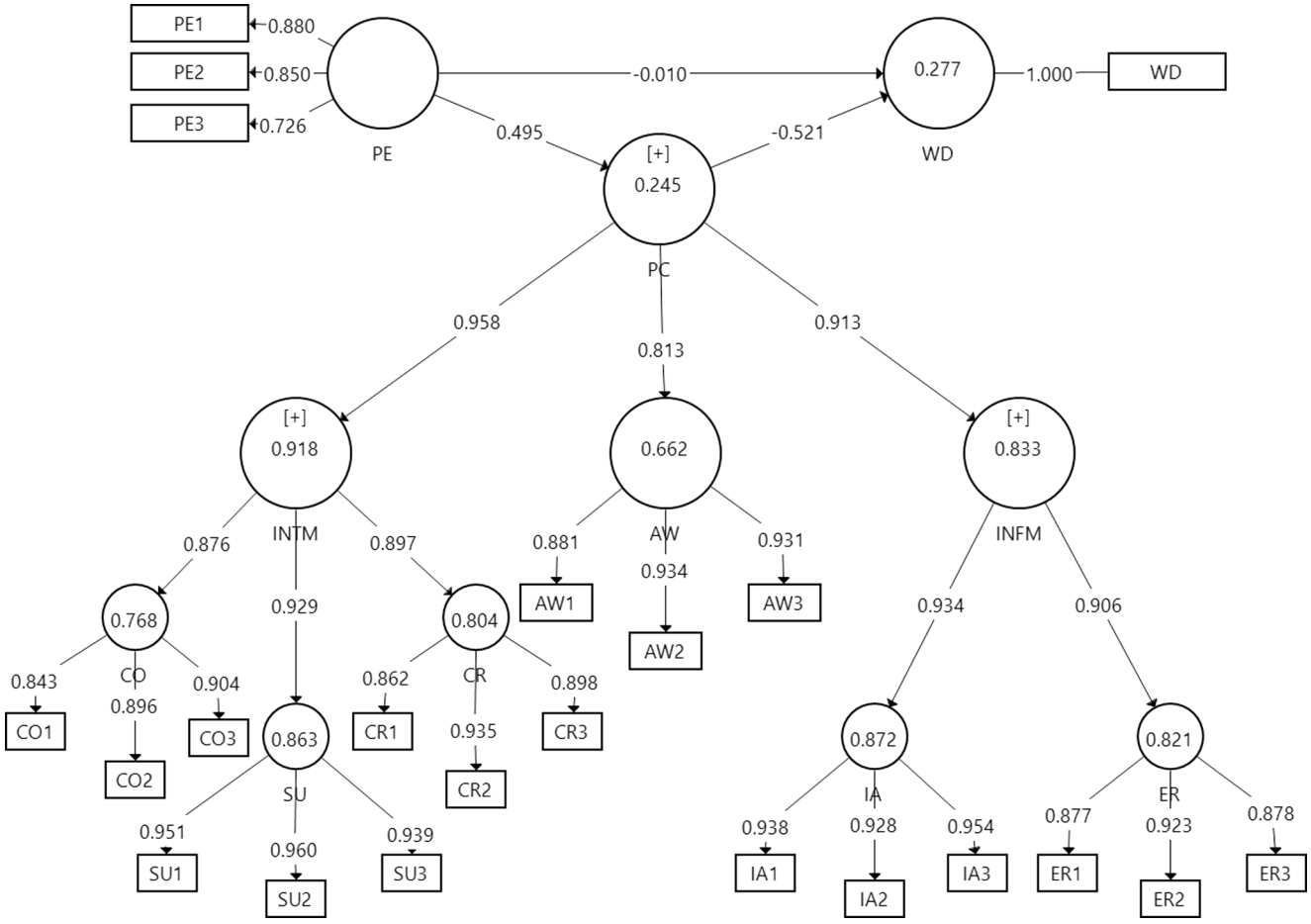

Fig. 2. The estimated nomological network – Context A.

Table 4
Results of the measurement model assessment – Airport context.

Indicator	Loading (IR)[1]	Confidence interval[2]	t-statistic	Rho_A	AVE
Collection (CO)					
CO1	0.843 (0.702)	0.767–0.887	27.396***	0.869	0.777
CO2	0.896 (0.801)	0.855–0.924	50.963***		
CO3	0.904 (0.826)	0.885–0.927	87.269***		
Secondary usage (SU)					
SU1	0.951 (0.904)	0.924–0.967	86.754***	0.947	0.903
SU2	0.960 (0.922)	0.942–0.974	118.992***		
SU3	0.939 (0.882)	0.907–0.961	69.381***		
Errors (ER)					
ER1	0.877 (0.762)	0.821–0.909	38.767***	0.874	0.797
ER2	0.923 (0.852)	0.886–0.947	60.567***		
ER3	0.878 (0.771)	0.829–0.913	42.569***		
Improper access (IA)					
IA1	0.938 (0.880)	0.914–0.958	85.539***	0.934	0.884
IA2	0.928 (0.861)	0.890–0.951	59.091***		
IA3	0.954 (0.910)	0.935–0.970	109.905***		
Control (CR)					
CR1	0.862 (0.743)	0.810–0.906	35.554***	0.890	0.808
CR2	0.935 (0.874)	0.912–0.952	90.768***		
CR3	0.898 (0.806)	0.850–0.927	47.63***		
Awareness (AW)					
AW1	0.881 (0.776)	0.820–0.925	33.323***	0.907	0.839
AW2	0.934 (0.872)	0.903–0.955	71.517***		
AW3	0.931 (0.867)	0.883–0.958	51.962***		
Privacy invasion experience (PE)					
PE1	0.880 (0.774)	0.834–0.921	40.019***	0.880	0.674
PE2	0.850 (0.723)	0.773–0.895	27.828***		
PE3	0.726 (0.527)	0.572–0.816	11.567***		
Information management (INFM)					
IA	0.934 (0.872)	0.915–0.950	106.769***	0.922	0.712
ER	0.906 (0.820)	0.780–0.886	31.379***		
Interaction management (INTM)					
CO	0.876 (0.767)	0.825–0.908	41.864***	0.943	0.674
SU	0.929 (0.863)	0.885–0.952	56.989***		
CR	0.897 (0.804)	0.862–0.924	57.745***		
Privacy concerns (PC)					
INFM	0.913 (0.833)	0.935–0.966	121.463***	0.963	0.600
AW	0.813 (0.660)	0.749–0.870	26.860***		
INTM	0.958 (0.918)	0.939–0.970	126.556***		
Willingness to provide personal data (WD)					
WD	1.000 (1.000)	NA^	NA^	1.000	1.000

[1] Indicator reliability; [2] Bias corrected; *** Significant at $p < 0.001$; ^ Not applicable: single item.

4.1. Step 1 and 2: Estimate loadings and check indicator reliability

According to Hair et al. (2020), the value of standardised loadings should be at least 0.708 with an associated t-statistic of above ±1.96, for a two-tailed test at the 5% level. They also recommend checking the 95% confidence intervals (bias-corrected) of the indicator loadings. As shown in Table 4, all indicator loadings were above the recommended threshold and significant at $p < 0.01$. The significance of the loadings is also confirmed by the corresponding 95% confidence intervals (bias-corrected). Indicator reliability is obtained by squaring a related loading. The loading values and their squared values (presented in brackets) suggest that all indicators are adequately reliable (Benitez et al., 2020).

4.2. Step 3 and 4: Check composite reliability and convergence validity

Composite reliability was used to test the internal consistency of the constructs, as recommended by Hair et al. (2020). For this approach, Benitez et al. (2020) emphasize using a novel and effective measure, Dijkstra–Henseler's ρA (rho_A), with a threshold of $\rho A > 0.7$. Hair et al. (2020) note that if reliability is 0.95 or higher, then individual items constituting a construct are redundant, meaning that they measure the same concept.

As shown in Table 4, all rho_A values are well above the recommended threshold. However, the rho_A value for privacy concerns is above 0.95, suggesting that at least one of the three dimensions constituting it is redundant. Convergent validity is checked by evaluating the value of the average variance extracted (AVE) with the recommended threshold being AVE > 0.5. Convergence validity for all constructs is established as the observed AVE values are above 0.5.

4.3. Step 5: Check discriminant validity

Discriminant validity is the extent to which a construct is distinct from other constructs in the conceptual model (Hair et al., 2017). Hair et al. (2020) and Benitez et al. (2020) recommend determining discriminant validity using the heterotrait-monotrait ratio of correlations (HTMT). The recommended thresholds are less than 0.90 for conceptually similar constructs, and less than 0.85 for constructs that are not conceptually similar. The results in Table 5 show that all HTMT values are below the recommended thresholds, confirming that each of the identified constructs is distinct from the others. Therefore, consistent with Hong and Thong (2013), our results support modelling privacy concerns as a third-order construct consisting of two second-order constructs (information management and interaction management) and one first-order construct (awareness).

Table 5
HTMT values for the constructs – Airport context.

	AW	CO	CR	ER	IA	INFM	INTM	PE	SU	PC
CO	0.624									
CR	0.751	0.762								
ER	0.555	0.536	0.748							
IA	0.765	0.697	0.898	0.768						
INFM	0.716	0.706	0.891	NA	NA					
INTM	0.762	NA	NA	0.704	0.86	0.884				
PE	0.410	0.376	0.504	0.478	0.461	0.511	0.473			
SU	0.722	0.798	0.823	0.655	0.777	0.819	NA	0.424		
PC	NA	NA	NA	NA	NA	NA	NA	NA	NA	
WD	0.398	0.685	0.499	0.303	0.469	0.445	0.597	0.256	0.476	NA

NA: Not applicable because one constitutes the other.

Table 6
Results of the structural models estimation – Airport context.

	Path	Coefficient	Std. Error	P Values	f^2	VIF	R^2	Q^2
Model 1[a]	PC-WD	−0.521	0.065	0.000***	1.956^{L}	1.324	0.277	0.256
	PE-WD	−0.010	0.072	0.885^{ns}	0.000^{N}			
	PE-PC	0.495	0.048	0.000***	0.324^{M}		0.245	0.144
Model 2[b]	PC-WD	−0.547	0.062	0.000***	0.337^{M}	1.283	0.306	0.285
	PE-WD	−0.012	0.068	0.861^{ns}	0.000^{N}			
	PE-PC	0.470	0.050	0.000***	0.283^{M}		0.221	0.137
Model 3[c]	PC-WD	−0.530	0.065	0.000***	0.297^{M}	1.322	0.285	0.264
	PE-WD	−0.007	0.071	0.922^{ns}	0.000^{N}			
	PE-PC	0.494	0.049	0.000***	0.322^{M}		0.244	0.148
Model 4[d]	PC-WD	−0.398	0.068	0.000***	0.150^{M}	1.307	0.193	0.170
	PE-WD	−0.074	0.077	0.333^{ns}	0.005^{N}			
	PE-PC	0.485	0.050	0.000***	0.307^{M}		0.235	0.147
Model 5[e]	PC -WD	−0.573	0.058	0.000***	0.385^{L}	1.269	0.331	0.311
	PE-WD	−0.006	0.067	0.923^{ns}	0.000^{N}			
	PE-PC	0.461	0.051	0.000***	0.269^{M}		0.212	0.141

[a] complete scale; [b] information management excluded; [c] awareness excluded; [d] interaction management excluded; [e] information management and awareness excluded; *** significant at $p < 0.001$; [ns] Not significant; [L] large effect; [M] medium effect; [N] no effect.

4.4. Step 6 and 7: Check nomological and concurrent validity of the construct

Assessing the nomological network further helps to determine the validity of the focal construct. It is performed by correlating each construct score with other constructs (concepts) in a conceptual model. Concurrent validity assesses the extent to which a construct score predicts scores on some criterion measure. We checked nomological and concurrent validity of privacy concerns by estimating the structural model that links it to a potential antecedent factor (privacy invasion experience) and an outcome variable (willingness to provide data). Model 1 in Table 6 shows the results where a complete scale is used.

Evaluation of the structural model should begin with the assessment of collinearity. As shown in Table 6, the observed value of VIF is well below 3, indicating the absence of collinearity problems (Hair et al., 2020). Next is the assessment of the size and significance of path coefficients. The results show that privacy concerns are significantly associated with reduced willingness to provide personal data for additional digital services at airports, the effect size being large. Likewise, privacy invasion experience is significantly related to increased privacy concerns, but the effect size is medium. Following Zhao et al. (2010), we also assessed the direct effect of privacy invasion experience on the willingness to provide personal data. The observed insignificant effect suggests that air passengers only become less willing to provide personal data for additional services at airports if their past privacy invasion led to increased privacy concerns. A structural model's predictive relevance is evaluated by assessing the value of Stone–Gaisser's Q^2. It is established when Q^2 is greater than zero, suggesting that the model makes reliable predictions of the willingness to provide personal data for additional services. The Stone–Gaisser's Q^2 values for the willingness to provide personal data confirm that privacy concerns are a relevant predictor of willingness to provide personal data for additional digital services at airports. Overall, nomological and concurrent validity of the scale for measuring privacy concerns are established.

4.5. Exploring the role of privacy concerns dimensions in the airport context

The analysis in Section 4.1 reveals that at least one of the three dimensions constituting privacy concerns is redundant. This section explores the observed redundancy by excluding interaction management, information management and awareness from the model, one at a time, and then examining the resulting R^2 for the target variable (willingness to provide personal data) and the change in the path coefficient of the relationship between privacy concerns and the willingness to provide personal data. Model 2, 3 and 4 in Table 6 show results after excluding information management, awareness, and interaction management, respectively.

The results suggest that either awareness or information management can be excluded from the privacy concerns measurement model without substantially changing the percentage of explained variation in the willingness to provide personal data. Compared to the complete model (Model 1: $R^2 = 0.277$; path coefficient = −0.521), the observed change in path coefficient when excluding information management is not significant at $p < 0.1$ (Model 2) (path coefficient changes to −0.547, $p \approx 0.337$). Insignificant change in path coefficient is also observed

when awareness is excluded (Model 3) (path coefficient changes to −0.530; p ≈ 0.444). However, excluding interaction management (Model 4) resulted in a substantial decline in R^2 (from 0.277 to 0.193), and the observed change in path coefficient (from −0.521 to −0.398) is significant at $p < 0.05$ ($p \approx 0.036$). This observation prompted further analysis to examine the effect of excluding awareness and information management (Model 5). Compared to Model 1, the change in the path coefficient is not significant at $p < 0.1$ (from −0.521 to −0.547; $p \approx 0.19$). Indeed, R^2 substantially increases (from 0.277 to 0.331). To conclude, interaction management seems to be the most important dimension of privacy concerns when predicting passengers' willingness to provide personal data for additional digital services at airports.

5. Results from the B2C retail context (Context B)

In this context, we follow the same steps as in Context A, except that we use a different dataset and a different context. According to Uncles and Kwok (2013) classification, the analysis conducted in this context is a close replication of the first context because the conceptual and methodological domains are held constant while the context is changed. Thus, CCA is conducted on a different dataset consisting of 233 respondents. Fig. 4 presents the estimated nomological network and its path coefficients. The results of the CCA steps follow.

5.1. Step 1 and 2: Estimate loadings and check indicator reliability

As shown in Table 7, as in Context A, all indicator loadings were above the recommended threshold (c.f. Section 4.1) and significant at $p < 0.01$. The significance of the loadings is also confirmed by the corresponding 95% confidence intervals (bias-corrected). The loading values and their squared values (presented in brackets) suggest that all indicators are adequately reliable.

5.2. Step 3 and 4: Check composite reliability and convergence validity

As shown in Table 7, all rho_A values are well above the recommended threshold (c.f. Section 4.2). However, as in Context A, the rho_A value for privacy concerns is above 0.95, suggesting that at least one of the three dimensions constituting it is redundant. Likewise, convergence validity for all constructs is established as the observed AVE values are above 0.5.

5.3. Step 5: Check discriminant validity

The results in Table 8 show that all HTMT values are below the recommended thresholds (c.f. Section 4.3), confirming that each of the identified constructs is distinct from the others. Therefore, as in Context A, our results support modelling privacy concerns as a third-order construct consisting of two second-order constructs (information management and interaction management) and one first-order construct (awareness).

5.4. Step 6 and 7: Check nomological and concurrent validity of the construct

As in Context A, we checked nomological and concurrent validity of privacy concerns by estimating the structural model that links it to a potential antecedent factor (privacy invasion experience) and an

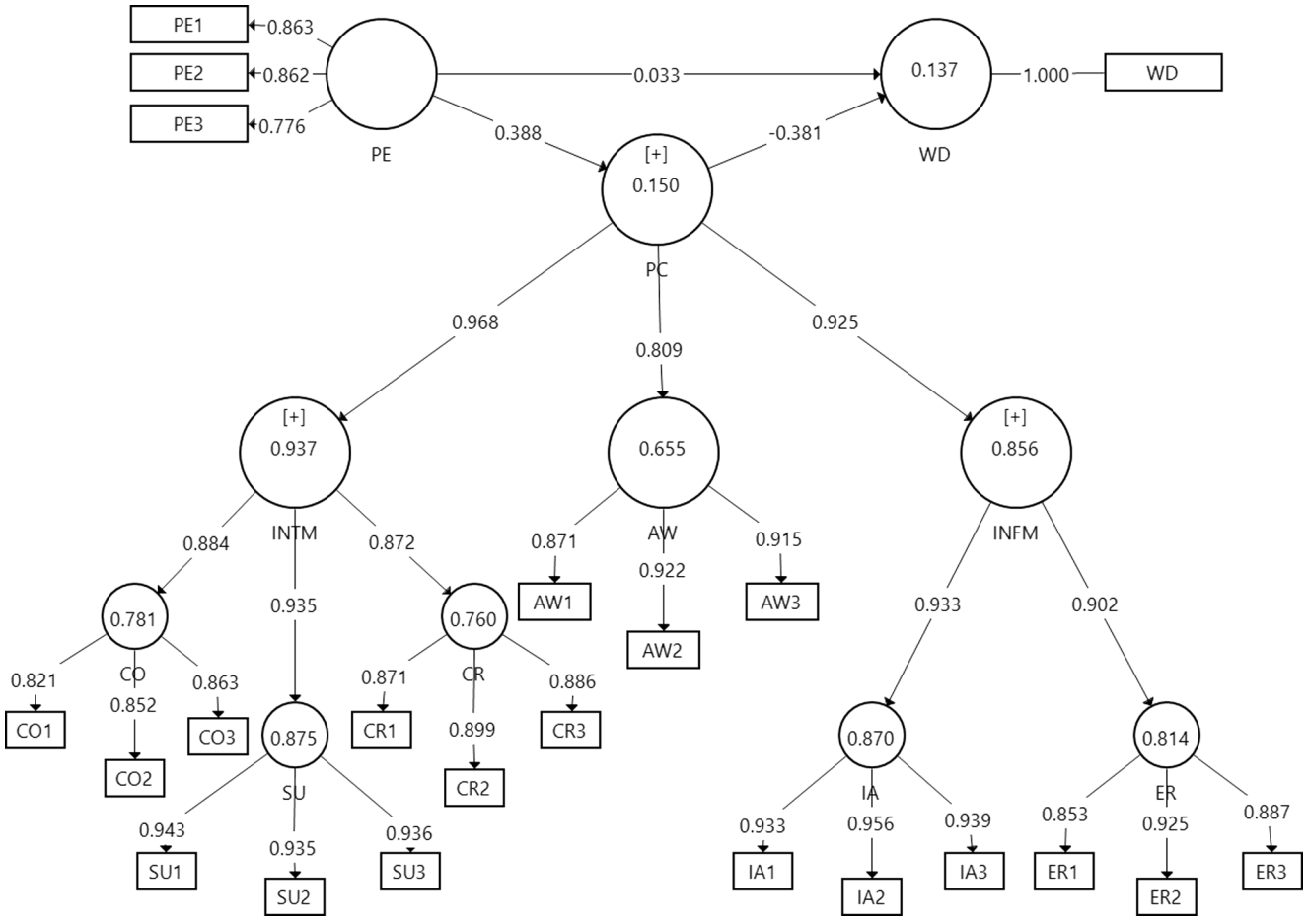

Fig. 4. The estimated nomological network – Context B.

Table 7
Results of the measurement model assessment - Retail context.

Indicator	Loading (IR)[1]	Confidence interval[2]	t-statistic	Rho_A	AVE
Collection (CO)					
CO1	0.821 (0.674)	0.742–0.872	25.116***	0.811	0.715
CO2	0.852 (0.726)	0.789–0.893	32.718***		
CO3	0.863 (0.745)	0.804–0.900	36.702***		
Secondary usage (SU)					
SU1	0.943 (0.889)	0.921–0.959	99.575***	0.932	0.879
SU2	0.935 (0.874)	0.886–0.962	50.639***		
SU3	0.936 (0.876)	0.899–0.960	61.744***		
Errors (ER)					
ER1	0.853 (0.728)	0.794–0.894	34.003***	0.876	0.790
ER2	0.925 (0.856)	0.899–0.942	84.973***		
ER3	0.887 (0.787)	0.858–0.909	68.357***		
Improper access (IA)					
IA1	0.933 (0.870)	0.906–0.953	79.742***	0.938	0.889
IA2	0.956 (0.914)	0.938–0.969	121.326***		
IA3	0.939 (0.882)	0.902–0.961	63.685***		
Control (CR)					
CR1	0.871 (0.759)	0.810–0.913	33.326***	0.867	0.784
CR2	0.899 (0.808)	0.865–0.923	60.768***		
CR3	0.886 (0.785)	0.841–0.918	45.188***		
Awareness (AW)					
AW1	0.871 (0.759)	0.794–0.913	30.096***	0.890	0.816
AW2	0.922 (0.850)	0.882–0.948	56.878***		
AW3	0.915 (0.837)	0.874–0.943	54.029***		
Privacy invasion experience (PE)					
PE1	0.863 (0.745)	0.782–0.935	22.944***	0.873	0.964
PE2	0.862 (0.743)	0.748–0.908	22.065***		
PE3	0.776 (0.602)	0.597–0.855	12.577***		
Information management (INFM)					
IA	0.933 (0.870)	0.915–0.950	113.524***	0.922	0.707
ER	0.902 (0.814)	0.780–0.886	60.327***		
Interaction management (INTM)					
CO	0.884 (0.781)	0.825–0.908	48.229***	0.933	0.639
SU	0.935 (0.874)	0.885–0.952	98.591***		
CR	0.872 (0.760)	0.862–0.924	42.114***		
Privacy concerns (PC)					
INFM	0.925 (0.937)	0.935–0.966	78.975***	0.962	0.591
AW	0.809 (0.654)	0.749–0.870	22.938***		
INTM	0.968 (0.856)	0.939–0.970	188.525***		
Willingness to provide personal data (WD)					
WD	1.000 (1.000)	NA^	NA^	1.000	1.000

[1] Indicator reliability; [2] Bias corrected; *** Significant at $p < 0.001$; ^ Not applicable: single item.

outcome variable (willingness to provide data). Model 1 in Table 9 shows the results where a complete scale is used.

As shown in Table 9, the observed value of VIF is well below 3, indicating, as in Context A, the absence of collinearity problems. Next is the assessment of the size and significance of path coefficients. As in Context A, the results show that privacy concerns are significantly associated with reduced willingness to provide personal data for additional online retail services, the effect size being large. Likewise, privacy invasion experience is significantly related to increased privacy concerns, but the effect size is medium. As in Context A, the direct effect of privacy invasion experience on the willingness to provide personal data is insignificant. This observation suggests that customers of online retailers, like air passengers, only become less willing to provide personal data for additional services if their past privacy invasion led to increased privacy concerns. The Stone–Gaisser's Q^2 values for the willingness to provide personal data confirm that privacy concerns are a relevant predictor of willingness to provide personal data for additional online retail services. Overall, as in Context A, nomological and concurrent validity of the scale for measuring privacy concerns are established.

5.5. Exploring the role of privacy concerns dimensions in the online retail context

The analysis in Section 4.2 reveals that at least one of the three dimensions constituting privacy concerns is redundant. As in Context A, this section explores the observed redundancy by excluding interaction management, information management and awareness from the model, one at a time, and then examining the resulting R^2 for the target variable (willingness to provide personal data) and the change in the path coefficient of the relationship between privacy concerns and willingness to provide personal data. Model 2, 3 and 4 in Table 9 show results after excluding information management, awareness, and interaction management, respectively.

The results suggest any of the three factors (interaction management, awareness, or information management) can be excluded from the privacy concerns measurement model without substantially changing the percentage of explained variation in the willingness to provide personal data (R^2). Compared to the complete model (Model 1: $R^2 = 0.137$; path coefficient $= -0.381$), the observed change in path coefficients is not significant at $p < 0.1$ ($p \approx 0.437$ when excluding awareness; $p \approx 0.442$ when excluding information management; $p \approx 0.500$ when excluding interaction management). This observation is different from Context A, where interaction management turned out to be a decisive factor in determining willingness to provide personal data for additional digital services at airports. Thus, further analysis was conducted to examine the effect of excluding two dimensions at a time. Model 4, 5 and 6 in Table 9 show the results of excluding information management and awareness,

Table 8
HTMT values for the constructs – Retail context.

	AW	CO	CR	ER	IA	INFM	INTM	PE	SU	PC
CO	0.803									
CR	0.733	0.752								
ER	0.542	0.674	0.776							
IA	0.744	0.782	0.846	0.752						
INFM	0.702	0.792	0.881	NA	NA					
INTM	0.803	NA	NA	0.758	0.896	0.900				
PE	0.221	0.304	0.426	0.355	0.386	0.402	0.414			
SU	0.704	0.879	0.795	0.658	0.854	0.824	NA	0.412		
PC	NA	NA	NA	NA	NA	NA	NA	NA	NA	
WD	0.271	0.442	0.307	0.267	0.367	0.346	0.392	0.113	0.348	NA

NA: Not applicable because one constitutes the other.

Table 9
Results of the structural models estimation – Retail context.

	Path	Coefficient	Std. Error	P Values	f^2	VIF	R^2	Q^2
Model 1[a]	PC-WD	−0.381	0.070	0.000***	1.985^{L}	1.177	0.137	0.114
	PE-WD	−0.033	0.075	0.665^{ns}	0.001^{N}			
	PE-PC	0.388	0.058	0.000***	0.177^{M}		0.150	0.088
Model 2[b]	PC-WD	−0.371	0.071	0.000***	0.137^{S}	1.159	0.133	0.113
	PE-WD	0.020	0.018	0.790^{ns}	0.000^{N}			
	PE-PC	0.371	0.057	0.000***	0.159^{M}		0.138	0.083
Model 3[c]	PC-WD	−0.392	0.069	0.000***	0.149^{S}	1.196	0.141	0.117
	PE-WD	0.045	0.074	0.550^{ns}	0.000^{N}			
	PE-PC	0.404	0.059	0.000***	0.196^{M}		0.164	0.099
Model 4[d]	PC-WD	−0.380	0.070	0.000***	0.142^{S}	1.176	0.136	0.113
	PE-WD	−0.032	0.074	0.668^{ns}	0.001^{N}			
	PE-PC	0.387	0.059	0.000***	0.176^{M}		0.150	0.088
Model 5[e]	PC-WD	−0.393	0.068	0.000***	0.152^{M}	1.188	0.143	0.123
	PE-WD	0.041	0.072	0.567^{ns}	0.002^{N}			
	PE-PC	0.398	0.057	0.000***	0.188^{M}		0.158	0.099
Model 6[f]	PC-WD	−0.339	0.071	0.000***	0.111^{S}	1.162	0.111	0.084
	PE-WD	0.015	0.077	0.848^{ns}	0.002^{N}			
	PE-PC	0.374	0.063	0.000***	0.162^{M}		0.140	0.097
Model 6[g]	PC-WD	−0.246	0.069	0.000***	0.062^{S}	1.059	0.074	0.084
	PE-WD	−0.071	0.068	0.365^{ns}	0.005^{N}			
	PE-PC	0.236	0.063	0.001***	0.059^{S}		0.056	0.097

[a] complete scale; [b] information management excluded; [c] awareness excluded; [d] interaction management excluded; [e] information management and awareness excluded; [f] interaction management and awareness excluded; [g] information management and interaction management excluded; *** significant at $p < 0.001$; [ns] not significant; [L] large effect; [M] medium effect; [N] no effect.

interaction management and awareness, and information management and interaction management, respectively.

The results show that excluding awareness and either information or interaction management does not significantly change the path coefficient at $p < 0.1$ ($p \approx 0.431$ when information management and awareness are excluded; $p \approx 0.275$ when interaction management and awareness excluded). Compared to the complete model, the change in R^2 is also not substantial. However, excluding both information and interaction management results in a significant decline in the path coefficient at $p < 0.05$ ($p \approx 0.028$), and a considerable change in R^2 compared to the complete model (from 0.137to 0.074). To conclude, information and interaction management seem to be the most important dimensions of privacy concerns when accounting for customers' willingness to provide personal data for additional services with online retailers.

6. Discussion

This study conducted CCA on a scale for measuring privacy concerns. The insights provided are important, especially now that privacy concerns have become a critical factor in digital business research and management. The study has extended earlier efforts to develop a scale for measuring privacy concerns by applying a recently developed approach – CCA (Hair et al., 2020). Following the in-built replication logic (Uncles and Kwok, 2013), the study is based on two different datasets representing two different contexts: airport digital services and online retail services. The results provide actionable research and managerial implications.

In terms of research implications, the results from both contexts are consistent with Hong and Thong (2013) as they confirm that privacy concerns constitute a third-order construct comprising two-second order constructs (interaction management and information management) and a first-order construct (awareness). Interestingly, the effect of privacy concerns on the willingness to provide data for additional services varies by context. While the complete model explained about 28% of the variation in willingness to provide data in the airport context, it only explained about 14% in the retail context. This is consistent with previous research that highlights the importance of context (e.g. Bansal et al., 2016). Besides, it appears that the relative importance of the three dimensions (interaction management, information management and awareness) also varies by context. In this study, interaction management is the most critical dimension in determining passengers' willingness to provide personal data for additional digital services at airports. In contrast, in the online retail context, any of the three dimensions can be excluded from the scale without causing a substantial change in the explanation of the willingness of shoppers to provide personal data for

additional services from online retailers. However, further analysis suggested that the percentage of explanation on the willingness to provide personal data remained almost intact in the online retail context when only interaction management or information management were the sole dimensions in the scale. This was not the case for awareness. These findings have implications for managers of airport digital services and online retail services, respectively.

For airport managers, the results suggest that privacy concerns matter more in their context compared to the online retail context – revealing twice as much effect on the willingness to provide data for additional services. Therefore, as airports continue to embrace digital transformation (Halpern et al. 2021a), they need to address privacy issues even more than their online retail counterparts. Three concerns comprising interaction management are the most critical: the amount of data collected and how it is collected, the use of data for other purposes, and loss of control on the data provided. Thus, as the range of additional digital services at airports increases (Halpern et al. 2020a), managers should carefully consider the type and amount of data requested from passengers for additional services, how they collect it, and the extent to which they provide them with adequate control of their data. While the other aspects (preventing improper access, informing passengers about personal data policies, and maintaining accurate data) are also important, interaction management aspects should be prioritised. As for managers of online retail services, the type and amount of data requested for additional services, how it is collected, customers' control of their data, preventing improper access, and maintaining accurate data, should be prioritised. Given that the effect of the dimensions of privacy concerns on the willingness to provide data for additional services varies by context, managers working in other business contexts where personal data are used, should consider examining the relative importance of each of the dimensions and subsequently prioritise those that are most important to the specific context of their business.

For researchers who investigate issues related to privacy concerns, the findings of this study imply that they should carefully select indicators of privacy concerns, depending on the research context in question. The common practice among researchers that include privacy concerns in their conceptual models is to measure it as a unidimensional construct, using a few items (e.g., Zlatolas et al., 2015; Morosan, 2018; Palos-Sanchez et al., 2019). Although this practice helps to shorten a questionnaire, the findings of this study suggest that it should be carefully considered because it may lead to invalid results, especially when the indicators do not include the most critical dimension(s) of privacy concerns for a given context. The findings of this study also provide a potential explanation for mixed results in past research related to privacy concerns, which was recognised as an issue in the introduction and literature review of this paper. For instance, recently, Ioannou et al. (2020) found that privacy concerns positively affect the willingness to share behavioural information. This observation is contrary to common sense and the findings of previous research. They argued that the positive effect was most likely due to the privacy paradox, meaning that individuals concerned about privacy would still be willing to share personal information given that they would gain something in return. While this explanation is partly sensible, our results offer another possible explanation. Since previous studies related to privacy concerns have been conducted in different contexts, mixed results might also be due to inadequate measurement caused by shortened scales. Thus, if researchers choose to use a shorter scale of privacy concerns, they must carefully consider their research context and include items of the most relevant dimensions of privacy concerns. This consideration is vital as the number of digital service contexts, where personal data are requested, is growing.

A limitation of this study is that it does not consider individual characteristics of the consumer because in addition to differences by context, there might also be differences by consumer. For instance, when investigating passenger preferences for using digital technologies at airports, Halpern et al. (2020b) found that privacy concerns associated with using them are significantly higher among foreigners versus those that live in the country of the airport that they are using – possibly reflecting a greater level of trust and/or willingness to provide personal data to airports in one's own country compared to those in other countries. In addition, when segmenting those same passengers, Halpern et al. (2021b) revealed three main groups: those that prefer to use traditional manual processes (such as with staff at a check-in desk), those that prefer automated technology-based processes (such as a self-service check-in kiosk), and those that prefer more personalised technology-based processes (such as using biometrics to check-in for their flight). The group that prefers more traditional manual processes, which consists mainly of infrequent leisure travellers, is most concerned about data privacy at airports, while the group that prefers more personalised processes, which consists mainly of frequent business travellers, is least concerned. The group that prefers automated technology-based processes is somewhere in-between. It is quite possible that similar differences exist in other contexts, including online retail, where privacy concerns are determined by the extent to which the user trusts and/or is familiar with the service provider that they are using, the frequency with which they use the service, and the types of products or services that they are using. There is certainly scope for more research in this area.

Similarly, data collection took place in Norway and while the overall findings of this study are expected to be transferable to other countries, there might be differences depending on the nationality of respondents. For instance, Norway is a country that is highly ranked on the European Commission's Digital Economy and Society Index (EC, 2020), meaning that the country has a higher integration of digital technologies compared to most other countries in Europe. This may therefore result in a greater willingness among Norwegians to provide personal data for digital services compared to respondents of countries that are less highly ranked in terms of digital progress.

7. Conclusion

This study has confirmed a scale for measuring privacy concerns that constitutes a third-order construct comprising two second-order constructs (interaction management and information management) and a first-order construct (awareness). To the best of our knowledge, it is one of the first studies to apply CCA – a recently proposed process for confirming PLS-SEM measurement models (Hair et al. 2020). Thus, besides confirming the privacy concerns scale, this paper also provides a valuable reference for future research that uses CCA to evaluate other measurement scales. As the findings of this study show consistent reliability scores in two different contexts (airport digital services and online retail services), future research related to privacy concerns should consider adopting and using the scale in this study in other contexts, and control for respondent characteristics (which was not done in this study), given the effect that these might have on privacy concerns.

The findings of this study also offer valuable insights for managers because they suggest that the effect of privacy concerns varies by context. This study included six dimensions of privacy: the data collection, the use of data for other purposes, loss of control, improper access, information about personal data policies, and maintaining accurate data. While all six of the dimensions are shown to be important, the findings of this study also reveal significant differences in the relative importance of them in each context. Thus, managers will need to prioritise those that are most important to the specific context of their business.

Although this study has confirmed a multi-dimensional scale for measuring privacy, researchers that include privacy concerns in their conceptual models tend to prefer a unidimensional scale. Besides, there has been intense debate in the literature over the validity of single-item scales (e.g. Sarstedt et al., 2016; Bergkvist, 2016). It appears that there is consensus that a carefully crafted single item can be used depending on the nature of the construct being measured. An interesting avenue for

future research is to assess the efficacy of carefully crafted unidimensional multi-item and single-item scales of privacy concerns versus a multi-dimensional scale that has been confirmed in this study.

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.

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 are an industry partner to the project.

References

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*, 1–21.

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

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. *Information and Management, 57*(2), Article 103168.

Bergkvist, L. (2016). The nature of doubly concrete constructs and how to identify them. *Journal of Business Research, 69*(9), 3427–3429.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (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.

EC (European Commission). (2020). Digital Economy and Society Index 2020: Norway. Brussels, EC.

Edwards, J. R. (2001). Multidimensional constructs in organizational behavior research: An integrative analytical framework. *Organizational Research Methods, 4*(2), 144–192.

Fan, D. X. F., Hsu, C. H. C., & Lin, B. (2020). Tourists' experiential value co-creation through online social contacts: Customer-dominant logic perspective. *Journal of Business Research, 108*(January), 163–173.

Fried, C. (1968). Privacy. *Yales Law Journal, 77*, 475–493.

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review, 102*(3), 349–353.

Hair, J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in pls-sem using confirmatory composite analysis. *Journal of Business Research, 109* (March), 101–110.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. London: Sage Publications.

Halpern, N., Budd, T., Suau-Sanchez, P., Bråthen, S., & Mwesiumo, D. (2020a). Conceptualising airport digital maturity and dimensions of technological and organisational transformation. *Journal of Airport Management, 14*(4), 1–22.

Halpern, N., Budd, T., Suau-Sanchez, P., Bråthen, S., & Mwesiumo, D. (2020b). *Survey on Passenger Preferences and Opinions Regarding Digital Technologies at Airports in Norway*. Oslo: Kristiania University College.

Halpern, N., Mwesiumo, D., Suau-Sanchez, P., Budd, T., & Bråthen, S. (2021a). Ready for digital transformation? The effect of organisational readiness, innovation, airport size and ownership on digital change at airports. *Journal of Air Transport Management, 90*, 101949. https://doi.org/10.1016/j.jairtraman.2020.101949.

Halpern, N., Mwesiumo, D., Suau-Sanchez, P., Budd, T., & Bråthen, S. (2021b). Segmentation of passenger preferences for using digital technologies at airports. *Journal of Air Transport Management, 91*(March), 1–13, 102005.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualisation and four empirical studies. *MIS Quarterly, 37*(1), 275–298.

Hubbard, R., & Lindsay, R. M. (2013). From significant difference to significant sameness: Proposing a paradigm shift in business research. *Journal of Business Research, 66*(9), 1377–1388.

Ioannou, A., Tussyadiah, I., & Lu, Y. (2020). Privacy concerns and disclosure of biometric and behavioral data for travel. *International Journal of Information Management, 54* (October), Article 102122.

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. *Computers in Human Behavior, 107*(June), Article 106260.

Kharouf, H., Biscaia, R., Garcia-Perez, A., & Hickman, E. (2020). Understanding online event experience: The importance of communication, engagement and interaction. *Journal of Business Research, 121*(December), 735–746.

Krishen, A. S., Raschke, R. L., Close, A. G., & Kachroo, P. (2017). A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services. *Journal of Business Research, 73*(April), 20–29.

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

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

Masur, P. K. (Ed.). (2019). *Situational Privacy and Self-Disclosure*. Cham: Springer International Publishing.

Meehan, M., 2019. Data privacy will be the most important issue in the next decade. Forbes. Available at: https://www.forbes.com/sites/marymeehan/2019/11/26/data-privacy-will-be-the-most-important-issue-in-the-next-decade/#3694c28f1882.

Miltgen, C. L., Henseler, J., Gelhard, C., & Popovič, A. (2016). Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research, 69* (10), 4659–4666.

Moor, J. H. (1990). The ethics of privacy protection. *Library Trends, 39*, 69–82.

Morosan, C. (2018). Information disclosure to biometric e-gates: The roles of perceived security, benefits, and emotions. *Journal of Travel Research, 57*(5), 644–657.

Mwesiumo, D., & Halpern, N. (2018). Acquiescence and conflict in exchanges between inbound tour operators and their overseas outbound partners: A case study on Tanzania. *Tourism Management, 69*(December), 345–355.

Mwesiumo, D., Halpern, N., & Buvik, A. (2019). Effect of detailed contracts and partner irreplaceability on interfirm conflicts in cross-border package tour operations: Inbound tour operatoŕs perspective. *Journal of Travel Research, 2*, 298–312.

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. *Journal of Business Research, 112*(May), 531–540.

Palos-Sanchez, P., Saura, J. R., & Martin-Velicia, F. (2019). A study of the effects of programmatic advertising on users' concerns about privacy overtime. *Journal of Business Research, 96*(March), 61–72.

Polites, G. L., Roberts, N., & Thatcher, J. (2012). Conceptualising models using multidimensional constructs: A review and guidelines for their use. *European Journal of Information Systems, 21*(1), 22–48.

Sarstedt, M., Diamantopoulos, A., Salzberger, T., & Baumgartner, P. (2016). Selecting single items to measure doubly concrete constructs: A cautionary tale. *Journal of Business Research, 69*(8), 3159–3167.

Sarstedt, M., Hair, J. F., Cheah, J.-H., Becker, J.-M., & Ringle, C. M. (2019). How to specify, estimate, and validate higher-order constructs in PLS-SEM. *Australasian Marketing Journal, 27*(3), 197–211.

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

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

Smith, S. M., Roster, C. A., Golden, L. L., & Albaum, G. S. (2016). A multi-group analysis of online survey respondent data quality: Comparing a regular usa consumer panel to mturk samples. *Journal of Business Research, 69*(8), 3139–3148.

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

Uncles, M. D., & Kwok, S. (2013). Designing research with in-built differentiated replication. *Journal of Business Research, 66*(9), 1398–1405.

Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2019). Data analytics in a privacy-concerned world. *Journal of Business Research, 122*(January), 915–925.

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 Information Review, 42*(6), 923–939.

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research, 37*(2), 197–206.

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior, 45*(April), 158–167.

Deodat Mwesiumo Deodat Mwesiumo is an Associate Professor in supply chain management at Molde University College, Specialized University in Logistics, Norway. His research activities focus on interorganisational relations in value chains and digital business management. His work has appeared in internationally accredited scientific journals, including Technovation, Tourism Management, Journal of Travel Research and Journal of Purchasing & Supply Management.

Nigel Halpern Nigel Halpern is Professor of Air Transport and Tourism Management at Kristiania University College, Norway. His main interests are in airport digital transformation, airport marketing and strategy, airport service quality, geographies of air transport and tourism, accessible tourism, wider impacts of air transport and tourism and interorganisational relations in air transport and tourism. He has published extensively including a book on Airport Marketing (Routledge, 2013), and the Routledge Companion to Air Transport Management (Routledge, 2018).

Thomas Budd Thomas Budd is a Lecturer in Airport Planning and Management in the Centre for Air Transport Management at Cranfield University, UK, and Course Director for the MSc in Airport Planning and Management. His research and teaching activities focus on issues of air transport environmental sustainability and resilience planning, and how disruptive technologies can be leveraged to facilitate safe, seamless and sustainable journeys. His research in this area has been widely published in leading peer-reviewed academic journals and industry textbooks, including The Journal of Transport Geography, Transportation Research: Part A and the Journal of Air Transport Management.

Pere Suau-Sanchez Pere Suau-Sanchez is a Senior Lecturer in Air Transport Management at Cranfield University and Associate Professor at the Open University of Catalonia. His teaching activities are focused on strategy and digital transformation. His research and consultancy activities expand over a wide range of topics, including digital aviation, airport connectivity, route development, airport strategy, spatial planning around airports and aircraft noise annoyance. He has participated in research grants and has also led aviation consultancy projects for a diverse range of international clients. He is a regular contributor to international press, including the BBC, CNN, Forbes, La Vanguardia, Expansión, among others.

Svein Bråthen Svein Bråthen is Full Professor in Transport Economics at Molde University College, Specialized University in Logistics, Norway. His main research activities are within Transport Economics including Economic Impact Assessment (EIA) of Transport Infrastructure (Cost Benefit Analysis, CBA), Regional Economics and Air Transport Economics. He has also worked with intermodal freight markets, logistics/supply chain management and funding of transport investments and transport services. On several occasions, he has done work for the Organisation for Economic Co-operation and Development/International Transport Forum on air transport issues. He has recently been member of an expert group dealing with air transport and its economic and environmental impacts, appointed by the Norwegian Government.